T-79.5501 Cryptology
Homework 9
November 24 & 25, 2005

1. (Stinson): This exercise illustrates another example of a protocol failure (due to Simmons) involving *RSA*; it is called the *common modulus* protocol failure. Suppose Bob has an *RSA cryptosystem* with modulus n and encryption exponent b_1, and Charlie has an *RSA Cryptosystem* with (the same) modulus n and encryption exponent b_2. Suppose also that $\gcd(b_1, b_2) = 1$. Now, consider the situation that arises if Alice encrypts the same plaintext x to send it to both Bob and Charlie. Thus, she computes $y_1 = x^{b_1} \bmod n$ and $y_2 = x^{b_2} \bmod n$ and then she sends y_1 to Bob and y_2 to Charlie. Suppose Oscar intercepts y_1 and y_2, and performs following computations:

   Input: n, b_1, b_2, y_1, y_2

   i) Compute $c_1 = b_1^{-1} \bmod b_2$
   ii) Compute $c_2 = (c_1 b_1 - 1)/b_2$
   iii) Compute $x_1 = y_1^{c_1}(y_2^{c_2})^{-1} \bmod n$

   (a) Prove that the value x_1 computed in step iii) is in fact Alice's plaintext, x. Thus Oscar can decrypt the message Alice sent, even though the cryptosystem may be "secure".
   (b) Illustrate the attack by computing x by this method if $n = 18721$, $b_1 = 43$, $b_2 = 7717$, $y_1 = 12677$ and $y_2 = 14702$.

2. Compute all square roots of 2 modulo $343 = 7^3$.

3. 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 $n = x^2 - d^2$. Attempt to factor $n = 400219845261001$ by searching for small non-negative integers t such that $x^2 - n = (\lceil\sqrt{n}\rceil + t)^2 - n$ is a perfect square. (This is a simple form of the Quadratic Sieve method. See also Homework 7, Problem 6, where this factorisation method works for $t = 0$.)

4. 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 $\mathbb{Z}_{8012003}$.

5. Suppose that $n = 355044523$ is the modulus and $b = 311711321$ is the public exponent in the *RSA Cryptosystem*. Using Wiener's Algorithm, attempt to factor n. If you succeed, determine also the secret exponent a and $\phi(n)$.