Garrett ©*2004*

Crypto Homework version 101

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Bringyourownrefreshments" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 5$, $b = 10$.

(1.3) The ciphertext GURERVFABOHFVARFFYVXRFUBJOHFVARFF was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}u\text{”}) = \text{“}t\text{”}$ and $E_{a,b}(\text{“}p\text{”}) = \text{“}k\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 100 times in a row, out of which there were 44 heads and 56 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 3 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'FOEW' and 'EFWO' do *not* have 'F' adjacent to 'O' and do *not* have 'E' adjacent to 'W' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 5 & 8 & 12 & 2 & 3 & 4 & 10 & 13 & 1 & 7 & 14 & 6 & 11 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 13 & 5 & 12 & 7 & 1 & 8 & 6 & 3 & 4 & 11 & 10 & 9 & 14 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 4 red balls and 5 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 8 red balls and 9 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 9 blue balls, and 12 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3211, 247 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 93343, 101951.

(5.3) Efficiently compute a multiplicative inverse of 331 modulo 1013.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24} - 1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56} - 1$ and $5^{72} - 1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 39 modulo 43.

(7.3) Find a cube root of 100 mod 179.

(7.4) Find a cube root of 214 modulo 241.

(7.5) Try to find a cube root of 32 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 51 is a non-prime Fermat pseudoprime base 35.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 115 say about the primality or not of 1409?

(8.4) Verify that 125 is a non-prime strong pseudoprime base 57.

(8.5) What does the Miller-Rabin test base 48 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16171$, and public (encryption) keys $e_A = 29, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 7133$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 5 \bmod 53 \\ x = 17 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 16 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 4.

(9.3) Consider the quadratic polynomial $x^2 - 5x + 6$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 5x + 6 = (x-2) \cdot (x-3)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 5x + 6 = 0 \bmod 299$. In addition to the 'obvious' roots 2, 3 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 47 is a cube root of 220 modulo the prime 331, find a cube root of 220 modulo 331^2.

Unit 10 due Wed Dec 1

(10.1) The integer 216409 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 216409. When you give the oracle $33 \cdot 33$ to take the square root, it returns 101605. Factor 216409.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 15) \,\%\, 29$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 102

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Astitchintimesavesnine" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "bus" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 5$.

(1.3) The ciphertext LAPYYJDLGPOTDYZESTYRXFNS was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}x\text{”}) = \text{“}j\text{”}$ and $E_{a,b}(\text{“}u\text{”}) = \text{“}i\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 102 times in a row, out of which there were 45 heads and 57 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 4 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 7 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'MVLD' and 'LMDV' do *not* have 'M' adjacent to 'V' and do *not* have 'L' adjacent to 'D' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 6 & 13 & 7 & 11 & 12 & 14 & 10 & 3 & 8 & 9 & 5 & 1 & 2 & 4 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 5 & 8 & 3 & 7 & 11 & 10 & 14 & 12 & 1 & 6 & 4 & 9 & 13 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 5 red balls and 7 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 5 red balls and 6 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 5 red balls, 6 blue balls, and 19 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 2783, 253 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 94579, 103793.

(5.3) Efficiently compute a multiplicative inverse of 337 modulo 1019.

(5.4) Systematically find $\gcd(n, n+3, n+23)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $3^{39} \,\%\, 79$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 39 modulo 47.

(7.3) Find a cube root of 145 mod 191.

(7.4) Find a cube root of 201 modulo 277.

(7.5) Try to find a cube root of 35 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 55 is a non-prime Fermat pseudoprime base 21.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 76 say about the primality or not of 1217?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 142.

(8.5) What does the Miller-Rabin test base 48 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17441$, and public (encryption) keys $e_A = 31, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 8863$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 6 \bmod 59 \\ x = 1 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 25 modulo 4747. Specifically, find two more in addition to the 'obvious' square roots ± 5.

(9.3) Consider the quadratic polynomial $x^2 - 7x + 12$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 7x + 12 = (x-3) \cdot (x-4)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 7x + 12 = 0 \bmod 391$. In addition to the 'obvious' roots 3, 4 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 67 is a cube root of 261 modulo the prime 347, find a cube root of 261 modulo 347^2.

Unit 10 due Wed Dec 1

(10.1) The integer 204889 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 204889. When you give the oracle $43 \cdot 43$ to take the square root, it returns 203608. Factor 204889.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 731, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (6 \cdot s_n + 12)\,\%\,29$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 6)\,\%\,107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 103

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Honestyisthebestpolicy" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "kit" by an affine cipher $E(x) = (ax + b)\,\%\,26$ with key $a = 9$, $b = 6$.

(1.3) The ciphertext DYLOYBXYDDYLODRKDSCDROSXPSXSDSFO was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}a\text{"}) = \text{"}l\text{"}$ and $E_{a,b}(\text{"}l\text{"}) = \text{"}c\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 104 times in a row, out of which there were 46 heads and 58 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 5 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 6-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 8 elements to a set with 13 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'TCSK' and 'STKC' do *not* have 'T' adjacent to 'C' and do *not* have 'S' adjacent to 'K' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 3 & 8 & 14 & 7 & 13 & 5 & 9 & 11 & 4 & 12 & 1 & 10 & 6 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 5 & 11 & 6 & 13 & 4 & 10 & 14 & 7 & 12 & 1 & 3 & 8 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 6 red balls and 9 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 9 red balls and 14 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 9 red balls, 14 blue balls, and 13 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 4901, 377 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 97781, 107753.

(5.3) Efficiently compute a multiplicative inverse of 347 modulo 1021.

(5.4) Systematically find $\gcd(n, n+5, n+19)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48}-1$ and $7^{54}-1$.

(6.3) Efficiently compute $2^{41} \,\%\, 83$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 58 modulo 59.

(7.3) Find a cube root of 12 mod 197.

(7.4) Find a cube root of 310 modulo 337.

(7.5) Try to find a cube root of 35 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 57 is a non-prime Fermat pseudoprime base 20.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1217?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 117.

(8.5) What does the Miller-Rabin test base 49 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 18203$, and public (encryption) keys $e_A = 37, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 11629$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 7 \bmod 61 \\ x = 2 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 36 modulo 5141. Specifically, find two more in addition to the 'obvious' square roots ± 6.

(9.3) Consider the quadratic polynomial $x^2 - 9x + 20$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 9x + 20 = (x-4)\cdot(x-5)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 9x + 20 = 0 \bmod 437$. In addition to the 'obvious' roots 4, 5 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 87 is a cube root of 105 modulo the prime 367, find a cube root of 105 modulo 367^2.

Unit 10 due Wed Dec 1

(10.1) The integer 202313 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 202313. When you give the oracle $41 \cdot 41$ to take the square root, it returns 198977. Factor 202313.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 689, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 11) \,\%\, 29$ with $s_o = 1$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 7) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 1, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 104

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Pennywiseandpoundfoolish" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "sue" by an affine cipher $E(x) = (ax + b) \,\%\, 26$ with key $a = 11$, $b = 7$.

(1.3) The ciphertext DGZFIUOQMERMEFFAEFMKUZFTQEMYQBXMOQ was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}d\text{"}) = \text{"}l\text{"}$ and $E_{a,b}(\text{"}o\text{"}) = \text{"}q\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 106 times in a row, out of which there were 47 heads and 59 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 2 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 6-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 9 elements to a set with 15 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'AJZR' and 'ZARJ' do *not* have 'A' adjacent to 'J' and do *not* have 'Z' adjacent to 'R' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 11 & 1 & 7 & 14 & 5 & 3 & 4 & 12 & 6 & 2 & 10 & 9 & 13 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 3 & 4 & 12 & 11 & 14 & 9 & 1 & 8 & 7 & 2 & 13 & 5 & 6 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 7 red balls and 11 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 6 red balls and 11 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 6 red balls, 11 blue balls, and 7 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3751, 341 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n \to +\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 87391, 111557.

(5.3) Efficiently compute a multiplicative inverse of 349 modulo 1031.

(5.4) Systematically find $\gcd(n, n+7, n+31)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21} - 1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64} - 1$ and $6^{72} - 1$.

(6.3) Efficiently compute $3^{44} \,\%\, 89$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 34 modulo 43.

(7.3) Find a cube root of 74 mod 131.

(7.4) Find a cube root of 31 modulo 349.

(7.5) Try to find a cube root of 35 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 14.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 124 say about the primality or not of 1217?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 68.

(8.5) What does the Miller-Rabin test base 50 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 19177$, and public (encryption) keys $e_A = 41, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 461$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 8 \bmod 47 \\ x = 3 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 49 modulo 5251. Specifically, find two more in addition to the 'obvious' square roots ± 7.

(9.3) Consider the quadratic polynomial $x^2 - 11x + 30$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 11x + 30 = (x - 5) \cdot (x - 6)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 11x + 30 = 0 \bmod 319$. In addition to the 'obvious' roots 5, 6 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 107 is a cube root of 209 modulo the prime 383, find a cube root of 209 modulo 383^2.

Unit 10 due Wed Dec 1

(10.1) The integer 173441 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 173441. When you give the oracle $31 \cdot 31$ to take the square root, it returns 172719. Factor 173441.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 611, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 15) \,\%\, 31$ with $s_o = 7$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (53 \cdot s_n + 8) \,\%\, 113$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 105

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Awinkisasgoodasanod" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "dog" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 8$.

(1.3) The ciphertext CQNAJRWRWBYJRWOJUUBVJRWUHXWCQNYJCRX was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 12 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}g\text{"}) = \text{"}z\text{"}$ and $E_{a,b}(\text{"}j\text{"}) = \text{"}s\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 87 times in a row, out of which there were 27 heads and 60 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 3 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 5-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 3 elements to a set with 5 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'HQGY' and 'GHYQ' do *not* have 'H' adjacent to 'Q' and do *not* have 'G' adjacent to 'Y' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 7 & 6 & 11 & 13 & 10 & 2 & 5 & 8 & 12 & 14 & 4 & 1 & 3 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 12 & 5 & 4 & 14 & 7 & 10 & 1 & 3 & 8 & 2 & 13 & 6 & 11 & 9 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 8 red balls and 8 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 3 red balls and 8 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 3 red balls, 8 blue balls, and 14 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2873, 221 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 88579, 101597.

(5.3) Efficiently compute a multiplicative inverse of 353 modulo 1033.

(5.4) Systematically find $\gcd(n, n+5, n+17)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $2^{29} \,\%\, 59$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 45 modulo 47.

(7.3) Find a cube root of 125 mod 137.

(7.4) Find a cube root of 104 modulo 193.

(7.5) Try to find a cube root of 36 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 11. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 19 say about the primality or not of 1601?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 43.

(8.5) What does the Miller-Rabin test base 51 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 15857$, and public (encryption) keys $e_A = 11, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 7091$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 9 \bmod 53 \\ x = 4 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 64 modulo 3277. Specifically, find two more in addition to the 'obvious' square roots ± 8.

(9.3) Consider the quadratic polynomial $x^2 - 13x + 42$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 13x + 42 = (x-6) \cdot (x-7)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 13x + 42 = 0 \bmod 299$. In addition to the 'obvious' roots 6, 7 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 127 is a cube root of 75 modulo the prime 401, find a cube root of 75 modulo 401^2.

Unit 10 due Wed Dec 1

(10.1) The integer 155929 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 155929. When you give the oracle $47 \cdot 47$ to take the square root, it returns 138885. Factor 155929.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 901, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (4 \cdot s_n + 16) \,\%\, 31$ with $s_o = 6$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 2) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 0, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0$^{\text{th}}$ state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 106

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Burnthecandleatbothends" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "cat" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 5$, $b = 9$.

(1.3) The ciphertext BPMZIQVQVAXIQVNITTAUIQVTGWVBPMOIZIOM was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 16 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(``j") = ``l"$ and $E_{a,b}(``o") = ``s"$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 89 times in a row, out of which there were 28 heads and 61 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 4 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 4-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 4 elements to a set with 7 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'OXNF' and 'NOFX' do *not* have 'O' adjacent to 'X' and do *not* have 'N' adjacent to 'F' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 13 & 3 & 5 & 11 & 4 & 8 & 10 & 7 & 6 & 9 & 1 & 14 & 2 & 12 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 4 & 13 & 2 & 1 & 14 & 9 & 12 & 6 & 7 & 3 & 11 & 5 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 9 red balls and 10 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 7 red balls and 5 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 7 red balls, 5 blue balls, and 8 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 2299, 209 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 92881, 107531.

(5.3) Efficiently compute a multiplicative inverse of 359 modulo 1039.

(5.4) Systematically find $\gcd(n, n+7, n+11)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $2^{30} \,\%\, 61$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 56 modulo 59.

(7.3) Find a cube root of 103 mod 149.

(7.4) Find a cube root of 122 modulo 211.

(7.5) Try to find a cube root of 39 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 66 is a non-prime Fermat pseudoprime base 31.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 42 say about the primality or not of 1601?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 150.

(8.5) What does the Miller-Rabin test base 52 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16789$, and public (encryption) keys $e_A = 19, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 13915$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 10 \bmod 59 \\ x = 5 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 81 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 9.

(9.3) Consider the quadratic polynomial $x^2 - 15x + 56$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 15x + 56 = (x - 7) \cdot (x - 8)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 15x + 56 = 0 \bmod 391$. In addition to the 'obvious' roots 7, 8 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 147 is a cube root of 78 modulo the prime 421, find a cube root of 78 modulo 421^2.

Unit 10 due Wed Dec 1

(10.1) The integer 140873 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 140873. When you give the oracle $43 \cdot 43$ to take the square root, it returns 121942. Factor 140873.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 779, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 13) \,\%\, 31$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 1, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 107

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Haveyourcakeandeatittoo" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "fox" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 10$.

(1.3) The ciphertext BHGBSGURSELVATCNAVAGBGURPYBFRG was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}m\text{"}) = \text{"}j\text{"}$ and $E_{a,b}(\text{"}t\text{"}) = \text{"}m\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 91 times in a row, out of which there were 29 heads and 62 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 5 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 7-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 5 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'VEUM' and 'UVME' do *not* have 'V' adjacent to 'E' and do *not* have 'U' adjacent to 'M' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 13 & 14 & 3 & 12 & 1 & 9 & 2 & 7 & 8 & 10 & 4 & 6 & 5 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 14 & 8 & 7 & 1 & 12 & 5 & 11 & 13 & 6 & 4 & 9 & 10 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 10 red balls and 12 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 4 red balls and 13 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 4 red balls, 13 blue balls, and 15 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3887, 299 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 101617, 114511.

(5.3) Efficiently compute a multiplicative inverse of 367 modulo 1049.

(5.4) Systematically find $\gcd(n, n+11, n+13)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $2^{33} \,\%\, 67$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 22 modulo 43.

(7.3) Find a cube root of 98 mod 167.

(7.4) Find a cube root of 26 modulo 223.

(7.5) Try to find a cube root of 39 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 69 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 61 say about the primality or not of 1601?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 99.

(8.5) What does the Miller-Rabin test base 53 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17869$, and public (encryption) keys $e_A = 23, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 16831$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 11 \bmod 61 \\ x = 6 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 100 modulo 3959. Specifically, find two more in addition to the 'obvious' square roots ± 10.

(9.3) Consider the quadratic polynomial $x^2 - 17x + 72$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 17x + 72 = (x-8) \cdot (x-9)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 17x + 72 = 0 \bmod 437$. In addition to the 'obvious' roots 8, 9 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 167 is a cube root of 204 modulo the prime 443, find a cube root of 204 modulo 443^2.

Unit 10 due Wed Dec 1

(10.1) The integer 106241 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 106241. When you give the oracle $61 \cdot 61$ to take the square root, it returns 59142. Factor 106241.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 799, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (6 \cdot s_n + 17) \,\%\, 31$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 4) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 1, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 108

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Meetinthealleyatmidnight" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 9$, $b = 5$.

(1.3) The ciphertext ESPCPTDYZMFDTYPDDWTVPDSZHMFDTYPDD was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}p\text{"}) = \text{"}t\text{"}$ and $E_{a,b}(\text{"}y\text{"}) = \text{"}a\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 93 times in a row, out of which there were 30 heads and 63 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 2 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'CLBT' and 'BCTL' do *not* have 'C' adjacent to 'L' and do *not* have 'B' adjacent to 'T' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 1 & 2 & 6 & 12 & 7 & 9 & 4 & 13 & 8 & 14 & 5 & 10 & 3 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 13 & 11 & 10 & 12 & 1 & 8 & 14 & 9 & 7 & 3 & 4 & 5 & 2 & 6 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 2 red balls and 5 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 8 red balls and 10 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 10 blue balls, and 9 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3509, 319 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 86609, 97403.

(5.3) Efficiently compute a multiplicative inverse of 373 modulo 1051.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21} - 1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48} - 1$ and $7^{54} - 1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 41 modulo 47.

(7.3) Find a cube root of 102 mod 173.

(7.4) Find a cube root of 85 modulo 241.

(7.5) Try to find a cube root of 39 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 45 is a non-prime Fermat pseudoprime base 17.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1601?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 89.

(8.5) What does the Miller-Rabin test base 54 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16459$, and public (encryption) keys $e_A = 29, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 4469$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 12 \bmod 47 \\ x = 7 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 121 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 11.

(9.3) Consider the quadratic polynomial $x^2 - 19x + 90$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 19x + 90 = (x - 9) \cdot (x - 10)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 19x + 90 = 0 \bmod 319$. In addition to the 'obvious' roots 9, 10 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 187 is a cube root of 379 modulo the prime 461, find a cube root of 379 modulo 461^2.

Unit 10 due Wed Dec 1

(10.1) The integer 106241 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 106241. When you give the oracle $19 \cdot 19$ to take the square root, it returns 96528. Factor 106241.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 19) \,\%\, 31$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 109

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Bringyourownrefreshments" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "bus" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 6$.

(1.3) The ciphertext KZOXXICKFONSCXYDRSXQWEMR was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 19 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}$("s") = "p" and $E_{a,b}$("d") = "i". Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 95 times in a row, out of which there were 31 heads and 64 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 3 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 7 elements to a set with 13 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'JSIA' and 'IJAS' do *not* have 'J' adjacent to 'S' and do *not* have 'I' adjacent to 'A' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 12 & 14 & 9 & 11 & 1 & 13 & 4 & 2 & 6 & 5 & 8 & 3 & 10 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 8 & 11 & 2 & 4 & 14 & 10 & 1 & 7 & 12 & 3 & 13 & 6 & 9 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 3 red balls and 7 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 5 red balls and 7 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 5 red balls, 7 blue balls, and 16 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 5239, 403 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 91261, 100729.

(5.3) Efficiently compute a multiplicative inverse of 379 modulo 1061.

(5.4) Systematically find $\gcd(n, n+3, n+23)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64}-1$ and $6^{72}-1$.

(6.3) Efficiently compute $3^{39} \,\%\, 79$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 31 modulo 59.

(7.3) Find a cube root of 118 mod 179.

(7.4) Find a cube root of 275 modulo 277.

(7.5) Try to find a cube root of 40 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 49 is a non-prime Fermat pseudoprime base 18.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 105 say about the primality or not of 1601?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 80.

(8.5) What does the Miller-Rabin test base 55 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 19939$, and public (encryption) keys $e_A = 31, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 9511$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 13 \bmod 53 \\ x = 8 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 144 modulo 4747. Specifically, find two more in addition to the 'obvious' square roots ± 12.

(9.3) Consider the quadratic polynomial $x^2 - 21x + 110$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 21x + 110 = (x - 10) \cdot (x - 11)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 21x + 110 = 0 \bmod 299$. In addition to the 'obvious' roots 10, 11 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 207 is a cube root of 12 modulo the prime 487, find a cube root of 12 modulo 487^2.

Unit 10 due Wed Dec 1

(10.1) The integer 140873 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 140873. When you give the oracle $7 \cdot 7$ to take the square root, it returns 65328. Factor 140873.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 731, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (8 \cdot s_n + 23)\,\%\,31$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 6)\,\%\,107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 110

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext “Astitchintimesavesnine” by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext “kit” by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 7$.

(1.3) The ciphertext FANQADZAFFANQFTMFUEFTQUZRUZUFUHQ was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 11 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}o\text{”}) = \text{“}x\text{”}$ and $E_{a,b}(\text{“}f\text{”}) = \text{“}w\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 97 times in a row, out of which there were 32 heads and 65 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 4 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 6-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 8 elements to a set with 10 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings ‘QZPH’ and ‘PQHZ’ do *not* have ‘Q’ adjacent to ‘Z’ and do *not* have ‘P’ adjacent to ‘H’ in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 11 & 2 & 9 & 1 & 5 & 4 & 6 & 8 & 12 & 10 & 3 & 14 & 13 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 13 & 5 & 7 & 10 & 2 & 4 & 12 & 14 & 6 & 3 & 9 & 11 & 1 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 4 red balls and 4 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 9 red balls and 4 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 9 red balls, 4 blue balls, and 10 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2057, 187 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 93881, 104641.

(5.3) Efficiently compute a multiplicative inverse of 313 modulo 1009.

(5.4) Systematically find $\gcd(n, n+5, n+19)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $2^{41} \,\%\, 83$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 3 modulo 43.

(7.3) Find a cube root of 139 mod 191.

(7.4) Find a cube root of 180 modulo 337.

(7.5) Try to find a cube root of 42 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 51 is a non-prime Fermat pseudoprime base 35.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 46 say about the primality or not of 1409?

(8.4) Verify that 265 is a non-prime strong pseudoprime base 23.

(8.5) What does the Miller-Rabin test base 56 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16463$, and public (encryption) keys $e_A = 37, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 13573$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 3 \bmod 59 \\ x = 9 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 4 modulo 5141. Specifically, find two more in addition to the 'obvious' square roots ± 2.

(9.3) Consider the quadratic polynomial $x^2 - 3x + 2$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 3x + 2 = (x-1) \cdot (x-2)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 3x + 2 = 0 \bmod 391$. In addition to the 'obvious' roots 1, 2 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 7 is a cube root of 62 modulo the prime 281, find a cube root of 62 modulo 281^2.

Unit 10 due Wed Dec 1

(10.1) The integer 155929 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 155929. When you give the oracle $17 \cdot 17$ to take the square root, it returns 105694. Factor 155929.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 689, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 11) \,\%\, 29$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 7) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 1, 1, 1, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 111

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Honestyisthebestpolicy" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "sue" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 5$, $b = 8$.

(1.3) The ciphertext ADWCFRLNJBOJBCCXBCJHRWCQNBJVNYUJLN was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 13 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}r\text{"}) = \text{"}p\text{"}$ and $E_{a,b}(\text{"}k\text{"}) = \text{"}g\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 99 times in a row, out of which there were 33 heads and 66 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 5 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 6-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 9 elements to a set with 12 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'XGWO' and 'WXOG' do *not* have 'X' adjacent to 'G' and do *not* have 'W' adjacent to 'O' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 12 & 4 & 14 & 6 & 3 & 10 & 11 & 7 & 8 & 13 & 5 & 1 & 2 & 9 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 12 & 14 & 13 & 8 & 4 & 7 & 2 & 1 & 11 & 9 & 6 & 5 & 3 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 5 red balls and 6 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 6 red balls and 12 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 6 red balls, 12 blue balls, and 17 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3211, 247 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 95663, 107587.

(5.3) Efficiently compute a multiplicative inverse of 317 modulo 1013.

(5.4) Systematically find $\gcd(n, n+7, n+31)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $3^{44} \,\%\, 89$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 40 modulo 47.

(7.3) Find a cube root of 191 mod 197.

(7.4) Find a cube root of 21 modulo 349.

(7.5) Try to find a cube root of 42 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 55 is a non-prime Fermat pseudoprime base 21.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 49 say about the primality or not of 1409?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 133.

(8.5) What does the Miller-Rabin test base 57 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17201$, and public (encryption) keys $e_A = 41, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 413$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 4 \bmod 61 \\ x = 10 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 9 modulo 5251. Specifically, find two more in addition to the 'obvious' square roots ± 3.

(9.3) Consider the quadratic polynomial $x^2 - 5x + 6$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 5x + 6 = (x - 2) \cdot (x - 3)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 5x + 6 = 0 \bmod 437$. In addition to the 'obvious' roots 2, 3 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 27 is a cube root of 35 modulo the prime 307, find a cube root of 35 modulo 307^2.

Unit 10 due Wed Dec 1

(10.1) The integer 173441 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 173441. When you give the oracle $29 \cdot 29$ to take the square root, it returns 62219. Factor 173441.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 611, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (4 \cdot s_n + 13)\,\%\,29$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (53 \cdot s_n + 8)\,\%\,113$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0$^{\text{th}}$ state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 112

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Pennywiseandpoundfoolish" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "dog" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 9$.

(1.3) The ciphertext BPMZIQVQVAXIQVNITTAUIQVTGWVBPMXIBQW was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}u\text{"}) = \text{"}t\text{"}$ and $E_{a,b}(\text{"}p\text{"}) = \text{"}k\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 101 times in a row, out of which there were 34 heads and 67 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 2 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 5-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 3 elements to a set with 7 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'ENDV' and 'DEVN' do *not* have 'E' adjacent to 'N' and do *not* have 'D' adjacent to 'V' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 6 & 13 & 4 & 5 & 14 & 11 & 9 & 12 & 7 & 3 & 8 & 1 & 10 & 2 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 7 & 12 & 9 & 11 & 4 & 8 & 14 & 10 & 13 & 5 & 1 & 6 & 3 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 6 red balls and 8 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 3 red balls and 9 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 3 red balls, 9 blue balls, and 11 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 2783, 253 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 86147, 99443.

(5.3) Efficiently compute a multiplicative inverse of 331 modulo 1019.

(5.4) Systematically find $\gcd(n, n+5, n+17)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21} - 1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140} - 1$ and $2^{120} - 1$.

(6.3) Efficiently compute $2^{29} \,\%\, 59$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 42 modulo 59.

(7.3) Find a cube root of 57 mod 131.

(7.4) Find a cube root of 27 modulo 193.

(7.5) Try to find a cube root of 43 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 57 is a non-prime Fermat pseudoprime base 20.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 115 say about the primality or not of 1409?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 12.

(8.5) What does the Miller-Rabin test base 58 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16157$, and public (encryption) keys $e_A = 11, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 2891$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 5 \bmod 47 \\ x = 11 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 16 modulo 3277. Specifically, find two more in addition to the 'obvious' square roots ± 4.

(9.3) Consider the quadratic polynomial $x^2 - 7x + 12$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 7x + 12 = (x-3) \cdot (x-4)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 7x + 12 = 0 \bmod 319$. In addition to the 'obvious' roots 3, 4 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 47 is a cube root of 220 modulo the prime 331, find a cube root of 220 modulo 331^2.

Unit 10 due Wed Dec 1

(10.1) The integer 202313 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 202313. When you give the oracle $13 \cdot 13$ to take the square root, it returns 35599. Factor 202313.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 901, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 15) \,\%\, 29$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 2) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 113

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Awinkisasgoodasanod" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "cat" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 9$, $b = 10$.

(1.3) The ciphertext GURENVAVAFCNVASNYYFZNVAYLBAGURTNENTR was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}x\text{”}) = \text{“}j\text{”}$ and $E_{a,b}(\text{“}u\text{”}) = \text{“}i\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 103 times in a row, out of which there were 35 heads and 68 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 3 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 4-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 4 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'LUKC' and 'KLCU' do *not* have 'L' adjacent to 'U' and do *not* have 'K' adjacent to 'C' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 6 & 7 & 13 & 10 & 2 & 11 & 5 & 1 & 9 & 4 & 3 & 14 & 12 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 12 & 6 & 8 & 7 & 14 & 4 & 11 & 13 & 5 & 3 & 2 & 1 & 9 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 7 red balls and 10 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 7 red balls and 6 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 7 red balls, 6 blue balls, and 18 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 4901, 377 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 87953, 103127.

(5.3) Efficiently compute a multiplicative inverse of 337 modulo 1021.

(5.4) Systematically find $\gcd(n, n+7, n+11)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48}-1$ and $7^{54}-1$.

(6.3) Efficiently compute $2^{30} \,\%\, 61$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 20 modulo 43.

(7.3) Find a cube root of 90 mod 137.

(7.4) Find a cube root of 147 modulo 211.

(7.5) Try to find a cube root of 44 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 14.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 76 say about the primality or not of 1217?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 17.

(8.5) What does the Miller-Rabin test base 59 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17113$, and public (encryption) keys $e_A = 19, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 3547$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 6 \bmod 53 \\ x = 12 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 25 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 5.

(9.3) Consider the quadratic polynomial $x^2 - 9x + 20$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 9x + 20 = (x - 4) \cdot (x - 5)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 9x + 20 = 0 \bmod 299$. In addition to the 'obvious' roots 4, 5 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 67 is a cube root of 261 modulo the prime 347, find a cube root of 261 modulo 347^2.

Unit 10 due Wed Dec 1

(10.1) The integer 204889 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 204889. When you give the oracle $23 \cdot 23$ to take the square root, it returns 143631. Factor 204889.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 779, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000th point of the LCG given by $s_{n+1} = (6 \cdot s_n + 12) \,\%\, 29$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5th pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0th state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 114

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Burnthecandleatbothends" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "fox" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 5$.

(1.3) The ciphertext ZFEZQESPQCJTYRALYTYEZESPNWZDPE was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}a\text{”}) = \text{“}l\text{”}$ and $E_{a,b}(\text{“}l\text{”}) = \text{“}c\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 105 times in a row, out of which there were 36 heads and 69 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 4 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 7-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 5 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'SBRJ' and 'RSJB' do *not* have 'S' adjacent to 'B' and do *not* have 'R' adjacent to 'J' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 1 & 9 & 11 & 7 & 13 & 8 & 14 & 4 & 5 & 12 & 6 & 3 & 10 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 3 & 14 & 11 & 10 & 12 & 1 & 13 & 8 & 6 & 4 & 2 & 7 & 5 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 8 red balls and 12 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 4 red balls and 14 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 4 red balls, 14 blue balls, and 12 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3751, 341 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n \to +\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 89711, 105559.

(5.3) Efficiently compute a multiplicative inverse of 347 modulo 1031.

(5.4) Systematically find $\gcd(n, n+11, n+13)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64}-1$ and $6^{72}-1$.

(6.3) Efficiently compute $2^{33} \,\%\, 67$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 35 modulo 47.

(7.3) Find a cube root of 32 mod 149.

(7.4) Find a cube root of 190 modulo 223.

(7.5) Try to find a cube root of 45 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1217?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 13.

(8.5) What does the Miller-Rabin test base 60 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 20701$, and public (encryption) keys $e_A = 23, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 1775$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 7 \bmod 59 \\ x = 13 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 36 modulo 3959. Specifically, find two more in addition to the 'obvious' square roots ± 6.

(9.3) Consider the quadratic polynomial $x^2 - 11x + 30$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 11x + 30 = (x-5)\cdot(x-6)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 11x + 30 = 0 \bmod 391$. In addition to the 'obvious' roots 5, 6 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 87 is a cube root of 105 modulo the prime 367, find a cube root of 105 modulo 367^2.

Unit 10 due Wed Dec 1

(10.1) The integer 216409 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 216409. When you give the oracle $13 \cdot 13$ to take the square root, it returns 123920. Factor 216409.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 799, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 11) \,\%\, 29$ with $s_o = 1$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 4) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 1, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 115

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Haveyourcakeandeatittoo" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 6$.

(1.3) The ciphertext DROBOSCXYLECSXOCCVSUOCRYGLECSXOCC was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}$("*d*") = "*l*" and $E_{a,b}$("*o*") = "*q*". Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 107 times in a row, out of which there were 37 heads and 70 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 5 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 8 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'ZIYQ' and 'YZQI' do *not* have 'Z' adjacent to 'I' and do *not* have 'Y' adjacent to 'Q' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 14 & 9 & 5 & 6 & 2 & 3 & 12 & 4 & 8 & 11 & 1 & 7 & 10 & 13 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 4 & 12 & 8 & 13 & 2 & 1 & 5 & 11 & 3 & 9 & 7 & 14 & 6 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 9 red balls and 9 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 8 red balls and 11 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 11 blue balls, and 19 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2873, 221 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 96983, 111047.

(5.3) Efficiently compute a multiplicative inverse of 349 modulo 1033.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 30 modulo 59.

(7.3) Find a cube root of 140 mod 167.

(7.4) Find a cube root of 220 modulo 241.

(7.5) Try to find a cube root of 46 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 66 is a non-prime Fermat pseudoprime base 31.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 124 say about the primality or not of 1217?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 38.

(8.5) What does the Miller-Rabin test base 61 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16867$, and public (encryption) keys $e_A = 29, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 6869$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 8 \bmod 61 \\ x = 14 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 49 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 7.

(9.3) Consider the quadratic polynomial $x^2 - 13x + 42$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 13x + 42 = (x-6) \cdot (x-7)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 13x + 42 = 0 \bmod 437$. In addition to the 'obvious' roots 6, 7 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 107 is a cube root of 209 modulo the prime 383, find a cube root of 209 modulo 383^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229193 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229193. When you give the oracle $19 \cdot 19$ to take the square root, it returns 60736. Factor 229193.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 15) \,\%\, 31$ with $s_o = 7$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 116

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Meetinthealleyatmidnight" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "bus" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 5$, $b = 7$.

(1.3) The ciphertext MBQZZKEMHQPUEZAFTUZSYGOT was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 12 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}g\text{"}) = \text{"}z\text{"}$ and $E_{a,b}(\text{"}j\text{"}) = \text{"}s\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 109 times in a row, out of which there were 38 heads and 71 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 2 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 7 elements to a set with 10 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'GPFX' and 'FGXP' do *not* have 'G' adjacent to 'P' and do *not* have 'F' adjacent to 'X' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 14 & 5 & 1 & 6 & 12 & 10 & 8 & 4 & 3 & 7 & 13 & 9 & 11 & 2 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 14 & 1 & 12 & 7 & 10 & 2 & 4 & 3 & 6 & 9 & 11 & 5 & 13 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 10 red balls and 11 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 5 red balls and 8 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 5 red balls, 8 blue balls, and 13 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 2299, 209 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 103459, 117581.

(5.3) Efficiently compute a multiplicative inverse of 353 modulo 1039.

(5.4) Systematically find $\gcd(n, n+3, n+23)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21}-1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $3^{39} \,\%\, 79$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 30 modulo 43.

(7.3) Find a cube root of 132 mod 173.

(7.4) Find a cube root of 193 modulo 277.

(7.5) Try to find a cube root of 47 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 69 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 19 say about the primality or not of 1601?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 47.

(8.5) What does the Miller-Rabin test base 62 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 15553$, and public (encryption) keys $e_A = 31, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 9871$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 9 \bmod 47 \\ x = 15 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 64 modulo 4747. Specifically, find two more in addition to the 'obvious' square roots ± 8.

(9.3) Consider the quadratic polynomial $x^2 - 15x + 56$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 15x + 56 = (x - 7) \cdot (x - 8)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 15x + 56 = 0 \bmod 319$. In addition to the 'obvious' roots 7, 8 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 127 is a cube root of 75 modulo the prime 401, find a cube root of 75 modulo 401^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229297 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229297. When you give the oracle $31 \cdot 31$ to take the square root, it returns 94303. Factor 229297.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 731, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (4 \cdot s_n + 16) \,\%\, 31$ with $s_o = 6$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 6) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 0, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 117

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Bringyourownrefreshments" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "kit" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 8$.

(1.3) The ciphertext CXKNXAWXCCXKNCQJCRBCQNRWORWRCREN was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 16 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}j\text{"}) = \text{"}l\text{"}$ and $E_{a,b}(\text{"}o\text{"}) = \text{"}s\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 82 times in a row, out of which there were 39 heads and 43 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 3 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 6-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 8 elements to a set with 12 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'NWME' and 'MNEW' do *not* have 'N' adjacent to 'W' and do *not* have 'M' adjacent to 'E' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 12 & 10 & 11 & 7 & 14 & 3 & 6 & 13 & 8 & 1 & 2 & 4 & 5 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 4 & 5 & 6 & 3 & 10 & 1 & 12 & 13 & 8 & 7 & 14 & 11 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 2 red balls and 4 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 9 red balls and 5 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 9 red balls, 5 blue balls, and 7 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3887, 299 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 89179, 99973.

(5.3) Efficiently compute a multiplicative inverse of 359 modulo 1049.

(5.4) Systematically find $\gcd(n, n+5, n+19)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $2^{41} \,\%\, 83$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 26 modulo 47.

(7.3) Find a cube root of 136 mod 179.

(7.4) Find a cube root of 307 modulo 337.

(7.5) Try to find a cube root of 48 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 45 is a non-prime Fermat pseudoprime base 17.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 42 say about the primality or not of 1601?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 72.

(8.5) What does the Miller-Rabin test base 63 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16799$, and public (encryption) keys $e_A = 37, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 11173$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 10 \bmod 53 \\ x = 16 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 81 modulo 5141. Specifically, find two more in addition to the 'obvious' square roots ± 9.

(9.3) Consider the quadratic polynomial $x^2 - 17x + 72$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 17x + 72 = (x-8) \cdot (x-9)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 17x + 72 = 0 \bmod 299$. In addition to the 'obvious' roots 8, 9 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 147 is a cube root of 78 modulo the prime 421, find a cube root of 78 modulo 421^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229297 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229297. When you give the oracle $21 \cdot 21$ to take the square root, it returns 172811. Factor 229297.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 689, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 13) \,\%\, 31$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 7) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 1, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 118

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Astitchintimesavesnine" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "sue" by an affine cipher $E(x) = (ax + b) \,\%\, 26$ with key $a = 9$, $b = 9$.

(1.3) The ciphertext ZCVBEQKMIANIABBWABIGQVBPMAIUMXTIKM was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(``m") = ``j"$ and $E_{a,b}(``t") = ``m"$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 84 times in a row, out of which there were 40 heads and 44 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 4 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 6-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 9 elements to a set with 14 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'UDTL' and 'TULD' do *not* have 'U' adjacent to 'D' and do *not* have 'T' adjacent to 'L' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 10 & 12 & 14 & 13 & 4 & 2 & 9 & 8 & 11 & 5 & 6 & 1 & 3 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 6 & 14 & 8 & 7 & 2 & 13 & 5 & 4 & 9 & 12 & 3 & 10 & 1 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 3 red balls and 6 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 6 red balls and 13 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 6 red balls, 13 blue balls, and 14 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3509, 319 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 91787, 104411.

(5.3) Efficiently compute a multiplicative inverse of 367 modulo 1051.

(5.4) Systematically find $\gcd(n, n+7, n+31)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48}-1$ and $7^{54}-1$.

(6.3) Efficiently compute $3^{44} \,\%\, 89$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 54 modulo 59.

(7.3) Find a cube root of 133 mod 191.

(7.4) Find a cube root of 311 modulo 349.

(7.5) Try to find a cube root of 49 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 49 is a non-prime Fermat pseudoprime base 18.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 61 say about the primality or not of 1601?

(8.4) Verify that 125 is a non-prime strong pseudoprime base 57.

(8.5) What does the Miller-Rabin test base 64 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17767$, and public (encryption) keys $e_A = 41, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 6401$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 11 \bmod 59 \\ x = 17 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 100 modulo 5251. Specifically, find two more in addition to the 'obvious' square roots ± 10.

(9.3) Consider the quadratic polynomial $x^2 - 19x + 90$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 19x + 90 = (x-9) \cdot (x-10)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 19x + 90 = 0 \bmod 391$. In addition to the 'obvious' roots 9, 10 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 167 is a cube root of 204 modulo the prime 443, find a cube root of 204 modulo 443^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229193 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229193. When you give the oracle $23 \cdot 23$ to take the square root, it returns 10917. Factor 229193.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 611, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000th point of the LCG given by $s_{n+1} = (6 \cdot s_n + 17) \,\%\, 31$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (53 \cdot s_n + 8) \,\%\, 113$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 1, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5th pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0th state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 119

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Honestyisthebestpolicy" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "dog" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 10$.

(1.3) The ciphertext GURENVAVAFCNVASNYYFZNVAYLBAGURCNGVB was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}p\text{”}) = \text{“}t\text{”}$ and $E_{a,b}(\text{“}y\text{”}) = \text{“}a\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 86 times in a row, out of which there were 41 heads and 45 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 5 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 5-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 3 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'BKAS' and 'ABSK' do *not* have 'B' adjacent to 'K' and do *not* have 'A' adjacent to 'S' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 8 & 13 & 14 & 4 & 1 & 11 & 7 & 5 & 9 & 12 & 2 & 3 & 6 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 11 & 8 & 2 & 14 & 9 & 1 & 4 & 6 & 13 & 7 & 5 & 12 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 4 red balls and 8 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 3 red balls and 10 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 3 red balls, 10 blue balls, and 8 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 5239, 403 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 94957, 96571.

(5.3) Efficiently compute a multiplicative inverse of 373 modulo 1061.

(5.4) Systematically find $\gcd(n, n+5, n+17)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64}-1$ and $6^{72}-1$.

(6.3) Efficiently compute $2^{29} \,\%\, 59$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 33 modulo 43.

(7.3) Find a cube root of 173 mod 197.

(7.4) Find a cube root of 119 modulo 193.

(7.5) Try to find a cube root of 50 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 51 is a non-prime Fermat pseudoprime base 35.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1601?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 142.

(8.5) What does the Miller-Rabin test base 65 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 21209$, and public (encryption) keys $e_A = 11, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 3803$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 12 \bmod 61 \\ x = 1 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 121 modulo 3277. Specifically, find two more in addition to the 'obvious' square roots ± 11.

(9.3) Consider the quadratic polynomial $x^2 - 21x + 110$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 21x + 110 = (x - 10) \cdot (x - 11)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 21x + 110 = 0 \bmod 437$. In addition to the 'obvious' roots 10, 11 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 187 is a cube root of 379 modulo the prime 461, find a cube root of 379 modulo 461^2.

Unit 10 due Wed Dec 1

(10.1) The integer 216409 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 216409. When you give the oracle $33 \cdot 33$ to take the square root, it returns 101605. Factor 216409.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 901, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 19) \,\%\, 31$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 2) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 120

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Pennywiseandpoundfoolish" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "cat" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 5$.

(1.3) The ciphertext ESPCLTYTYDALTYQLWWDXLTYWJZYESPRLCLRP was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 19 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}s\text{”}) = \text{“}p\text{”}$ and $E_{a,b}(\text{“}d\text{”}) = \text{“}i\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 88 times in a row, out of which there were 42 heads and 46 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 2 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 4-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 4 elements to a set with 6 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'IRHZ' and 'HIZR' do *not* have 'I' adjacent to 'R' and do *not* have 'H' adjacent to 'Z' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 12 & 6 & 8 & 11 & 13 & 1 & 9 & 5 & 7 & 4 & 2 & 14 & 10 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 3 & 12 & 5 & 2 & 9 & 13 & 11 & 1 & 14 & 6 & 4 & 8 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 5 red balls and 5 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 7 red balls and 7 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 7 red balls, 7 blue balls, and 15 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2057, 187 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 84281, 99457.

(5.3) Efficiently compute a multiplicative inverse of 379 modulo 1009.

(5.4) Systematically find $\gcd(n, n+7, n+11)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21}-1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $2^{30} \,\%\, 61$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 13 modulo 47.

(7.3) Find a cube root of 40 mod 131.

(7.4) Find a cube root of 88 modulo 211.

(7.5) Try to find a cube root of 12 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 55 is a non-prime Fermat pseudoprime base 21.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 11. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 105 say about the primality or not of 1601?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 117.

(8.5) What does the Miller-Rabin test base 66 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 15251$, and public (encryption) keys $e_A = 19, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 1579$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 13 \bmod 47 \\ x = 2 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 144 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 12.

(9.3) Consider the quadratic polynomial $x^2 - 12x + 11$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 12x + 11 = (x-1) \cdot (x-11)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 12x + 11 = 0 \bmod 319$. In addition to the 'obvious' roots 1, 11 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 207 is a cube root of 12 modulo the prime 487, find a cube root of 12 modulo 487^2.

Unit 10 due Wed Dec 1

(10.1) The integer 204889 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 204889. When you give the oracle $43 \cdot 43$ to take the square root, it returns 203608. Factor 204889.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 779, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (8 \cdot s_n + 23) \,\%\, 31$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 121

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Awinkisasgoodasanod" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "fox" by an affine cipher $E(x) = (ax + b) \,\%\, 26$ with key $a = 5$, $b = 6$.

(1.3) The ciphertext YEDYPDROPBISXQZKXSXDYDROMVYCOD was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 11 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}o\text{"}) = \text{"}x\text{"}$ and $E_{a,b}(\text{"}f\text{"}) = \text{"}w\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 90 times in a row, out of which there were 43 heads and 47 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 3 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 7-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 5 elements to a set with 8 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'PYOG' and 'OPGY' do *not* have 'P' adjacent to 'Y' and do *not* have 'O' adjacent to 'G' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 4 & 12 & 13 & 1 & 11 & 3 & 2 & 9 & 14 & 7 & 8 & 6 & 10 & 5 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 14 & 12 & 10 & 13 & 4 & 8 & 9 & 5 & 1 & 2 & 3 & 7 & 6 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 6 red balls and 7 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 4 red balls and 4 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 4 red balls, 4 blue balls, and 9 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3211, 247 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 86701, 103321.

(5.3) Efficiently compute a multiplicative inverse of 313 modulo 1013.

(5.4) Systematically find $\gcd(n, n+11, n+13)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $2^{33} \,\%\, 67$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 55 modulo 59.

(7.3) Find a cube root of 55 mod 137.

(7.4) Find a cube root of 2 modulo 223.

(7.5) Try to find a cube root of 12 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 57 is a non-prime Fermat pseudoprime base 20.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 46 say about the primality or not of 1409?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 68.

(8.5) What does the Miller-Rabin test base 67 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16171$, and public (encryption) keys $e_A = 23, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 4151$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 3 \bmod 53 \\ x = 4 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 4 modulo 3959. Specifically, find two more in addition to the 'obvious' square roots ± 2.

(9.3) Consider the quadratic polynomial $x^2 - 3x + 2$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 3x + 2 = (x - 2) \cdot (x - 1)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 3x + 2 = 0 \bmod 299$. In addition to the 'obvious' roots 2, 1 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 7 is a cube root of 62 modulo the prime 281, find a cube root of 62 modulo 281^2.

Unit 10 due Wed Dec 1

(10.1) The integer 202313 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 202313. When you give the oracle $41 \cdot 41$ to take the square root, it returns 198977. Factor 202313.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 799, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 11)\,\%\,29$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 4)\,\%\,103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 1, 1, 1, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 122

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Burnthecandleatbothends" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 7$.

(1.3) The ciphertext FTQDQUEZANGEUZQEEXUWQETAINGEUZQEE was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 13 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(``r") = ``p"$ and $E_{a,b}(``k") = ``g"$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 92 times in a row, out of which there were 44 heads and 48 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 4 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 10 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'WFVN' and 'VWNF' do *not* have 'W' adjacent to 'F' and do *not* have 'V' adjacent to 'N' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 13 & 6 & 14 & 9 & 1 & 10 & 11 & 2 & 7 & 4 & 8 & 3 & 12 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 4 & 9 & 5 & 11 & 1 & 3 & 2 & 14 & 13 & 6 & 7 & 10 & 12 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 7 red balls and 9 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 8 red balls and 12 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 12 blue balls, and 16 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 2783, 253 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 89077, 106499.

(5.3) Efficiently compute a multiplicative inverse of 317 modulo 1019.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 29 modulo 43.

(7.3) Find a cube root of 110 mod 149.

(7.4) Find a cube root of 26 modulo 241.

(7.5) Try to find a cube root of 13 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 14.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 49 say about the primality or not of 1409?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 43.

(8.5) What does the Miller-Rabin test base 68 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17441$, and public (encryption) keys $e_A = 29, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 4145$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 4 \bmod 59 \\ x = 5 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 9 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 3.

(9.3) Consider the quadratic polynomial $x^2 - 5x + 6$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 5x + 6 = (x-3) \cdot (x-2)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 5x + 6 = 0 \bmod 391$. In addition to the 'obvious' roots 3, 2 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 27 is a cube root of 35 modulo the prime 307, find a cube root of 35 modulo 307^2.

Unit 10 due Wed Dec 1

(10.1) The integer 173441 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 173441. When you give the oracle $31 \cdot 31$ to take the square root, it returns 172719. Factor 173441.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (4 \cdot s_n + 13) \,\%\, 29$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 123

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Haveyourcakeandeatittoo" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "bus" by an affine cipher $E(x) = (ax + b) \,\%\, 26$ with key $a = 9$, $b = 8$.

(1.3) The ciphertext JYNWWHBJENMRBWXCQRWPVDLQ was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}u\text{"}) = \text{"}t\text{"}$ and $E_{a,b}(\text{"}p\text{"}) = \text{"}k\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 94 times in a row, out of which there were 45 heads and 49 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 5 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 7 elements to a set with 12 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'DMCU' and 'CDUM' do *not* have 'D' adjacent to 'M' and do *not* have 'C' adjacent to 'U' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 12 & 6 & 3 & 2 & 14 & 5 & 13 & 11 & 4 & 10 & 1 & 8 & 9 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 11 & 5 & 12 & 10 & 13 & 8 & 6 & 3 & 1 & 2 & 14 & 4 & 7 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 8 red balls and 11 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 5 red balls and 9 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 5 red balls, 9 blue balls, and 10 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 4901, 377 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 93673, 108389.

(5.3) Efficiently compute a multiplicative inverse of 331 modulo 1021.

(5.4) Systematically find $\gcd(n, n+3, n+23)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48}-1$ and $7^{54}-1$.

(6.3) Efficiently compute $3^{39} \,\%\, 79$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 43 modulo 47.

(7.3) Find a cube root of 15 mod 167.

(7.4) Find a cube root of 74 modulo 277.

(7.5) Try to find a cube root of 14 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 115 say about the primality or not of 1409?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 150.

(8.5) What does the Miller-Rabin test base 69 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 18203$, and public (encryption) keys $e_A = 31, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 1735$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 5 \bmod 61 \\ x = 6 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 16 modulo 4747. Specifically, find two more in addition to the 'obvious' square roots ± 4.

(9.3) Consider the quadratic polynomial $x^2 - 7x + 12$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 7x + 12 = (x-4) \cdot (x-3)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 7x + 12 = 0 \bmod 437$. In addition to the 'obvious' roots 4, 3 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 47 is a cube root of 220 modulo the prime 331, find a cube root of 220 modulo 331^2.

Unit 10 due Wed Dec 1

(10.1) The integer 155929 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 155929. When you give the oracle $47 \cdot 47$ to take the square root, it returns 138885. Factor 155929.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 731, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 15) \,\%\, 29$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 6) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 124

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Meetinthealleyatmidnight" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "kit" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 9$.

(1.3) The ciphertext BWJMWZVWBBWJMBPIBQABPMQVNQVQBQDM was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}x\text{”}) = \text{“}j\text{”}$ and $E_{a,b}(\text{“}u\text{”}) = \text{“}i\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 96 times in a row, out of which there were 46 heads and 50 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 2 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 6-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 8 elements to a set with 14 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'KTJB' and 'JKBT' do *not* have 'K' adjacent to 'T' and do *not* have 'J' adjacent to 'B' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 6 & 8 & 12 & 1 & 11 & 2 & 7 & 4 & 14 & 13 & 5 & 3 & 10 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 4 & 12 & 10 & 9 & 14 & 6 & 13 & 7 & 8 & 1 & 3 & 11 & 5 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 9 red balls and 13 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 9 red balls and 6 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 9 red balls, 6 blue balls, and 17 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3751, 341 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 98741, 113977.

(5.3) Efficiently compute a multiplicative inverse of 337 modulo 1031.

(5.4) Systematically find $\gcd(n, n+5, n+19)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21} - 1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64} - 1$ and $6^{72} - 1$.

(6.3) Efficiently compute $2^{41} \% 83$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 33 modulo 59.

(7.3) Find a cube root of 162 mod 173.

(7.4) Find a cube root of 17 modulo 337.

(7.5) Try to find a cube root of 15 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 66 is a non-prime Fermat pseudoprime base 31.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 76 say about the primality or not of 1217?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 99.

(8.5) What does the Miller-Rabin test base 70 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 19177$, and public (encryption) keys $e_A = 37, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 8173$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 6 \bmod 47 \\ x = 7 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 25 modulo 5141. Specifically, find two more in addition to the 'obvious' square roots ± 5.

(9.3) Consider the quadratic polynomial $x^2 - 9x + 20$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 9x + 20 = (x - 5) \cdot (x - 4)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 9x + 20 = 0 \bmod 319$. In addition to the 'obvious' roots 5, 4 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 67 is a cube root of 261 modulo the prime 347, find a cube root of 261 modulo 347^2.

Unit 10 due Wed Dec 1

(10.1) The integer 140873 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 140873. When you give the oracle $43 \cdot 43$ to take the square root, it returns 121942. Factor 140873.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 689, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (6 \cdot s_n + 12) \,\%\, 29$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 7) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 125

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Bringyourownrefreshments" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "sue" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 10$.

(1.3) The ciphertext EHAGJVPRNFSNFGGBFGNLVAGURFNZRCYNPR was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{``}a\text{''}) = \text{``}l\text{''}$ and $E_{a,b}(\text{``}l\text{''}) = \text{``}c\text{''}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 98 times in a row, out of which there were 47 heads and 51 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 3 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 6-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 9 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'RAQI' and 'QRIA' do *not* have 'R' adjacent to 'A' and do *not* have 'Q' adjacent to 'I' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 8 & 7 & 12 & 2 & 11 & 6 & 1 & 5 & 13 & 14 & 4 & 9 & 3 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 6 & 14 & 13 & 12 & 1 & 2 & 9 & 4 & 8 & 7 & 5 & 3 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 10 red balls and 10 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 6 red balls and 14 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 6 red balls, 14 blue balls, and 11 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2873, 221 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n \to +\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 106529, 121879.

(5.3) Efficiently compute a multiplicative inverse of 347 modulo 1033.

(5.4) Systematically find $\gcd(n, n+7, n+31)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24} - 1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121} - 1$ and $3^{99} - 1$.

(6.3) Efficiently compute $3^{44} \,\%\, 89$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 18 modulo 43.

(7.3) Find a cube root of 154 mod 179.

(7.4) Find a cube root of 167 modulo 349.

(7.5) Try to find a cube root of 16 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 69 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1217?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 89.

(8.5) What does the Miller-Rabin test base 71 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 15857$, and public (encryption) keys $e_A = 41, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 761$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 7 \bmod 53 \\ x = 8 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 36 modulo 5251. Specifically, find two more in addition to the 'obvious' square roots ± 6.

(9.3) Consider the quadratic polynomial $x^2 - 11x + 30$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 11x + 30 = (x-6) \cdot (x-5)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 11x + 30 = 0 \bmod 299$. In addition to the 'obvious' roots 6, 5 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 87 is a cube root of 105 modulo the prime 367, find a cube root of 105 modulo 367^2.

Unit 10 due Wed Dec 1

(10.1) The integer 106241 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 106241. When you give the oracle $61 \cdot 61$ to take the square root, it returns 59142. Factor 106241.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 611, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 11) \,\%\, 29$ with $s_o = 1$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (53 \cdot s_n + 8) \,\%\, 113$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0,1,0,1,0,1,0,1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0,0,0,0,0,1,0,1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Garrett ©2004

Crypto Homework version 126

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Astitchintimesavesnine" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "dog" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 5$, $b = 5$.

(1.3) The ciphertext ESPCLTYTYDALTYQLWWDXLTYWJZYESPALETZ was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}d\text{"}) = \text{"}l\text{"}$ and $E_{a,b}(\text{"}o\text{"}) = \text{"}q\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 79 times in a row, out of which there were 27 heads and 52 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 4 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 5-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 3 elements to a set with 6 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'YHXP' and 'XYPH' do *not* have 'Y' adjacent to 'H' and do *not* have 'X' adjacent to 'P' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 1 & 7 & 3 & 8 & 5 & 13 & 4 & 10 & 12 & 14 & 2 & 6 & 11 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 14 & 6 & 11 & 12 & 1 & 8 & 3 & 10 & 7 & 2 & 5 & 4 & 13 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 2 red balls and 3 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 3 red balls and 11 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 3 red balls, 11 blue balls, and 18 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 2299, 209 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 89693, 92263.

(5.3) Efficiently compute a multiplicative inverse of 349 modulo 1039.

(5.4) Systematically find $\gcd(n, n+5, n+17)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $2^{29} \,\%\, 59$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 22 modulo 47.

(7.3) Find a cube root of 127 mod 191.

(7.4) Find a cube root of 122 modulo 193.

(7.5) Try to find a cube root of 17 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 45 is a non-prime Fermat pseudoprime base 17.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 124 say about the primality or not of 1217?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 80.

(8.5) What does the Miller-Rabin test base 73 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16789$, and public (encryption) keys $e_A = 11, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 7511$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 8 \bmod 59 \\ x = 9 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 49 modulo 3277. Specifically, find two more in addition to the 'obvious' square roots ± 7.

(9.3) Consider the quadratic polynomial $x^2 - 13x + 42$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 13x + 42 = (x-7)\cdot(x-6)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 13x + 42 = 0 \bmod 391$. In addition to the 'obvious' roots 7, 6 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 107 is a cube root of 209 modulo the prime 383, find a cube root of 209 modulo 383^2.

Unit 10 due Wed Dec 1

(10.1) The integer 106241 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 106241. When you give the oracle $19 \cdot 19$ to take the square root, it returns 96528. Factor 106241.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 901, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 15) \,\%\, 31$ with $s_o = 7$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 2) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 127

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Honestyisthebestpolicy" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "cat" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 6$.

(1.3) The ciphertext DROBKSXSXCZKSXPKVVCWKSXVIYXDROQKBKQO was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 12 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}g\text{”}) = \text{“}z\text{”}$ and $E_{a,b}(\text{“}j\text{”}) = \text{“}s\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 81 times in a row, out of which there were 28 heads and 53 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 5 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 4-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 4 elements to a set with 8 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'FOEW' and 'EFWO' do *not* have 'F' adjacent to 'O' and do *not* have 'E' adjacent to 'W' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 6 & 12 & 5 & 3 & 11 & 4 & 13 & 1 & 14 & 9 & 8 & 7 & 10 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 10 & 2 & 6 & 9 & 5 & 12 & 14 & 13 & 7 & 1 & 3 & 8 & 4 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 3 red balls and 5 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 7 red balls and 8 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 7 red balls, 8 blue balls, and 12 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3887, 299 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 92839, 96521.

(5.3) Efficiently compute a multiplicative inverse of 353 modulo 1049.

(5.4) Systematically find $\gcd(n, n+7, n+11)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $2^{30} \,\%\, 61$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 47 modulo 59.

(7.3) Find a cube root of 155 mod 197.

(7.4) Find a cube root of 104 modulo 211.

(7.5) Try to find a cube root of 18 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 49 is a non-prime Fermat pseudoprime base 18.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 19 say about the primality or not of 1601?

(8.4) Verify that 265 is a non-prime strong pseudoprime base 23.

(8.5) What does the Miller-Rabin test base 73 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17869$, and public (encryption) keys $e_A = 19, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 8335$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 9 \bmod 61 \\ x = 10 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 64 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 8.

(9.3) Consider the quadratic polynomial $x^2 - 15x + 56$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 15x + 56 = (x - 8) \cdot (x - 7)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 15x + 56 = 0 \bmod 437$. In addition to the 'obvious' roots 8, 7 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 127 is a cube root of 75 modulo the prime 401, find a cube root of 75 modulo 401^2.

Unit 10 due Wed Dec 1

(10.1) The integer 140873 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 140873. When you give the oracle $7 \cdot 7$ to take the square root, it returns 65328. Factor 140873.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 779, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (4 \cdot s_n + 16) \,\%\, 31$ with $s_o = 6$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 0, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 128

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Pennywiseandpoundfoolish" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "fox" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 9$, $b = 7$.

(1.3) The ciphertext AGFARFTQRDKUZSBMZUZFAFTQOXAEQF was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 16 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}j\text{”}) = \text{“}l\text{”}$ and $E_{a,b}(\text{“}o\text{”}) = \text{“}s\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 83 times in a row, out of which there were 29 heads and 54 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 2 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 7-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 5 elements to a set with 10 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'MVLD' and 'LMDV' do *not* have 'M' adjacent to 'V' and do *not* have 'L' adjacent to 'D' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 9 & 13 & 14 & 7 & 3 & 5 & 6 & 8 & 4 & 10 & 2 & 12 & 1 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 4 & 8 & 5 & 9 & 12 & 13 & 3 & 6 & 2 & 7 & 10 & 14 & 1 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 4 red balls and 7 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 4 red balls and 5 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 4 red balls, 5 blue balls, and 19 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3509, 319 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n \to +\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 83659, 100337.

(5.3) Efficiently compute a multiplicative inverse of 359 modulo 1051.

(5.4) Systematically find $\gcd(n, n+11, n+13)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21} - 1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48} - 1$ and $7^{54} - 1$.

(6.3) Efficiently compute $2^{33} \,\%\, 67$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 27 modulo 43.

(7.3) Find a cube root of 23 mod 131.

(7.4) Find a cube root of 182 modulo 223.

(7.5) Try to find a cube root of 19 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 51 is a non-prime Fermat pseudoprime base 35.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 42 say about the primality or not of 1601?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 133.

(8.5) What does the Miller-Rabin test base 74 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16459$, and public (encryption) keys $e_A = 23, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 14087$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 10 \bmod 47 \\ x = 11 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 81 modulo 3959. Specifically, find two more in addition to the 'obvious' square roots ± 9.

(9.3) Consider the quadratic polynomial $x^2 - 17x + 72$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 17x + 72 = (x - 9) \cdot (x - 8)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 17x + 72 = 0 \bmod 319$. In addition to the 'obvious' roots 9, 8 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 147 is a cube root of 78 modulo the prime 421, find a cube root of 78 modulo 421^2.

Unit 10 due Wed Dec 1

(10.1) The integer 155929 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 155929. When you give the oracle $17 \cdot 17$ to take the square root, it returns 105694. Factor 155929.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 799, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000th point of the LCG given by $s_{n+1} = (5 \cdot s_n + 13) \% 31$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 4) \% 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 1, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 129

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Awinkisasgoodasanod" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 8$.

(1.3) The ciphertext CQNANRBWXKDBRWNBBURTNBQXFKDBRWNBB was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}$("m") = "j" and $E_{a,b}$("t") = "m". Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 85 times in a row, out of which there were 30 heads and 55 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 3 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 12 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'TCSK' and 'STKC' do *not* have 'T' adjacent to 'C' and do *not* have 'S' adjacent to 'K' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 1 & 5 & 9 & 12 & 13 & 6 & 2 & 3 & 8 & 14 & 4 & 10 & 11 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 4 & 1 & 14 & 12 & 13 & 2 & 11 & 10 & 3 & 7 & 9 & 6 & 5 & 8 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 5 red balls and 9 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 8 red balls and 13 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 13 blue balls, and 13 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 5239, 403 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 84823, 102709.

(5.3) Efficiently compute a multiplicative inverse of 367 modulo 1061.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64}-1$ and $6^{72}-1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 44 modulo 47.

(7.3) Find a cube root of 20 mod 137.

(7.4) Find a cube root of 115 modulo 241.

(7.5) Try to find a cube root of 21 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 55 is a non-prime Fermat pseudoprime base 21.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 61 say about the primality or not of 1601?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 12.

(8.5) What does the Miller-Rabin test base 75 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 19939$, and public (encryption) keys $e_A = 29, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 3389$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 11 \bmod 53 \\ x = 12 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 100 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 10.

(9.3) Consider the quadratic polynomial $x^2 - 19x + 90$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 19x + 90 = (x - 10) \cdot (x - 9)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 19x + 90 = 0 \bmod 299$. In addition to the 'obvious' roots 10, 9 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 167 is a cube root of 204 modulo the prime 443, find a cube root of 204 modulo 443^2.

Unit 10 due Wed Dec 1

(10.1) The integer 173441 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 173441. When you give the oracle $29 \cdot 29$ to take the square root, it returns 62219. Factor 173441.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (6 \cdot s_n + 17) \,\%\, 31$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 1, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 130

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Burnthecandleatbothends" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "bus" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 9$.

(1.3) The ciphertext IXMVVGAIDMLQAVWBPQVOUCKP was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}p\text{”}) = \text{“}t\text{”}$ and $E_{a,b}(\text{“}y\text{”}) = \text{“}a\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 87 times in a row, out of which there were 31 heads and 56 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 4 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 7 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'AJZR' and 'ZARJ' do *not* have 'A' adjacent to 'J' and do *not* have 'Z' adjacent to 'R' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 4 & 6 & 11 & 1 & 13 & 8 & 2 & 10 & 12 & 9 & 5 & 7 & 14 & 3 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 3 & 1 & 13 & 6 & 5 & 10 & 9 & 12 & 2 & 8 & 4 & 14 & 11 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 6 red balls and 6 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 5 red balls and 10 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 5 red balls, 10 blue balls, and 7 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2057, 187 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 87809, 106091.

(5.3) Efficiently compute a multiplicative inverse of 373 modulo 1009.

(5.4) Systematically find $\gcd(n, n+3, n+23)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $3^{39} \,\%\, 79$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 38 modulo 59.

(7.3) Find a cube root of 39 mod 149.

(7.4) Find a cube root of 37 modulo 277.

(7.5) Try to find a cube root of 21 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 57 is a non-prime Fermat pseudoprime base 20.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 11. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1601?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 17.

(8.5) What does the Miller-Rabin test base 11 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16463$, and public (encryption) keys $e_A = 31, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 6271$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 12 \bmod 59 \\ x = 13 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 121 modulo 4747. Specifically, find two more in addition to the 'obvious' square roots ± 11.

(9.3) Consider the quadratic polynomial $x^2 - 11x + 10$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 11x + 10 = (x-1) \cdot (x-10)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 11x + 10 = 0 \bmod 391$. In addition to the 'obvious' roots 1, 10 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 187 is a cube root of 379 modulo the prime 461, find a cube root of 379 modulo 461^2.

Unit 10 due Wed Dec 1

(10.1) The integer 202313 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 202313. When you give the oracle $13 \cdot 13$ to take the square root, it returns 35599. Factor 202313.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 731, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 19) \,\%\, 31$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 6) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 131

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Haveyourcakeandeatittoo" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "kit" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 5$, $b = 10$.

(1.3) The ciphertext GBORBEABGGBORGUNGVFGURVASVAVGVIR was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 19 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}s\text{"}) = \text{"}p\text{"}$ and $E_{a,b}(\text{"}d\text{"}) = \text{"}i\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 89 times in a row, out of which there were 32 heads and 57 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 5 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 6-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 8 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'HQGY' and 'GHYQ' do *not* have 'H' adjacent to 'Q' and do *not* have 'G' adjacent to 'Y' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 6 & 3 & 9 & 7 & 1 & 11 & 4 & 2 & 13 & 12 & 14 & 5 & 8 & 10 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 13 & 5 & 11 & 10 & 1 & 8 & 7 & 3 & 12 & 14 & 9 & 4 & 6 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 7 red balls and 8 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 9 red balls and 7 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 9 red balls, 7 blue balls, and 14 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3211, 247 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 93011, 109309.

(5.3) Efficiently compute a multiplicative inverse of 379 modulo 1013.

(5.4) Systematically find $\gcd(n, n+5, n+19)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $2^{41} \,\%\, 83$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 5 modulo 43.

(7.3) Find a cube root of 57 mod 167.

(7.4) Find a cube root of 56 modulo 337.

(7.5) Try to find a cube root of 22 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 14.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 105 say about the primality or not of 1601?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 13.

(8.5) What does the Miller-Rabin test base 12 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17201$, and public (encryption) keys $e_A = 37, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 3661$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 13 \bmod 61 \\ x = 14 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 144 modulo 5141. Specifically, find two more in addition to the 'obvious' square roots ± 12.

(9.3) Consider the quadratic polynomial $x^2 - 13x + 22$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 13x + 22 = (x-2)\cdot(x-11)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 13x + 22 = 0 \bmod 437$. In addition to the 'obvious' roots 2, 11 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 207 is a cube root of 12 modulo the prime 487, find a cube root of 12 modulo 487^2.

Unit 10 due Wed Dec 1

(10.1) The integer 204889 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 204889. When you give the oracle $23 \cdot 23$ to take the square root, it returns 143631. Factor 204889.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 689, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (8 \cdot s_n + 23) \,\%\, 31$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 7) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0$^{\text{th}}$ state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 132

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Meetinthealleyatmidnight" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "sue" by an affine cipher $E(x) = (ax + b)\,\%\,26$ with key $a = 7$, $b = 5$.

(1.3) The ciphertext CFYEHTNPLDQLDEEZDELJTYESPDLXPAWLNP was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 11 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}o\text{”}) = \text{“}x\text{”}$ and $E_{a,b}(\text{“}f\text{”}) = \text{“}w\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 91 times in a row, out of which there were 33 heads and 58 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 2 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 6-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 9 elements to a set with 13 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'OXNF' and 'NOFX' do *not* have 'O' adjacent to 'X' and do *not* have 'N' adjacent to 'F' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 4 & 5 & 9 & 10 & 13 & 12 & 1 & 8 & 7 & 14 & 3 & 6 & 2 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 10 & 11 & 5 & 9 & 14 & 3 & 4 & 6 & 7 & 2 & 13 & 12 & 1 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 8 red balls and 10 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 6 red balls and 4 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 6 red balls, 4 blue balls, and 8 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 2783, 253 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 95371, 112351.

(5.3) Efficiently compute a multiplicative inverse of 313 modulo 1019.

(5.4) Systematically find $\gcd(n, n+7, n+31)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21}-1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $3^{44} \,\%\, 89$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 15 modulo 47.

(7.3) Find a cube root of 19 mod 173.

(7.4) Find a cube root of 251 modulo 349.

(7.5) Try to find a cube root of 25 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 46 say about the primality or not of 1409?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 38.

(8.5) What does the Miller-Rabin test base 14 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16157$, and public (encryption) keys $e_A = 41, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 13961$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 3 \bmod 47 \\ x = 14 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 4 modulo 5251. Specifically, find two more in addition to the 'obvious' square roots ± 2.

(9.3) Consider the quadratic polynomial $x^2 - 4x + 3$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 4x + 3 = (x - 3) \cdot (x - 1)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 4x + 3 = 0 \bmod 319$. In addition to the 'obvious' roots 3, 1 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 7 is a cube root of 62 modulo the prime 281, find a cube root of 62 modulo 281^2.

Unit 10 due Wed Dec 1

(10.1) The integer 216409 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 216409. When you give the oracle $13 \cdot 13$ to take the square root, it returns 123920. Factor 216409.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 611, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 11) \,\%\, 29$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (53 \cdot s_n + 8) \,\%\, 113$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 1, 1, 1, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 133

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Bringyourownrefreshments" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "dog" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 9$, $b = 6$.

(1.3) The ciphertext DROBKSXSXCZKSXPKVVCWKSXVIYXDROZKDSY was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 13 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}r\text{”}) = \text{“}p\text{”}$ and $E_{a,b}(\text{“}k\text{”}) = \text{“}g\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 93 times in a row, out of which there were 34 heads and 59 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 3 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 5-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 3 elements to a set with 8 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'VEUM' and 'UVME' do *not* have 'V' adjacent to 'E' and do *not* have 'U' adjacent to 'M' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 13 & 11 & 2 & 14 & 10 & 1 & 6 & 4 & 7 & 8 & 9 & 12 & 5 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 11 & 7 & 13 & 6 & 5 & 4 & 9 & 12 & 1 & 3 & 10 & 14 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 9 red balls and 12 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 3 red balls and 12 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 3 red balls, 12 blue balls, and 15 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 4901, 377 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 101671, 105187.

(5.3) Efficiently compute a multiplicative inverse of 317 modulo 1021.

(5.4) Systematically find $\gcd(n, n+5, n+17)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48}-1$ and $7^{54}-1$.

(6.3) Efficiently compute $2^{29} \,\%\, 59$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 6 modulo 59.

(7.3) Find a cube root of 172 mod 179.

(7.4) Find a cube root of 164 modulo 193.

(7.5) Try to find a cube root of 25 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 66 is a non-prime Fermat pseudoprime base 31.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 49 say about the primality or not of 1409?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 47.

(8.5) What does the Miller-Rabin test base 14 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17113$, and public (encryption) keys $e_A = 11, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 4595$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 4 \bmod 53 \\ x = 15 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 9 modulo 3277. Specifically, find two more in addition to the 'obvious' square roots ± 3.

(9.3) Consider the quadratic polynomial $x^2 - 6x + 8$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 6x + 8 = (x - 4) \cdot (x - 2)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 6x + 8 = 0 \bmod 299$. In addition to the 'obvious' roots 4, 2 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 27 is a cube root of 35 modulo the prime 307, find a cube root of 35 modulo 307^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229193 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229193. When you give the oracle $19 \cdot 19$ to take the square root, it returns 60736. Factor 229193.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 901, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (4 \cdot s_n + 13) \,\%\, 29$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 2) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0$^{\text{th}}$ state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 134

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Astitchintimesavesnine" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "cat" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 7$.

(1.3) The ciphertext FTQDMUZUZEBMUZRMXXEYMUZXKAZFTQSMDMSQ was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}u\text{”}) = \text{“}t\text{”}$ and $E_{a,b}(\text{“}p\text{”}) = \text{“}k\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 95 times in a row, out of which there were 35 heads and 60 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 4 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 4-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 4 elements to a set with 10 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'CLBT' and 'BCTL' do *not* have 'C' adjacent to 'L' and do *not* have 'B' adjacent to 'T' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 4 & 6 & 10 & 9 & 3 & 5 & 12 & 13 & 8 & 11 & 14 & 7 & 1 & 2 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 12 & 7 & 11 & 14 & 2 & 13 & 10 & 6 & 5 & 1 & 8 & 9 & 3 & 4 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 10 red balls and 14 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 7 red balls and 9 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 7 red balls, 9 blue balls, and 9 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3751, 341 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n \to +\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 107143, 112669.

(5.3) Efficiently compute a multiplicative inverse of 331 modulo 1031.

(5.4) Systematically find $\gcd(n, n+7, n+11)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64}-1$ and $6^{72}-1$.

(6.3) Efficiently compute $2^{30} \,\%\, 61$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 19 modulo 43.

(7.3) Find a cube root of 121 mod 191.

(7.4) Find a cube root of 143 modulo 211.

(7.5) Try to find a cube root of 25 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 69 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 115 say about the primality or not of 1409?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 72.

(8.5) What does the Miller-Rabin test base 15 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 20701$, and public (encryption) keys $e_A = 19, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 3223$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 5 \bmod 59 \\ x = 16 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 16 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 4.

(9.3) Consider the quadratic polynomial $x^2 - 8x + 15$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 8x + 15 = (x-5) \cdot (x-3)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 8x + 15 = 0 \bmod 391$. In addition to the 'obvious' roots 5, 3 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 47 is a cube root of 220 modulo the prime 331, find a cube root of 220 modulo 331^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229297 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229297. When you give the oracle $31 \cdot 31$ to take the square root, it returns 94303. Factor 229297.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 779, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (5 \cdot s_n + 15) \,\%\, 29$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0$^{\text{th}}$ state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 135

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Honestyisthebestpolicy" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "fox" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 8$.

(1.3) The ciphertext XDCXOCQNOAHRWPYJWRWCXCQNLUXBNC was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}x\text{"}) = \text{"}j\text{"}$ and $E_{a,b}(\text{"}u\text{"}) = \text{"}i\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 97 times in a row, out of which there were 36 heads and 61 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 5 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 7-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 5 elements to a set with 7 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'JSIA' and 'IJAS' do *not* have 'J' adjacent to 'S' and do *not* have 'I' adjacent to 'A' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 4 & 13 & 2 & 7 & 5 & 9 & 12 & 11 & 14 & 6 & 10 & 8 & 1 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 10 & 5 & 14 & 8 & 13 & 11 & 9 & 1 & 7 & 4 & 2 & 6 & 12 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 2 red balls and 2 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 4 red balls and 6 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 4 red balls, 6 blue balls, and 16 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2873, 221 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 90721, 95861.

(5.3) Efficiently compute a multiplicative inverse of 337 modulo 1033.

(5.4) Systematically find $\gcd(n, n+11, n+13)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $2^{33} \,\%\, 67$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 29 modulo 47.

(7.3) Find a cube root of 137 mod 197.

(7.4) Find a cube root of 112 modulo 223.

(7.5) Try to find a cube root of 26 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 45 is a non-prime Fermat pseudoprime base 17.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 11. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 76 say about the primality or not of 1217?

(8.4) Verify that 125 is a non-prime strong pseudoprime base 57.

(8.5) What does the Miller-Rabin test base 17 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16867$, and public (encryption) keys $e_A = 23, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 2887$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 6 \bmod 61 \\ x = 17 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 25 modulo 3959. Specifically, find two more in addition to the 'obvious' square roots ± 5.

(9.3) Consider the quadratic polynomial $x^2 - 10x + 24$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 10x + 24 = (x-6) \cdot (x-4)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 10x + 24 = 0 \bmod 437$. In addition to the 'obvious' roots 6, 4 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 67 is a cube root of 261 modulo the prime 347, find a cube root of 261 modulo 347^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229297 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229297. When you give the oracle $21 \cdot 21$ to take the square root, it returns 172811. Factor 229297.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 799, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (6 \cdot s_n + 12) \,\%\, 29$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 4) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 136

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Pennywiseandpoundfoolish" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \,\%\, 26$ with key $a = 5$, $b = 9$.

(1.3) The ciphertext BPMZMQAVWJCAQVMAATQSMAPWEJCAQVMAA was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}a\text{”}) = \text{“}l\text{”}$ and $E_{a,b}(\text{“}l\text{”}) = \text{“}c\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 99 times in a row, out of which there were 37 heads and 62 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 2 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'QZPH' and 'PQHZ' do *not* have 'Q' adjacent to 'Z' and do *not* have 'P' adjacent to 'H' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 10 & 9 & 8 & 1 & 13 & 11 & 2 & 6 & 12 & 4 & 7 & 14 & 3 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 14 & 12 & 3 & 8 & 13 & 1 & 10 & 7 & 11 & 9 & 6 & 4 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 3 red balls and 4 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 8 red balls and 14 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 14 blue balls, and 10 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 2299, 209 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 81793, 99677.

(5.3) Efficiently compute a multiplicative inverse of 347 modulo 1039.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21}-1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 10 modulo 59.

(7.3) Find a cube root of 6 mod 131.

(7.4) Find a cube root of 135 modulo 241.

(7.5) Try to find a cube root of 29 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 49 is a non-prime Fermat pseudoprime base 18.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1217?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 142.

(8.5) What does the Miller-Rabin test base 17 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 15553$, and public (encryption) keys $e_A = 29, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 8969$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 7 \bmod 47 \\ x = 1 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 36 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 6.

(9.3) Consider the quadratic polynomial $x^2 - 12x + 35$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 12x + 35 = (x-7)\cdot(x-5)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 12x + 35 = 0 \bmod 319$. In addition to the 'obvious' roots 7, 5 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 87 is a cube root of 105 modulo the prime 367, find a cube root of 105 modulo 367^2.

Unit 10 due Wed Dec 1

(10.1) The integer 229193 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 229193. When you give the oracle $23 \cdot 23$ to take the square root, it returns 10917. Factor 229193.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 11) \,\%\, 29$ with $s_o = 1$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 1, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 137

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Awinkisasgoodasanod" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "bus" by an affine cipher $E(x) = (ax + b) \,\%\, 26$ with key $a = 7$, $b = 10$.

(1.3) The ciphertext NCRAALFNIRQVFABGUVATZHPU was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}d\text{"}) = \text{"}l\text{"}$ and $E_{a,b}(\text{"}o\text{"}) = \text{"}q\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 101 times in a row, out of which there were 38 heads and 63 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 3 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 7 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'XGWO' and 'WXOG' do *not* have 'X' adjacent to 'G' and do *not* have 'W' adjacent to 'O' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 1 & 4 & 5 & 14 & 2 & 13 & 10 & 6 & 11 & 9 & 3 & 7 & 12 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 13 & 8 & 2 & 3 & 7 & 5 & 11 & 1 & 4 & 14 & 12 & 6 & 9 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 4 red balls and 6 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 5 red balls and 11 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 5 red balls, 11 blue balls, and 17 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3887, 299 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 84197, 103027.

(5.3) Efficiently compute a multiplicative inverse of 349 modulo 1049.

(5.4) Systematically find $\gcd(n, n+3, n+23)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $3^{39} \,\%\, 79$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 26 modulo 43.

(7.3) Find a cube root of 122 mod 137.

(7.4) Find a cube root of 201 modulo 277.

(7.5) Try to find a cube root of 29 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 51 is a non-prime Fermat pseudoprime base 35.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 124 say about the primality or not of 1217?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 117.

(8.5) What does the Miller-Rabin test base 18 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16799$, and public (encryption) keys $e_A = 31, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 10135$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 8 \bmod 53 \\ x = 2 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 49 modulo 4747. Specifically, find two more in addition to the 'obvious' square roots ± 7.

(9.3) Consider the quadratic polynomial $x^2 - 14x + 48$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 14x + 48 = (x - 8) \cdot (x - 6)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 14x + 48 = 0 \bmod 299$. In addition to the 'obvious' roots 8, 6 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 107 is a cube root of 209 modulo the prime 383, find a cube root of 209 modulo 383^2.

Unit 10 due Wed Dec 1

(10.1) The integer 216409 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 216409. When you give the oracle $33 \cdot 33$ to take the square root, it returns 101605. Factor 216409.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 731, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 15)\,\%\,31$ with $s_o = 7$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 6)\,\%\,107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 138

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Burnthecandleatbothends" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "kit" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 9$, $b = 5$.

(1.3) The ciphertext EZMPZCYZEEZMPESLETDESPTYQTYTETGP was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 12 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}g\text{"}) = \text{"}z\text{"}$ and $E_{a,b}(\text{"}j\text{"}) = \text{"}s\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 103 times in a row, out of which there were 39 heads and 64 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 4 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 6-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 8 elements to a set with 13 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'ENDV' and 'DEVN' do *not* have 'E' adjacent to 'N' and do *not* have 'D' adjacent to 'V' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 3 & 10 & 13 & 11 & 4 & 12 & 1 & 14 & 8 & 2 & 7 & 9 & 6 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 13 & 12 & 9 & 10 & 4 & 2 & 11 & 8 & 14 & 6 & 3 & 1 & 7 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 5 red balls and 8 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 9 red balls and 8 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 9 red balls, 8 blue balls, and 11 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3509, 319 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 85907, 105419.

(5.3) Efficiently compute a multiplicative inverse of 353 modulo 1051.

(5.4) Systematically find $\gcd(n, n+5, n+19)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48}-1$ and $7^{54}-1$.

(6.3) Efficiently compute $2^{41} \,\%\, 83$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 39 modulo 47.

(7.3) Find a cube root of 117 mod 149.

(7.4) Find a cube root of 111 modulo 337.

(7.5) Try to find a cube root of 29 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 55 is a non-prime Fermat pseudoprime base 21.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 19 say about the primality or not of 1601?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 68.

(8.5) What does the Miller-Rabin test base 19 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17767$, and public (encryption) keys $e_A = 37, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 7093$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 9 \bmod 59 \\ x = 3 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 64 modulo 5141. Specifically, find two more in addition to the 'obvious' square roots ± 8.

(9.3) Consider the quadratic polynomial $x^2 - 16x + 63$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 16x + 63 = (x - 9) \cdot (x - 7)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 16x + 63 = 0 \bmod 391$. In addition to the 'obvious' roots 9, 7 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 127 is a cube root of 75 modulo the prime 401, find a cube root of 75 modulo 401^2.

Unit 10 due Wed Dec 1

(10.1) The integer 204889 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 204889. When you give the oracle $43 \cdot 43$ to take the square root, it returns 203608. Factor 204889.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 689, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (4 \cdot s_n + 16) \,\%\, 31$ with $s_o = 6$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 7) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 0, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0$^{\text{th}}$ state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 139

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Haveyourcakeandeatittoo" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "sue" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 6$.

(1.3) The ciphertext BEXDGSMOKCPKCDDYCDKISXDROCKWOZVKMO was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 16 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}j\text{”}) = \text{“}l\text{”}$ and $E_{a,b}(\text{“}o\text{”}) = \text{“}s\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 105 times in a row, out of which there were 40 heads and 65 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 5 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 6-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 9 elements to a set with 15 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'LUKC' and 'KLCU' do *not* have 'L' adjacent to 'U' and do *not* have 'K' adjacent to 'C' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 12 & 1 & 2 & 7 & 9 & 14 & 10 & 8 & 13 & 4 & 5 & 6 & 11 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 5 & 11 & 9 & 7 & 14 & 8 & 1 & 4 & 12 & 6 & 13 & 3 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 6 red balls and 10 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 6 red balls and 5 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 6 red balls, 5 blue balls, and 18 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 5239, 403 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 91687, 109969.

(5.3) Efficiently compute a multiplicative inverse of 359 modulo 1061.

(5.4) Systematically find $\gcd(n, n+7, n+31)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64}-1$ and $6^{72}-1$.

(6.3) Efficiently compute $3^{44} \,\%\, 89$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 50 modulo 59.

(7.3) Find a cube root of 99 mod 167.

(7.4) Find a cube root of 178 modulo 349.

(7.5) Try to find a cube root of 30 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 57 is a non-prime Fermat pseudoprime base 20.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 42 say about the primality or not of 1601?

(8.4) Verify that 185 is a non-prime strong pseudoprime base 43.

(8.5) What does the Miller-Rabin test base 20 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 21209$, and public (encryption) keys $e_A = 41, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 17345$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 10 \bmod 61 \\ x = 4 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 81 modulo 5251. Specifically, find two more in addition to the 'obvious' square roots ± 9.

(9.3) Consider the quadratic polynomial $x^2 - 18x + 80$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 18x + 80 = (x - 10) \cdot (x - 8)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 18x + 80 = 0 \bmod 437$. In addition to the 'obvious' roots 10, 8 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 147 is a cube root of 78 modulo the prime 421, find a cube root of 78 modulo 421^2.

Unit 10 due Wed Dec 1

(10.1) The integer 202313 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 202313. When you give the oracle $41 \cdot 41$ to take the square root, it returns 198977. Factor 202313.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 611, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 13) \,\%\, 31$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (53 \cdot s_n + 8) \,\%\, 113$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 1, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 140

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Meetinthealleyatmidnight" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "dog" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 3$, $b = 7$.

(1.3) The ciphertext FTQDMUZUZEBMUZRMXXEYMUZXKAZFTQBMFUA was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}m\text{”}) = \text{“}j\text{”}$ and $E_{a,b}(\text{“}t\text{”}) = \text{“}m\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 107 times in a row, out of which there were 41 heads and 66 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 2 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 5-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 3 elements to a set with 5 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'SBRJ' and 'RSJB' do *not* have 'S' adjacent to 'B' and do *not* have 'R' adjacent to 'J' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 13 & 12 & 1 & 11 & 7 & 10 & 14 & 5 & 8 & 4 & 3 & 6 & 2 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 6 & 12 & 13 & 2 & 11 & 3 & 9 & 10 & 7 & 1 & 14 & 4 & 8 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 7 red balls and 7 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 3 red balls and 13 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 3 red balls, 13 blue balls, and 12 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2057, 187 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 94697, 100879.

(5.3) Efficiently compute a multiplicative inverse of 367 modulo 1009.

(5.4) Systematically find $\gcd(n, n+5, n+17)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21}-1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $2^{29} \,\%\, 59$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 26 modulo 43.

(7.3) Find a cube root of 49 mod 173.

(7.4) Find a cube root of 180 modulo 193.

(7.5) Try to find a cube root of 31 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 14.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 61 say about the primality or not of 1601?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 150.

(8.5) What does the Miller-Rabin test base 21 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 15251$, and public (encryption) keys $e_A = 11, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 4091$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 11 \bmod 47 \\ x = 5 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 100 modulo 3277. Specifically, find two more in addition to the 'obvious' square roots ± 10.

(9.3) Consider the quadratic polynomial $x^2 - 10x + 9$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 10x + 9 = (x-1) \cdot (x-9)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 10x + 9 = 0 \bmod 319$. In addition to the 'obvious' roots 1, 9 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 167 is a cube root of 204 modulo the prime 443, find a cube root of 204 modulo 443^2.

Unit 10 due Wed Dec 1

(10.1) The integer 173441 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 173441. When you give the oracle $31 \cdot 31$ to take the square root, it returns 172719. Factor 173441.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 901, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (6 \cdot s_n + 17) \,\%\, 31$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 2) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 1, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0$^{\text{th}}$ state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 141

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Bringyourownrefreshments" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "cat" by an affine cipher $E(x) = (ax + b)\,\%\,26$ with key $a = 5$, $b = 8$.

(1.3) The ciphertext CQNAJRWRWBYJRWOJUUBVJRWUHXWCQNPJAJPN was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}p\text{"}) = \text{"}t\text{"}$ and $E_{a,b}(\text{"}y\text{"}) = \text{"}a\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 109 times in a row, out of which there were 42 heads and 67 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 3 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 4-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 4 elements to a set with 7 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'ZIYQ' and 'YZQI' do *not* have 'Z' adjacent to 'I' and do *not* have 'Y' adjacent to 'Q' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 6 & 10 & 13 & 8 & 7 & 9 & 4 & 14 & 12 & 2 & 3 & 11 & 1 & 5 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 1 & 11 & 14 & 12 & 4 & 6 & 3 & 10 & 8 & 2 & 5 & 7 & 13 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 8 red balls and 9 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 7 red balls and 10 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 7 red balls, 10 blue balls, and 19 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3211, 247 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 98201, 103861.

(5.3) Efficiently compute a multiplicative inverse of 373 modulo 1013.

(5.4) Systematically find $\gcd(n, n+7, n+11)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $2^{30} \,\%\, 61$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 45 modulo 47.

(7.3) Find a cube root of 11 mod 179.

(7.4) Find a cube root of 153 modulo 211.

(7.5) Try to find a cube root of 32 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1601?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 99.

(8.5) What does the Miller-Rabin test base 22 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16171$, and public (encryption) keys $e_A = 19, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 1675$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 12 \bmod 53 \\ x = 6 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 121 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 11.

(9.3) Consider the quadratic polynomial $x^2 - 12x + 20$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 12x + 20 = (x - 2) \cdot (x - 10)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 12x + 20 = 0 \bmod 299$. In addition to the 'obvious' roots 2, 10 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 187 is a cube root of 379 modulo the prime 461, find a cube root of 379 modulo 461^2.

Unit 10 due Wed Dec 1

(10.1) The integer 155929 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 155929. When you give the oracle $47 \cdot 47$ to take the square root, it returns 138885. Factor 155929.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 779, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 19) \,\%\, 31$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 142

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Astitchintimesavesnine" by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext "fox" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 9$.

(1.3) The ciphertext WCBWNBPMNZGQVOXIVQVBWBPMKTWAMB was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 19 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}$("*s*") = "*p*" and $E_{a,b}$("*d*") = "*i*". Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 111 times in a row, out of which there were 43 heads and 68 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 4 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 7-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 5 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'GPFX' and 'FGXP' do *not* have 'G' adjacent to 'P' and do *not* have 'F' adjacent to 'X' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 5 & 13 & 1 & 3 & 10 & 8 & 7 & 12 & 14 & 9 & 4 & 6 & 2 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 12 & 6 & 8 & 4 & 2 & 13 & 7 & 5 & 14 & 3 & 11 & 1 & 10 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 9 red balls and 11 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 4 red balls and 7 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 4 red balls, 7 blue balls, and 13 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 2783, 253 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 102257, 109289.

(5.3) Efficiently compute a multiplicative inverse of 379 modulo 1019.

(5.4) Systematically find $\gcd(n, n+11, n+13)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $2^{33} \,\%\, 67$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 8 modulo 59.

(7.3) Find a cube root of 115 mod 191.

(7.4) Find a cube root of 66 modulo 223.

(7.5) Try to find a cube root of 35 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 66 is a non-prime Fermat pseudoprime base 31.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 105 say about the primality or not of 1601?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 89.

(8.5) What does the Miller-Rabin test base 23 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17441$, and public (encryption) keys $e_A = 23, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 13439$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 13 \bmod 59 \\ x = 7 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 144 modulo 3959. Specifically, find two more in addition to the 'obvious' square roots ± 12.

(9.3) Consider the quadratic polynomial $x^2 - 14x + 33$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 14x + 33 = (x-3) \cdot (x-11)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 14x + 33 = 0 \bmod 391$. In addition to the 'obvious' roots 3, 11 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 207 is a cube root of 12 modulo the prime 487, find a cube root of 12 modulo 487^2.

Unit 10 due Wed Dec 1

(10.1) The integer 140873 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 140873. When you give the oracle $43 \cdot 43$ to take the square root, it returns 121942. Factor 140873.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 799, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (8 \cdot s_n + 23) \,\%\, 31$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 4) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 1, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 143

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Honestyisthebestpolicy" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 9$, $b = 10$.

(1.3) The ciphertext GURERVFABOHFVARFFYVXRFUBJOHFVARFF was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 11 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}o\text{"}) = \text{"}x\text{"}$ and $E_{a,b}(\text{"}f\text{"}) = \text{"}w\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 113 times in a row, out of which there were 44 heads and 69 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 5 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'NWME' and 'MNEW' do *not* have 'N' adjacent to 'W' and do *not* have 'M' adjacent to 'E' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 14 & 5 & 12 & 13 & 1 & 10 & 3 & 7 & 2 & 8 & 6 & 11 & 4 & 9 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 12 & 4 & 2 & 10 & 7 & 8 & 5 & 9 & 3 & 6 & 14 & 13 & 11 & 1 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 10 red balls and 13 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 8 red balls and 4 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 4 blue balls, and 7 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 4901, 377 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 108371, 116353.

(5.3) Efficiently compute a multiplicative inverse of 313 modulo 1021.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48}-1$ and $7^{54}-1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 19 modulo 43.

(7.3) Find a cube root of 119 mod 197.

(7.4) Find a cube root of 216 modulo 241.

(7.5) Try to find a cube root of 35 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 69 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 46 say about the primality or not of 1409?

(8.4) Verify that 169 is a non-prime strong pseudoprime base 80.

(8.5) What does the Miller-Rabin test base 24 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 18203$, and public (encryption) keys $e_A = 29, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 14837$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 3 \bmod 61 \\ x = 8 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 4 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 2.

(9.3) Consider the quadratic polynomial $x^2 - 5x + 4$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 5x + 4 = (x-4) \cdot (x-1)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 5x + 4 = 0 \bmod 437$. In addition to the 'obvious' roots 4, 1 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 7 is a cube root of 62 modulo the prime 281, find a cube root of 62 modulo 281^2.

Unit 10 due Wed Dec 1

(10.1) The integer 106241 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 106241. When you give the oracle $61 \cdot 61$ to take the square root, it returns 59142. Factor 106241.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 11) \,\%\, 29$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 1, 1, 1, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 144

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Pennywiseandpoundfoolish" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "bus" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 5$.

(1.3) The ciphertext LAPYYJDLGPOTDYZESTYRXFNS was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 13 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}r\text{”}) = \text{“}p\text{”}$ and $E_{a,b}(\text{“}k\text{”}) = \text{“}g\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 115 times in a row, out of which there were 45 heads and 70 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 2 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 7 elements to a set with 13 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'UDTL' and 'TULD' do *not* have 'U' adjacent to 'D' and do *not* have 'T' adjacent to 'L' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 8 & 12 & 11 & 10 & 7 & 4 & 9 & 14 & 13 & 5 & 3 & 6 & 1 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 12 & 4 & 6 & 13 & 8 & 1 & 5 & 2 & 3 & 14 & 7 & 10 & 11 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 2 red balls and 6 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 5 red balls and 12 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 5 red balls, 12 blue balls, and 14 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 3751, 341 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 79927, 98431.

(5.3) Efficiently compute a multiplicative inverse of 317 modulo 1031.

(5.4) Systematically find $\gcd(n, n+3, n+23)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21} - 1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64} - 1$ and $6^{72} - 1$.

(6.3) Efficiently compute $3^{39} \,\%\, 79$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 41 modulo 47.

(7.3) Find a cube root of 120 mod 131.

(7.4) Find a cube root of 131 modulo 277.

(7.5) Try to find a cube root of 35 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 45 is a non-prime Fermat pseudoprime base 17.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 49 say about the primality or not of 1409?

(8.4) Verify that 265 is a non-prime strong pseudoprime base 23.

(8.5) What does the Miller-Rabin test base 25 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 19177$, and public (encryption) keys $e_A = 31, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 17071$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 4 \bmod 47 \\ x = 9 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 9 modulo 4747. Specifically, find two more in addition to the 'obvious' square roots ± 3.

(9.3) Consider the quadratic polynomial $x^2 - 7x + 10$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 7x + 10 = (x - 5) \cdot (x - 2)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 7x + 10 = 0 \bmod 319$. In addition to the 'obvious' roots 5, 2 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 27 is a cube root of 35 modulo the prime 307, find a cube root of 35 modulo 307^2.

Unit 10 due Wed Dec 1

(10.1) The integer 106241 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 106241. When you give the oracle $19 \cdot 19$ to take the square root, it returns 96528. Factor 106241.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 731, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (4 \cdot s_n + 13) \,\%\, 29$ with $s_o = 4$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 6) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0$^{\text{th}}$ state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 145

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Awinkisasgoodasanod" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "kit" by an affine cipher $E(x) = (ax + b)\,\%\,26$ with key $a = 3$, $b = 6$.

(1.3) The ciphertext DYLOYBXYDDYLODRKDSCDROSXPSXSDSFO was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 15 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}u\text{”}) = \text{“}t\text{”}$ and $E_{a,b}(\text{“}p\text{”}) = \text{“}k\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 117 times in a row, out of which there were 46 heads and 71 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 3 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 6-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 8 elements to a set with 10 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'BKAS' and 'ABSK' do *not* have 'B' adjacent to 'K' and do *not* have 'A' adjacent to 'S' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 13 & 11 & 12 & 14 & 7 & 10 & 2 & 1 & 4 & 3 & 6 & 9 & 8 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 8 & 12 & 7 & 3 & 9 & 10 & 1 & 5 & 2 & 4 & 6 & 14 & 13 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 3 red balls and 3 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 9 red balls and 9 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 9 red balls, 9 blue balls, and 8 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2873, 221 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 82319, 102307.

(5.3) Efficiently compute a multiplicative inverse of 331 modulo 1033.

(5.4) Systematically find $\gcd(n, n+5, n+19)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $2^{41} \,\%\, 83$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 57 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 52 modulo 59.

(7.3) Find a cube root of 87 mod 137.

(7.4) Find a cube root of 218 modulo 337.

(7.5) Try to find a cube root of 36 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 49 is a non-prime Fermat pseudoprime base 18.

(8.2) An RSA cipher was set up with modulus 24163 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 115 say about the primality or not of 1409?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 133.

(8.5) What does the Miller-Rabin test base 26 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 15857$, and public (encryption) keys $e_A = 37, e_B = 1409$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 3373$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 5 \bmod 53 \\ x = 10 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 16 modulo 5141. Specifically, find two more in addition to the 'obvious' square roots ± 4.

(9.3) Consider the quadratic polynomial $x^2 - 9x + 18$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 9x + 18 = (x - 6) \cdot (x - 3)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 9x + 18 = 0 \bmod 299$. In addition to the 'obvious' roots 6, 3 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 47 is a cube root of 220 modulo the prime 331, find a cube root of 220 modulo 331^2.

Unit 10 due Wed Dec 1

(10.1) The integer 140873 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 140873. When you give the oracle $7 \cdot 7$ to take the square root, it returns 65328. Factor 140873.

(10.2) Use Pollard's rho method to find a proper factor of 1313.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 689, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 15) \,\%\, 29$ with $s_o = 3$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 7) \,\%\, 107$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1011011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 146

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Burnthecandleatbothends" by a shift cipher with key 10.

(1.2) (Short answer) Encrypt the plaintext "sue" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 5$, $b = 7$.

(1.3) The ciphertext DGZFIUOQMERMEFFAEFMKUZFTQEMYQBXMOQ was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 17 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}x\text{"}) = \text{"}j\text{"}$ and $E_{a,b}(\text{"}u\text{"}) = \text{"}i\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 90 times in a row, out of which there were 47 heads and 43 tails. What is the probability that the next flip will be a head?

(2.2) There are 3 blue balls and 4 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 9 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 6-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 9 elements to a set with 12 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 8-element set to a 7-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'IRHZ' and 'HIZR' do *not* have 'I' adjacent to 'R' and do *not* have 'H' adjacent to 'Z' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 14 & 12 & 6 & 10 & 9 & 4 & 2 & 7 & 3 & 13 & 8 & 11 & 5 & 1 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 14 & 9 & 6 & 12 & 8 & 1 & 3 & 10 & 7 & 4 & 13 & 5 & 11 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 4 red balls and 5 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 6 red balls and 6 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 6 red balls, 6 blue balls, and 15 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 2299, 209 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 85273, 106793.

(5.3) Efficiently compute a multiplicative inverse of 337 modulo 1039.

(5.4) Systematically find $\gcd(n, n+7, n+31)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $5^{56}-1$ and $5^{72}-1$.

(6.3) Efficiently compute $3^{44} \,\%\, 89$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 30 modulo 127 so that b itself is a square modulo 127.

(7.2) Try to find a square root of 5 modulo 43.

(7.3) Find a cube root of 46 mod 149.

(7.4) Find a cube root of 261 modulo 349.

(7.5) Try to find a cube root of 39 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 51 is a non-prime Fermat pseudoprime base 35.

(8.2) An RSA cipher was set up with modulus 30883 and encryption exponent 13. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 76 say about the primality or not of 1217?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 12.

(8.5) What does the Miller-Rabin test base 27 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16789$, and public (encryption) keys $e_A = 41, e_B = 401$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 16121$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 6 \bmod 59 \\ x = 11 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 25 modulo 5251. Specifically, find two more in addition to the 'obvious' square roots ± 5.

(9.3) Consider the quadratic polynomial $x^2 - 11x + 28$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 11x + 28 = (x - 7) \cdot (x - 4)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 11x + 28 = 0 \bmod 391$. In addition to the 'obvious' roots 7, 4 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 67 is a cube root of 261 modulo the prime 347, find a cube root of 261 modulo 347^2.

Unit 10 due Wed Dec 1

(10.1) The integer 155929 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 155929. When you give the oracle $17 \cdot 17$ to take the square root, it returns 105694. Factor 155929.

(10.2) Use Pollard's rho method to find a proper factor of 1649.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 611, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (6 \cdot s_n + 12) \,\%\, 29$ with $s_o = 2$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (53 \cdot s_n + 8) \,\%\, 113$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100001 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 147

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext “Haveyourcakeandeatittoo” by a shift cipher with key 12.

(1.2) (Short answer) Encrypt the plaintext “dog” by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 7$, $b = 8$.

(1.3) The ciphertext CQNAJRWRWBYJRWOJUUBVJRWUHXWCQNYJCRX was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}a\text{”}) = \text{“}l\text{”}$ and $E_{a,b}(\text{“}l\text{”}) = \text{“}c\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 71 times in a row, out of which there were 27 heads and 44 tails. What is the probability that the next flip will be a head?

(2.2) There are 4 blue balls and 5 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 5-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 3 elements to a set with 7 elements?

(2.5) How many surjective functions are there from a 10-element set to a 2-element set?

(2.6) How many surjective functions are there from a 9-element set to a 8-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings ‘PYOG’ and ‘OPGY’ do *not* have ‘P’ adjacent to ‘Y’ and do *not* have ‘O’ adjacent to ‘G’ in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 8 & 7 & 1 & 9 & 11 & 14 & 3 & 13 & 12 & 6 & 2 & 4 & 10 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 14 & 12 & 1 & 7 & 9 & 2 & 3 & 5 & 10 & 6 & 13 & 8 & 11 & 4 \end{pmatrix}$$

(3.4) How many permutations of order 30 are there of 10 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 5 red balls and 7 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 3 red balls and 14 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 3 red balls, 14 blue balls, and 9 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3887, 299 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-9)$ is not prime for any $n \geq 11$.

(5.2) Efficiently compute the greatest common divisor of 89701, 97289.

(5.3) Efficiently compute a multiplicative inverse of 347 modulo 1049.

(5.4) Systematically find $\gcd(n, n+5, n+17)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{107}.

Unit 6 due Wed Oct 27

(6.1) Factor $(5^{10}-1)/4 = 2441406$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $2^{140}-1$ and $2^{120}-1$.

(6.3) Efficiently compute $2^{29} \,\%\, 59$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 5 modulo 131 so that b itself is a square modulo 131.

(7.2) Try to find a square root of 40 modulo 47.

(7.3) Find a cube root of 141 mod 167.

(7.4) Find a cube root of 105 modulo 193.

(7.5) Try to find a cube root of 39 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 55 is a non-prime Fermat pseudoprime base 21.

(8.2) An RSA cipher was set up with modulus 20591 and encryption exponent 17. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 102 say about the primality or not of 1217?

(8.4) Verify that 145 is a non-prime strong pseudoprime base 17.

(8.5) What does the Miller-Rabin test base 28 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 17869$, and public (encryption) keys $e_A = 11, e_B = 491$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 4799$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 7 \bmod 61 \\ x = 12 \bmod 71 \end{cases}$$

(9.2) Find four different square roots of 36 modulo 3277. Specifically, find two more in addition to the 'obvious' square roots ± 6.

(9.3) Consider the quadratic polynomial $x^2 - 13x + 40$ as having coefficients in $\mathbf{Z}/437$. In addition to the 'obvious' factorization $x^2 - 13x + 40 = (x-8) \cdot (x-5)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 13x + 40 = 0 \bmod 437$. In addition to the 'obvious' roots 8, 5 mod 437, find two other completely different roots mod 437.

(9.5) Noting that 87 is a cube root of 105 modulo the prime 367, find a cube root of 105 modulo 367^2.

Unit 10 due Wed Dec 1

(10.1) The integer 173441 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 173441. When you give the oracle $29 \cdot 29$ to take the square root, it returns 62219. Factor 173441.

(10.2) Use Pollard's rho method to find a proper factor of 1843.

(10.3) Use Pollard's $p-1$ method to find a proper factor p of 901, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1537, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1537}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (7 \cdot s_n + 11) \,\%\, 29$ with $s_o = 1$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 2) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 0, 1, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 31$ and 0^{th} state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1100111 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 148

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Meetinthealleyatmidnight" by a shift cipher with key 9.

(1.2) (Short answer) Encrypt the plaintext "cat" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 9$, $b = 9$.

(1.3) The ciphertext BPMZIQVQVAXIQVNITTAUIQVTGWVBPMOIZIOM was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 18 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}$("*d*") = "*l*" and $E_{a,b}$("*o*") = "*q*". Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 73 times in a row, out of which there were 28 heads and 45 tails. What is the probability that the next flip will be a head?

(2.2) There are 5 blue balls and 2 red balls in an urn. What is the probability of drawing at least 6 blue balls out of 8 draws (with replacement)?

(2.3) How many pairs of disjoint 4-element and 5-element subsets of a 13-element set are there?

(2.4) How many injections are there from a set with 4 elements to a set with 9 elements?

(2.5) How many surjective functions are there from a 11-element set to a 2-element set?

(2.6) How many surjective functions are there from a 10-element set to a 9-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'WFVN' and 'VWNF' do *not* have 'W' adjacent to 'F' and do *not* have 'V' adjacent to 'N' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 8 & 10 & 11 & 1 & 2 & 14 & 13 & 3 & 6 & 12 & 7 & 9 & 4 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 8 & 12 & 14 & 7 & 4 & 5 & 6 & 11 & 3 & 13 & 9 & 1 & 2 \end{pmatrix}$$

(3.4) How many permutations of order 15 are there of 9 things?

(3.5) (*) How many permutations of 7 things are there with at least 3 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 6 red balls and 9 blue balls in an urn. What is the expected number of red balls drawn in 13 draws (with replacement)?

(4.2) There are 7 red balls and 11 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 7 red balls, 11 blue balls, and 16 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 667, 3509, 319 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n \to +\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-6)$ is not prime for any $n \geq 8$.

(5.2) Efficiently compute the greatest common divisor of 93349, 101659.

(5.3) Efficiently compute a multiplicative inverse of 349 modulo 1051.

(5.4) Systematically find $\gcd(n, n+7, n+11)$ for arbitrary n.

(5.5) Find the ones'-place digit of 7^{101}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{21} - 1 = 2097151$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $7^{48} - 1$ and $7^{54} - 1$.

(6.3) Efficiently compute $2^{30} \,\%\, 61$.

(6.4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

(6.5) Relatively gracefully, by hand factor

$$2^{22} + 1 = 4194305$$

or

$$2^{26} + 1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34} + 1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 59 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 37 modulo 59.

(7.3) Find a cube root of 79 mod 173.

(7.4) Find a cube root of 82 modulo 211.

(7.5) Try to find a cube root of 39 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 57 is a non-prime Fermat pseudoprime base 20.

(8.2) An RSA cipher was set up with modulus 26207 and encryption exponent 19. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 124 say about the primality or not of 1217?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 13.

(8.5) What does the Miller-Rabin test base 29 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16459$, and public (encryption) keys $e_A = 19, e_B = 503$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 9379$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 8 \bmod 47 \\ x = 13 \bmod 83 \end{cases}$$

(9.2) Find four different square roots of 49 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 7.

(9.3) Consider the quadratic polynomial $x^2 - 15x + 54$ as having coefficients in $\mathbf{Z}/319$. In addition to the 'obvious' factorization $x^2 - 15x + 54 = (x - 9) \cdot (x - 6)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 15x + 54 = 0 \bmod 319$. In addition to the 'obvious' roots 9, 6 mod 319, find two other completely different roots mod 319.

(9.5) Noting that 107 is a cube root of 209 modulo the prime 383, find a cube root of 209 modulo 383^2.

Unit 10 due Wed Dec 1

(10.1) The integer 202313 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 202313. When you give the oracle $13 \cdot 13$ to take the square root, it returns 35599. Factor 202313.

(10.2) Use Pollard's rho method to find a proper factor of 1177.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 779, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1591, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1591}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (3 \cdot s_n + 15) \,\%\, 31$ with $s_o = 7$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 0, 0, 1)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0^{th} state/seed $s_o = 10$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 10$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1101101 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 149

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Bringyourownrefreshments" by a shift cipher with key 13.

(1.2) (Short answer) Encrypt the plaintext "fox" by an affine cipher $E(x) = (ax + b) \% 26$ with key $a = 11$, $b = 10$.

(1.3) The ciphertext BHGBSGURSELVATCNAVAGBGURPYBFRG was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 12 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{“}g\text{”}) = \text{“}z\text{”}$ and $E_{a,b}(\text{“}j\text{”}) = \text{“}s\text{”}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 75 times in a row, out of which there were 29 heads and 46 tails. What is the probability that the next flip will be a head?

(2.2) There are 6 blue balls and 3 red balls in an urn. What is the probability of drawing at least 7 blue balls out of 10 draws (with replacement)?

(2.3) How many pairs of disjoint 2-element and 7-element subsets of a 14-element set are there?

(2.4) How many injections are there from a set with 5 elements to a set with 11 elements?

(2.5) How many surjective functions are there from a 8-element set to a 2-element set?

(2.6) How many surjective functions are there from a 11-element set to a 10-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'DMCU' and 'CDUM' do *not* have 'D' adjacent to 'M' and do *not* have 'C' adjacent to 'U' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 13 & 8 & 12 & 11 & 3 & 10 & 4 & 5 & 1 & 14 & 6 & 2 & 7 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 6 & 11 & 7 & 4 & 2 & 8 & 1 & 12 & 14 & 9 & 13 & 3 & 5 \end{pmatrix}$$

(3.4) How many permutations of order 12 are there of 8 things?

(3.5) (*) How many permutations of 9 things are there with at least 5 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 7 red balls and 11 blue balls in an urn. What is the expected number of red balls drawn in 15 draws (with replacement)?

(4.2) There are 4 red balls and 8 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 4 red balls, 8 blue balls, and 10 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 589, 5239, 403 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-3)(n-5)$ is not prime for any $n \geq 7$.

(5.2) Efficiently compute the greatest common divisor of 97507, 104813.

(5.3) Efficiently compute a multiplicative inverse of 353 modulo 1061.

(5.4) Systematically find $\gcd(n, n+11, n+13)$ for arbitrary n.

(5.5) Find the ones'-place digit of 9^{103}.

Unit 6 due Wed Oct 27

(6.1) Factor $2^{24}-1 = 16777215$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $6^{64}-1$ and $6^{72}-1$.

(6.3) Efficiently compute $2^{33} \,\%\, 67$.

(6.4) Verify (with reasonable efficiency) that 2 is a primitive root modulo 83.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 85 modulo 107 so that b itself is a square modulo 107.

(7.2) Try to find a square root of 27 modulo 43.

(7.3) Find a cube root of 29 mod 179.

(7.4) Find a cube root of 95 modulo 223.

(7.5) Try to find a cube root of 40 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 14.

(8.2) An RSA cipher was set up with modulus 32663 and encryption exponent 23. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 19 say about the primality or not of 1601?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 38.

(8.5) What does the Miller-Rabin test base 30 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 19939$, and public (encryption) keys $e_A = 23, e_B = 809$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 15383$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 9 \bmod 53 \\ x = 14 \bmod 79 \end{cases}$$

(9.2) Find four different square roots of 64 modulo 3959. Specifically, find two more in addition to the 'obvious' square roots ± 8.

(9.3) Consider the quadratic polynomial $x^2 - 17x + 70$ as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 17x + 70 = (x - 10) \cdot (x - 7)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 17x + 70 = 0 \bmod 299$. In addition to the 'obvious' roots 10, 7 mod 299, find two other completely different roots mod 299.

(9.5) Noting that 127 is a cube root of 75 modulo the prime 401, find a cube root of 75 modulo 401^2.

Unit 10 due Wed Dec 1

(10.1) The integer 204889 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 204889. When you give the oracle $23 \cdot 23$ to take the square root, it returns 143631. Factor 204889.

(10.2) Use Pollard's rho method to find a proper factor of 1417.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 799, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1739, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1739}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000$^{\text{th}}$ point of the LCG given by $s_{n+1} = (4 \cdot s_n + 16) \,\%\, 31$ with $s_o = 6$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (43 \cdot s_n + 4) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 0, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5$^{\text{th}}$ pseudorandom bit generated by the BBS pRNG with modulus $n = 43 \cdot 11$ and 0$^{\text{th}}$ state/seed $s_o = 7$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 11$ and seed $s_o = 7$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1110011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.

Crypto Homework version 150

Unit 1 due Wed Sept 15

(1.1) (Short answer) Encrypt the plaintext "Astitchintimesavesnine" by a shift cipher with key 11.

(1.2) (Short answer) Encrypt the plaintext "bin" by an affine cipher $E(x) = (ax + b) \,\%\, 26$ with key $a = 3$, $b = 5$.

(1.3) The ciphertext ESPCPTDYZMFDTYPDDWTVPDSZHMFDTYPDD was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(1.4) Find a multiplicative inverse of 16 modulo 43 (without using the Euclidean algorithm). Show your work. Explain.

(1.5) An affine cipher with unknown key (a, b) encrypts $E_{a,b}(\text{"}j\text{"}) = \text{"}l\text{"}$ and $E_{a,b}(\text{"}o\text{"}) = \text{"}s\text{"}$. Determine the key.

Unit 2 due Wed Sept 22

(2.1) (Short answer) You flipped a fair coin 77 times in a row, out of which there were 30 heads and 47 tails. What is the probability that the next flip will be a head?

(2.2) There are 2 blue balls and 4 red balls in an urn. What is the probability of drawing at least 5 blue balls out of 7 draws (with replacement)?

(2.3) How many pairs of disjoint 3-element and 4-element subsets of a 12-element set are there?

(2.4) How many injections are there from a set with 6 elements to a set with 8 elements?

(2.5) How many surjective functions are there from a 9-element set to a 2-element set?

(2.6) How many surjective functions are there from a 7-element set to a 6-element set?

Unit 3 due Wed Sept 29

(3.1) As in double anagramming: How many *simultaneous* permutations of the two strings 'KTJB' and 'JKBT' do *not* have 'K' adjacent to 'T' and do *not* have 'J' adjacent to 'B' in either rearranged string?

(3.2) Compute P^4, where P is the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 9 & 7 & 12 & 10 & 2 & 13 & 8 & 1 & 11 & 6 & 5 & 3 & 14 & 4 \end{pmatrix}$$

(3.3) Determine the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 13 & 10 & 5 & 7 & 2 & 14 & 11 & 9 & 4 & 6 & 8 & 3 & 1 & 12 \end{pmatrix}$$

(3.4) How many permutations of order 18 are there of 12 things?

(3.5) (*) How many permutations of 8 things are there with at least 4 fixed-points?

Unit 4 due Wed Oct 6

(4.1) There are 8 red balls and 8 blue balls in an urn. What is the expected number of red balls drawn in 11 draws (with replacement)?

(4.2) There are 8 red balls and 5 blue balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.3) There are 8 red balls, 5 blue balls, and 17 green balls in an urn. You draw repeatedly (with replacement). What is the expected number of draws necessary so that you'll have drawn at least one ball of each color?

(4.4) Find the greatest common divisor and least common multiple of 289, 2057, 187 by the naive method factoring them into primes and comparing prime factors.

(4.5) (*) Let $f(n)$ be the number of permutations of n things with no fixed points. Determine

$$\lim_{n\to+\infty} \frac{f(n)}{n!}$$

Unit 5 due Wed Oct 20

(5.1) Explain why $(n-4)(n-8)$ is not prime for any $n \geq 10$.

(5.2) Efficiently compute the greatest common divisor of 98767, 107257.

(5.3) Efficiently compute a multiplicative inverse of 359 modulo 1009.

(5.4) Systematically find $\gcd(n, n+2, n+101)$ for arbitrary n.

(5.5) Find the ones'-place digit of 3^{105}.

Unit 6 due Wed Oct 27

(6.1) Factor $(3^{16}-1)/2 = 21523360$ *gracefully* (meaning using high-school algebra identities to find several large factors as the beginning, which has the effect of making clear *before* any computations are done that the run-time will be small).

(6.2) Efficiently find the greatest common divisor of $3^{121}-1$ and $3^{99}-1$.

(6.3) Efficiently compute $5^{36} \,\%\, 73$.

(6.4) Verify (with reasonable efficiency) that 11 is a primitive root modulo 47.

(6.5) Relatively gracefully, by hand factor

$$2^{22}+1 = 4194305$$

or

$$2^{26}+1 = 67108865$$

Slightly out of reach of purely hand computation is

$$2^{34}+1 = 17179869185$$

Unit 7 due Wed Nov 3

(7.1) Find a square root b of 14 modulo 103 so that b itself is a square modulo 103.

(7.2) Try to find a square root of 35 modulo 47.

(7.3) Find a cube root of 109 mod 191.

(7.4) Find a cube root of 6 modulo 241.

(7.5) Try to find a cube root of 42 modulo 61.

Unit 8 due Wed Nov 17

(8.1) Verify that 65 is a non-prime Fermat pseudoprime base 47.

(8.2) An RSA cipher was set up with modulus 18349 and encryption exponent 11. What is the decryption exponent?

(8.3) What does the Miller-Rabin test base 42 say about the primality or not of 1601?

(8.4) Verify that 85 is a non-prime strong pseudoprime base 47.

(8.5) What does the Miller-Rabin test base 31 say about the primality or not of 85?

(8.6) (*) Alice and Bob have RSA setups with the same modulus $n = 16463$, and public (encryption) keys $e_A = 29, e_B = 1103$, respectively. Alice wants to break into Bob's stuff. Alice's decryption exponent is $d_A = 4469$. How does she find Bob's decryption exponent d_B, or something just as good?

Unit 9 due Wed Nov 25

(9.1) Find a solution to the system

$$\begin{cases} x = 10 \bmod 59 \\ x = 15 \bmod 73 \end{cases}$$

(9.2) Find four different square roots of 81 modulo 4429. Specifically, find two more in addition to the 'obvious' square roots ± 9.

(9.3) Consider the quadratic polynomial $x^2 - 9x + 8$ as having coefficients in $\mathbf{Z}/391$. In addition to the 'obvious' factorization $x^2 - 9x + 8 = (x - 1) \cdot (x - 8)$ find another completely different factorization.

(9.4) Consider the quadratic equation $x^2 - 9x + 8 = 0 \bmod 391$. In addition to the 'obvious' roots 1, 8 mod 391, find two other completely different roots mod 391.

(9.5) Noting that 147 is a cube root of 78 modulo the prime 421, find a cube root of 78 modulo 421^2.

Unit 10 due Wed Dec 1

(10.1) The integer 216409 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 216409. When you give the oracle $13 \cdot 13$ to take the square root, it returns 123920. Factor 216409.

(10.2) Use Pollard's rho method to find a proper factor of 1133.

(10.3) Use Pollard's $p - 1$ method to find a proper factor p of 817, using list of primes $2, 3$.

(10.4) Use the random squares algorithm to find a proper factor of 1333, using factor base $2, 3, 5$. That is, for successive integers a just above $\sqrt{1333}$, successively compute $a^2 - n$, recording those pairs a, b such that b is a product of primes from the factor base, etc. The luckiest case is when $a^2 - n$ is a square...

Unit 11 due Wed Dec 15

(11.1) Find the 1000^{th} point of the LCG given by $s_{n+1} = (5 \cdot s_n + 13) \,\%\, 31$ with $s_o = 5$.

(11.2) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 5) \,\%\, 103$.

(11.3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (1, 0, 0, 0, 1, 0, 0, 0)$$

That is, determine the size of the loop of states that will repeat.

(11.4) Find the 5^{th} pseudorandom bit generated by the BBS pRNG with modulus $n = 31 \cdot 23$ and 0^{th} state/seed $s_o = 5$.

(11.5) Find the period length of the BBS pRNG with modulus $n = 31 \cdot 23$ and seed $s_o = 5$. What is the loop of pseudorandom bits?

(11.6) Verify that the binary string 1000011 (interpreted as a polynomial, powers going from highest to lowest, coefficients in $\mathbf{F}_2$) is **primitive**.