CS381 Exercise 8

Name: Zhang Yupeng

Student ID: 5130309468

1. If x=2 (mod 3) x=3 (mod 5) x=4 (mod 7), what is x?

Solution:

First,we have:

$$b_1 = 2, m_1 = 3; b_2 = 3, m_2 = 5; b_3 = 4, m_3 = 7.$$

So, we have $M = 105$ that:

$$M_1 = 35, M_1' = 2, M_2 = 21, M_2' = 1, M_3 = 15, M_3' = 1.$$

So, we have:

$x = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 4 \times 15 \times 1$(mod 3×5×7), $x = 263$(mod 105).

In conclusion,

$$x = 53 + 105k, k \in N$$

2. Compute $\phi(24) = \#\{?\}$, and $\phi(n)$ for $n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$

Solution:

$$\phi(24) = \phi(2^3 3^1) = 24 \times (1 - 1/2)(1 - 1/3) = 8$$

$$\phi(n) = n(1 - 1/p_1)(1 - 1/p_2)(1 - 1/p_3)$$

3. Prove：in ElGamal Signature Algorithm, the Verification test $g^m = y_a^R R^S$ (mod p) is valid.

Solution:

According to $S = r^{-1}(m - x_a R)$(mod p-1), we know $m = Sr + x_a R$(mod p-1).

Then we have $g^m = g^{Sr + x_a R}$ (mod p)

$= g^{Sr} g^{x_a R}$ (mod p)

$= (g^r)^S (g^{x_a})^R$ (mod p)

$= R^S y_a^R$ (mod p).

So, the verification test is valid.

4. ElGamal scheme uses a random integer r for each message,

A) what will happen if r is used twice in encryption?

Solution:

If r is used twice in encryption, then the adversary can use the same r to get the plaintexts.

When knowing r is the same as the r used the last time, since $S = my_b^r$ (mod p), the adversary can calculate the plaintexts m since the y_b is the public key.

B) what will happen if r is used twice in signature?

Solution:

If r is used twice in signature, then the adversary may fabricate the signature.

When knowing r is the same as the r used the last time, since $S = r^{-1}(m - x_a R)$(mod p-1), the adversary can get $x_a = R^{-1}(m - Sr)$(mod p-1).

By knowing x_a, the adversary can calculate R and S to fabricate the signature.

5. Is it possible to achieve confidentiality with DH key exchange? Is it possible to achieve authenticity with DH key exchange?

Solution:

1. DH key exchange can achieve confidentiality.

   Since finding discrete logarithms is a very difficult problem and is unrealistic to be done in reasonable time.

   Thus, the secrete key shared by the two ends is safe for them to encrypt the message, so the DH key can achieve confidentiality.

2. DH key exchange cannot achieve authenticity.

   Because the adversary can implement a man-in-the-middle attact that interfere the key transmission between the two ends and send the fabricated information and pretend to be the person who transmits the message.

   Thus, the DH key cannot get authenticity.