T-79.5501 Cryptology
Homework 8
March 20, 2007

1. (Stinson 5.10) Suppose that $n = pq$ where p and q are distinct odd primes and $ab \equiv 1(\bmod (p-1)(q-1))$. The RSA encryption operation is $e(x) = x^b \bmod n$ and the decryption operation is $d(y) = y^a \bmod n$. In the text-book it is proved that $d(e(x)) = x$ if $x \in \mathbb{Z}_n^*$. Prove that the same statement is true for any $x \in \mathbb{Z}_n$.

2. (Stinson 5.14) Prove that RSA Cryptosystem is not secure against a chosen ciphertext attack using the following steps.
   (a) First, show that the encryption operation is multiplicative, that is, $e_K(x_1 x_2) = e_K(x_1)e_K(x_2)$, for any two plaintexts x_1 and x_2.
   (b) Next, use the multiplicative property to construct an example how you can decrypt a given ciphertext y by obtaining the decryption $\hat{x}$ of a different (but related) ciphertext $\hat{y}$.

3. (a) Evaluate the Jacobi symbol
$$\left(\frac{801}{2005}\right).$$
   You should not do any factoring other than dividing out powers of 2.
   (b) Let n be a composite integer and a an integer such that $1 < a < n$. Then n is called *Euler pseudoprime* to the base a if
$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \,(\mathrm{mod} n).$$
   Show that 2005 is an Euler pseudoprime to the base 801.

4. 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) for $n = 4007923$ to determine x, and further to determine p and q.

5. (a) Find all square roots of 1 modulo 4453.
   (b) 2777 is a square root of 3586 modulo 4453. Find all square roots of 3586 modulo 4453.

6. A prime p is said to be a *safe prime* or *Sophie Germain 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 is a safe prime, since 4006001 is a prime. Find some element of multiplicative order 4006001 in $\mathbb{Z}_{8012003}$.