T-79.503 Foundations of Cryptology
Homework 10
November 19, 2003

1. (Stinson 5.24) Suppose throughout this question that p is an odd prime and $\gcd(a,p) = 1$.

   a) Suppose that $i \geq 2$ and $b^2 \equiv a \pmod{p^{i-1}}$. Prove that there is a unique $x \in \mathbb{Z}_p^i$, such that $x^2 \equiv a \pmod{p^i}$ and $x \equiv b \pmod{p^{i-1}}$. Describe how this x can be computed efficiently.

   b) Illustrate your method in the following situation: starting with the congruence $6^2 \equiv 17 \pmod{19}$, find square roots of 17 modulo 19^2 and modulo 19^3.

2. (exam 8 Jan 2002) The module is $2002 = 2 \times 7 \times 11 \times 13$. Compute some nontrivial solution to the congruence

$$x^8 \equiv 1 (\bmod 2002),$$

   that is, a solution different from ± 1 modulo 2002.

3. (exam 4 Sept 2002) The module is $2002 = 2 \times 7 \times 11 \times 13$.

   a) What is the number of solutions of the congruence

$$x^4 \equiv 9 \pmod{2002}$$

   b) What is the number of solutions of the congruence

$$x^9 \equiv 4 \pmod{2002}$$

4. Compute

$$2^{120} (\bmod 122183).$$

   Then using the $p-1$ method, attempt to factor 122183.

5. Suppose that $n = 84773093$ and $b = 37869107$ in the RSA Cryptosystem. Using Wiener's Algorithm, attempt to factor n. If you succeed, determine the secret exponent a and $\phi(n)$.

6. The integers 26945 and 459312 are square roots of the integer 80833 modulo 540143. Compute the prime factors of 540143.

7. Bob and Bart are using the Rabin Cryptosystem. Bob's modulus is $n_1 = 2183$ and Bart's modulus is $n_2 = 2173$. Alice wants to encrypt an integer x, $0 < x < 2173$, to both of them. She sends ciphertext $y_1 = 1111$ to Bob and the ciphertext $y_2 = 2027$ to Bart. Determine x. (You can ignore the fact that the prime factors of the moduli are not congruent to 3 (mod 4) as usually is the case in Rabin cryptosystem. Also, you should find the solution without factoring the moduli.)