SP12-CSE20 Discrete Mathematics
Homework 3 Solution

May 15, 2012

1 Cryptography

1.1 Problem 2.12

Suppose that N is a prime in the RSA protocol of Example 17. How can the spy Joe find the message M if he has e, N and the encrypted message $M^e \bmod N = C$?

Joe needs to decode the encrypted message, C, with help of d, since

$$C^d = (M^e \bmod N)^d = M^{ed} \bmod N = M \bmod N \tag{1}$$

However, to get the number d, Joe needs to calculate $f(N)$ first, since

$$ed \bmod f(N) \equiv 1 \tag{2}$$

Therefore the first step is to find $f(N)$. By definition, $f(N)$ is the number of integers within the range of $[1, N-1]$ which are coprime with N. As a result, when N is a prime, all positive integers smaller than N are coprime with it, so we have $f(N) = N - 1$.

The next step is to find the value of d, which is the inverse of $e \bmod f(N)$. He can use an extended *Euclidean* algorithm to calculate the inverse number as follows. To find d in order to satisfy $ed \equiv 1 \bmod f(N)$, it is necessary to have $gcd(e, f(N)) = 1$. Otherwise, assume $gcd(e, f(N)) = x > 1$, $e = k_e x$ and $f(N) = k_f x$. Since $ed \equiv 1 \bmod f(N)$, suppose $ed = k_{ed} f(N) + 1$, we have $ed = dk_e x = k_{ed} k_f x + 1$, thus $x(dk_e - k_{ed} k_f) = 1$. This contradicts

with the assumption that $x > 1$. As a result, we have $gcd(e, f(N)) = 1$. Theorem 5 on page NT-16 states that every common divisor of e and $f(N)$ (certainly including $gcd(e, f(N))$) can be expressed as $a_f f(N) + a_e e$, where both a_f and a_e are integers. How to find a_f and a_e is illustrated in Example 13 on page NT-19, where *Euclidean* algorithm is used again. After we get the value of a_f and a_e satisfying $a_f f(N) + a_e e = gcd(e, f(N)) = 1$, we have $a_e e \equiv 1 - a_f f(N) \equiv 1 \bmod f(N)$. As a result, a_e is the inverse of e with modulo $f(N)$ and we have $d = a_e$.

With help of d we can decrypt the received message C into the original message M using Equation 1.

1.2 Problem 2.13

Using the same numbers as in Example 17, decrypt the message 2.

As shown in Example 17, we have $N = 77$, $e = 13$ and $d = 37$. Now the received message $M^e \bmod N = 2$, the original message is computed as

$$(M^e)^d \bmod N = 2^{37} \bmod 77 = 137438953472 \bmod 77 = 51 \tag{3}$$

As a result, the original message is 51.

1.3 Problem 2.14

Consider the RSA protocol (Example 17). Suppose that $N = 5 \times 13$ and $e = 7$. What is d?

We have $N = p \times q = 5 \times 13$, thus $f(N) = (p-1)(q-1) = 4 \times 12 = 48$. Since we have $e = 7$ and $ed \equiv 1 \bmod (f(N) = 48)$, following the solution to Problem 2.12 we can easily generate the value of d. Specifically, we have $gcd(e, f(N)) = 1 = 7e - 1 \times f(N)$, while $7e \equiv 1 + f(N) \equiv 1 \bmod f(N)$. As a result, we have $7e \equiv 1 \bmod f(N)$ and $d = 7$.

1.4 Problem 2.15

Consider the RSA protocol (Example 17). Explain why d and e must both be chosen to be odd.

Suppose not and at least one of the two variables (e and d) is an even number, therefore the multiplication of d and e becomes an even number, suppose it to be $ed = 2k_{ed}$. We have $N = p \times q$ where both p and q are large prime numbers. As a result, $p \equiv q \equiv 1 \bmod 2$ and let $p = 2k_p + 1$ and $q = 2k_q + 1$, respectively. We have $f(N) = (p-1)(q-1) = 4k_pk_q$ and $ed \equiv 1 \bmod (f(N) = 4k_pk_q)$, thus $ed = k'_{ed}f(N) + 1 = 4k'_{ed}k_pk_q + 1$, and ed is an odd number. However, this contradicts to our earlier assumption that ed is an even number as $ed = 2k_{ed}$. As a result, we must have both d and e to be odd numbers in the RST protocol.