T-79.5501 Cryptology
Homework 9
March 27, 2007

1. 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 8, Problem 4, where this factorisation method works for $t = 0$.)

2. The integers 26945 and 459312 are square roots of the integer 80833 modulo 540143. Based on this information find some nontrivial integer divisors of 540143.

3. It is given that

$$2^{4!} \equiv 1655213 \, (\mathrm{mod} 15122003).$$

   Use the Pollard $p - 1$ algorithm to find a nontrivial divisor of 15122003.

4. The integer $n = 89855713$ is known to be a product of two primes. Further, it is given that $\phi(n) = 89836740$. Determine the factors of n.

5. (Stinson 5.30) Suppose that Bob has carelessly revealed his decryption exponent to be $a = 14039$ in an *RSA Cryptosystem* with public key $n = 36581$ and $b = 4679$. Implement the randomized algorithm to factor n given this information. Test your algorithm with the "random choices $w = 9983$ and $w = 13461$.

6. (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 $y_2 = 14702$.