Math 5248 Cryptology and number theory
Fall 2005, Vic Reiner
Midterm exam 2- Due Wednesday November 16, in class

Instructions: This is an open book, open library, open notes, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult. Explain your reasoning- answers without justification or proof (where appropriate) will receive **no credit**.

1. (20 points total) Alice establishes an RSA cipher with Bob by publishing the modulus $n = 589$ (keeping secret its factorization $n = pq$ into two primes p, q), and publishing an encryption exponent $e = 7$.

(a) (5 points) How would Bob encrypt the plaintext $x = 12$, that is, what ciphertext y would he send to Alice?

(b) (10 points) If Alice received from Bob the ciphertext $y = 547$, how would she decrypt it, and what plaintext x would she recover?

(c) (5 points) Given Alice's fixed choice of the modulus $n = 589$, how many encryption exponents e are available for Alice to choose?

2. (20 points total) In all three parts of this problem, answers with no explanation or those found *by brute force* will receive no credit.

(a)(5 points) Find a square root $\bar{x}_1$ of $\bar{5}$ in $\mathbb{Z}/19$ such that $\bar{x}_1$ itself is a perfect square in $\mathbb{Z}/19$.

(b)(5 points) Find a square root $\bar{x}_2$ of $\bar{5}$ in $\mathbb{Z}/31$ such that $\bar{x}_2$ is *not* itself a perfect square.

(c)(10 points) Find *all* square roots $\bar{x}$ of $\bar{5}$ in $\mathbb{Z}/589$, and explain how you know that you've found all of them.

3. (15 points) Find *any* square root of $\bar{5}$ in $\mathbb{Z}/19^3$ using Hensel's Lemma. Brute forces answers will again receive no credit.

4. (15 points) Let $G = (\mathbb{Z}/m)^\times$ with group operation given by multiplication. Prove that the subset H consisting of those $\bar{x}$ which are perfect squares,

$$H := \{\bar{x} \in (\mathbb{Z}/m)^\times : \text{ there exists } \bar{z} \text{ in } (\mathbb{Z}/m)^\times \text{ with } \bar{x} = \bar{z}^2\},$$

is a subgroup of G.

5. (15 points) Prove the following fact, whose relevance for RSA encryption is explained below.

> Suppose $n = pq$ where p, q are prime, and d, e are integers satisfying $de \equiv 1 \mod (p-1)(q-1)$.
>
> Then for *any* element $\bar{x}$ of $\mathbb{Z}/n$, whether or not $\bar{x}$ lies in $(\mathbb{Z}/n)^\times$, one has
> $$(\bar{x}^d)^e = \bar{x}.$$

Relevance to RSA: This means that Alice, after publishing the modulus n and encryption exponent e, does *not* need to restrict Bob by asking him to only encrypt plaintexts $\bar{x}$ that lie in $(\mathbb{Z}/n)^\times$; *any* plaintexts in $\mathbb{Z}/n$ will encrypt/decrypt correctly. Note that any way in which Alice might communicate such a restriction would have tipped off Bob (and hence also Eve) about either the value of $\varphi(n)$, or equivalently, the factorization $n = pq$.

6. (15 points) Prove the following fact, whose relevance for a form of the *common modulus attack* on RSA is explained below.

> Suppose n is a given modulus, and D is a multiplicative inverse for e modulo $k \cdot \varphi(n)$, that is,
> $$\overline{De} = \bar{1} \in \mathbb{Z}/k\varphi(n).$$
> where k is any integer. Then
> $$(\bar{x}^e)^D = \bar{x}$$
> for any $\bar{x}$ in $(\mathbb{Z}/n)^\times$.

Relevance to common modulus attack on RSA: Imagine that even though the factorization $n = pq$ and the value of $\varphi(n)$ are still secret, someone leaked to Eve a pair of encryption and decryption exponents d', e' that were set up for the same modulus n. Then even though Eve does not have the factorization $n = pq$, she *does* know $d'e' - 1 = k\varphi(n)$ for some integer k, and since she knows the public encryption exponent e, she can compute quickly via Euclid's algorithm a multiplicative inverse D for e mod $d'e' - 1$. Then using the fact above, Eve is able to quickly decrypt Bob's messages to Alice simply by raising them to the D^{th} power mod n.