T-79.503 Foundations of Cryptology
Homework 9
November 12, 2003

1. a) Use the square-and-multiply algorithm to compute $2^{615} \bmod 667$.
   b) Determine $2^{-1} \bmod 667$. Compare this with a) and explain the result.

2. (Stinson 5.14) Prove that RSA Cryptosystem is not secure against a chosen ciphertext attack. In particular, use the multiplicative property of RSA Cryptosystem to decrypt a given ciphertext y by obtaining the decryption $\hat{x}$ of a different ciphertext $\hat{y}$.

3. A prime p is said to be a *safe prime* if $(p-1)/2$ is a prime.

   a) Let p be a safe prime, that is, $p = 2q + 1$ where q is a prime. Prove that an element in $\mathbb{Z}_p$ has multiplicative order q if and only if it is a quadratic residue and not equal to 1 mod p.
   b) The integer 08012003 (which is a date of last January's exam) is a safe prime, since 4006001 is a prime. Find some element of multiplicative order 4006001 in $\mathbb{Z}_{8012003}$.

4. If a composite integer n, $n > 1$, passes the Solovay-Strassen primality test with the test value $a \in \mathbb{Z}_n$, then n is called *Euler pseudo-prime* to the base a.

   a) Is 21 Euler pseudo-prime to the base 2?
   b) Is 33 Euler pseudo-prime to the base 2?

5. (Stinson 5.20) Evaluate the following Jacobi symbols using the four properties presented in Section 5.4. You should not do any factoring other than dividing out powers of 2.

$$\left(\frac{610}{987}\right), \left(\frac{20964}{1987}\right).$$

6. Let $n = pq$, where p and q are primes. We can assume that $p > q > 2$ and we denote $d = \frac{p-q}{2}$ and $x = \frac{p+q}{2}$. Then $n = x^2 - d^2$.

   a) Show that if $d < \sqrt{p+q}$ then x can be computed by taking the square root of n and by rounding the result up to the nearest integer.
   b) Test the method described in a) (if you have a calculator available) for $n = 4007923$ to determine x, and further to determine p and q.