Math 5248 Cryptology and number theory
Fall 2005, Vic Reiner
Final exam - Due Wednesday December 14, 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) Find any square root of $\bar{8}$ in $\mathbb{Z}/23^3 31^2$, using no brute force: the only methods you should employ are principal square roots, Sun Ze, and Hensel's Lemma.

2. (15 points total) Check whether or not $n = 169 (= 13^2)$ is a pseudoprime for the base $b = 19$ with respect to each of these primality tests:

(a)(5 points) Fermat.

(b)(5 points) Solovay-Strassen.

(c)(5 points) Miller-Rabin test.

3. (20 points total)

(a)(10 points) Someone tells you that the composite number $n = 67591$ has a prime factor p for which $p-1$ is $\{2\}$-smooth. Use Pollard's $p-1$ method to find p and to factor n.

(b)(10 points) Alice published the RSA modulus $n = 16637$, and Eve wants to factor it into $n = pq$ for two primes p, q. Luckily, Eve has the keys to her sister's square-root oracle, which she is borrowing for the weekend. She inputs to the square-root oracle the perfect square $\bar{4} = \bar{2}^2$ in $\mathbb{Z}/16637$, and the oracle spits back the square-root $\overline{129}$ for $\bar{4}$ in $\mathbb{Z}/16637$. Use the oracle's output to factor n for Eve.

4. (16 points total) For each of the following assertions, either prove it, or disprove it by exhibiting a counterexample.

(a)(8 points) For all positive integers n and every $\bar{x} \in \mathbb{Z}/n$, one has $\bar{x}^n = \bar{x}$.

(b)(8 points) For all positive integers n and every $\bar{x} \in \mathbb{Z}/n$, one has $\bar{x}^{\varphi(n)+1} = \bar{x}$. Here $\varphi(n)$ denotes the Euler-phi function of n.

5. (14 points) Let b, n be positive integers with $GCD(b, n) = 1$. Prove that if the Jacobi symbol $\left(\frac{b}{n}\right)_2$ equals -1, then $\bar{b}$ is definitely *not* a square in $\mathbb{Z}/n$, whether or not n is prime.

6. (15 points) Let p be a prime with $p \equiv 3 \mod 4$, and let H be the subset of perfect squares in $(\mathbb{Z}/p)^\times$:

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

Show that the *squaring map*

$$\begin{array}{rccc} f: & H & \to & H \\ & f(\bar{x}) & = & \bar{x}^2 \end{array}$$

is a *bijection* from H to H, that is, f is one-to-one and onto (or injective and surjective, or a one-to-one correspondence).