T-79.503 Fundamentals of Cryptology
Homework 9
November 18, 2004

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. Alice is using the RSA Cryptosystem and her modulus is $n = pq = 167 \times 2003 = 334501$. Decrypt the ciphertext $y = 2003$.

3. 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.

4. (Stinson 5.14) Show that RSA encryption is multiplicative, that is, $e_K(x_1x_2) = e_K(x_1)e_K(x_2)$, for each $x_1,\ x_2 \in \mathcal{P}$. Using this property, prove that RSA Cryptosystem is not secure against a chosen ciphertext attack. In particular, show that an attacker can decrypt a given ciphertext $y$ by obtaining the decryption $\hat{x}$ of a different ciphertext $\hat{y}$.

5. 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 is a safe prime, since 4006001 is a prime. Find some element of multiplicative order 4006001 in $\mathbb{Z}_{8012003}$.