

# MAS 433 Tutorial 6

Wang Xueou (087199E16)

October 26, 2011

**Question 1** Solution:

Addition group is not secure. In group  $(Z_p, +)$ , we have the following key exchange protocol:

Alice	Bob
step 1: generate random number $r_a$	generate random number $r_b$
step 2: compute $Y_a = r_a \times g \bmod p$	compute $Y_b = r_b \times g \bmod p$
step 3: send $Y_a$ to Bob	send $Y_b$ to Alice
step 4: compute $K_a = r_a \times Y_b \bmod p$	compute $K_b = r_b \times Y_a \bmod p$

Then we have  $K_a = K_b = r_a \times r_b \times g \bmod p$ . However, this is not secure. The attacker may get  $Y_a$  and  $Y_b$ , then he just constructs a table  $T_1$  for  $r_a^i = i, i = 1, 2, \dots, p$  and compute  $K_a^i = r_a^i \times Y_b \bmod p$ . Then he tries  $r_b^j = j, j = 1, 2, \dots, p$  and compute  $K_b^j = r_b^j \times Y_a \bmod p$  until  $K_b^j = K_a^i$  for some  $i$  in  $T_1$ .

**Question 2** Solution:

$$n = 161 = 7 \times 23$$

$$\varphi(n) = (7 - 1) \times (23 - 1) = 132$$

Since  $e \cdot d = 1 \bmod \varphi(n)$ , we apply the extended Euclidean algorithm to  $(e, \varphi(n))$ :

$$\begin{aligned} 132 &= 26 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \\ 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (132 - 26 \times 5) \\ &= -2 \times 132 + 53 \times 5 \end{aligned}$$

So  $5^{-1} \bmod 132 \equiv 53$ , i.e.,  $d = 53$ .

To decrypt 3, we compute:

$$\begin{aligned} m &= c^d \bmod n \\ &= 3^{53} \bmod 161 \\ &= (3^{13})^4 \times 3 \bmod 161 \\ &= 101^4 \times 3 \bmod 161 \\ &= 144 \times 3 \bmod 161 \\ &= 110 \end{aligned}$$

The message is 110.

**Question 3** Solution:

**3.1.**

CBC mode: padded with random bits or constant bits.

SHA-1:

1. pad bit '1' to the end of the message
2. pad some zeros
3. pad the message length (in bits)
4. After padding, the overall length should be multiple of the block size

CMAC: pad by bit '1' followed by some zero bits

RSA:

1.  $m||o||r$ , where,  $m$  is the plaintext message of  $(n - k_0 - k_1)$  bits,  $o$  is some zeros of length  $k_1$ , and  $r$  is a random and secret number of  $k_0$  bits
2.  $X = (m||o) \oplus G(r)$ , where  $G$  is a random function
3.  $Y = H(X) \oplus r$ , where  $H$  is also a random function
4. Then encrypt the padded message  $X||Y$

**3.2.**

It is not secure to use small modulus  $n$ . RSA is based on the difficulty in factorizing large numbers. A small integer  $n$  is easy to be factorized so that an attacker can get  $p$  and  $q$  easily.

It is not secure to use small public key exponent  $e$ . There may be two situations:

-Attack 1 Example

Suppose  $e = 3$ , then for small  $m$  (say,  $m < n^{1/3}$ ), we have  $c = m^3 \bmod n = m^3$ . This means  $m$  can be recovered from  $c$  easily.

-Attack 2 Example

Suppose  $e = 3$  and  $m$  is large. The same message  $m$  is sent to 3 different receivers, then we have

$$c_1 = m^3 \bmod n_1 \quad (1)$$

$$c_2 = m^3 \bmod n_2 \quad (2)$$

$$c_3 = m^3 \bmod n_3 \quad (3)$$

Then we can find some  $m'$  such that  $m'$  satisfies (1), (2) and (3). From Chinese Remainder Theorem, we know  $m^3 \equiv m' \bmod n_1 n_2 n_3$ , i.e.,  $m^3$  can be known. Thus  $m$  can be recovered easily.

It is not secure to use small private key  $d$ . The value of  $d$  must be large for security reason. Otherwise the following attacks can be applied:

- Brute force attack: the size of  $d$  should be more than 128 bits. The complexity is  $2^{128}$
- Advanced attack:
  - If  $d < n^{0.25}$ ,  $d$  can be recovered from  $e$  and  $n$  easily.
  - If  $d < n^{0.292}$ ,  $d$  can be recovered from  $e$  and  $n$  easily.
  - It is conjectured that if  $d < n^{0.5}$ ,  $d$  can be recovered from  $e$  and  $n$  easily.

**Question 4** Solution:

**4.1.**

Let  $g = \gcd(p-1, q-1)$ . Since  $e \cdot d \equiv 1 \bmod(\lambda(n))$ , we can write  $e \cdot d = \beta\lambda(n) + 1$

Let  $x = c^d \bmod n$ , then

$$\begin{aligned} x \bmod p &= ((m^e)^d \bmod n) \bmod p \\ &= (m^e)^d \bmod p \\ &= m^{\frac{\beta(p-1)(q-1)}{g} + 1} \bmod p \end{aligned}$$

If  $m$  and  $p$  are co-prime, by Fermat's little theorem:  $m^{p-1} \bmod p = 1$ , then

$$\begin{aligned} x \bmod p &= m^{\frac{\beta(p-1)(q-1)}{g} + 1} \bmod p \\ &= (m^{p-1} \bmod p)^{\frac{\beta(q-1)}{g}} m \bmod p \\ &= m \bmod p \end{aligned} \quad (4)$$

If  $m$  is a multiple of  $p$ , then

$$\begin{aligned} x \bmod p &= m^{\frac{\beta(p-1)(q-1)}{g} + 1} \bmod p \\ &= 0 \\ &= m \bmod p \end{aligned} \quad (5)$$

From (4) and (5), we have:

$$x \equiv m \bmod p \quad (6)$$

Similarly:

$$x \equiv m \pmod{q} \quad (7)$$

From (6) and (7) and Chinese Remainder Theorem:

$$x \equiv m \pmod{pq} = m$$

**4.2.**

$$\begin{aligned} n &= 161 = 7 \times 23 \\ \lambda(n) &= \frac{(7-1) \times (23-1)}{\gcd(7-1, 23-1)} = \frac{6 \times 22}{2} = 66 \end{aligned}$$

Since  $e \cdot d \equiv 1 \pmod{\lambda(n)}$ , we apply the extended Euclidean algorithm to  $(e, \lambda(n))$ :

$$\begin{aligned} 66 &= 13 \times 5 + 1 \\ 1 &= 66 - 13 \times 5 \end{aligned}$$

So  $5^{-1} \pmod{66} \equiv -13 \pmod{66} = 53$ , i.e.,  $d = 53$ .

To decrypt 3, we compute:

$$\begin{aligned} m &= c^d \pmod{n} \\ &= 3^{53} \pmod{161} \\ &= (3^{13})^4 \times 3 \pmod{161} \\ &= 101^4 \times 3 \pmod{161} \\ &= 144 \times 3 \pmod{161} \\ &= 110 \end{aligned}$$

The message is 110.

**Question 5** Solution:

**5.1.** If they share the same modulus, each user can factorize  $n$  easily from  $e_i$  and  $d_i$ . Then each user can find the private keys of other users.

-Factorize  $n$  from  $e$  and  $d$

1) Since  $e \cdot d \equiv 1 \pmod{\varphi(n)}$ ,

$$e \cdot d - 1 = \beta(p-1)(q-1),$$

we know that  $e \cdot d - 1$  is even.

2) Randomly select an integer  $x$ , compute

$$y = x^{(e \cdot d - 1)/2} \pmod{n}$$

3) We know that  $x^{e \cdot d - 1} \pmod{n} = x^{\beta \varphi(n)} \pmod{n} = 1$  by Euler's Theorem.

4) from 2) and 3), we know that

$$y^2 = 1 \pmod{n}$$

Thus  $\gcd(y-1, n)$  gives a factor of  $n$  if  $y \not\equiv \pm 1 \pmod{n}$ .

## 5.2.

Suppose

$$c_A = m^{e_A} \pmod{n}$$

$$c_B = m^{e_B} \pmod{n}$$

Now we use the extended Euclidean Algorithm to find  $a$  and  $b$  such that  $a \times e_A + b \times e_B = 1$ . In fact, one of  $a$  and  $b$  must be negative, and suppose  $a$  is negative (It is similar if  $b$  is negative). We can get

$$\begin{aligned} c_A^a \times c_B^b &= (m^{e_A} \pmod{n})^a \times (m^{e_B} \pmod{n})^b \\ &= m^{a \times e_A + b \times e_B} \\ &= m \end{aligned} \tag{8}$$

In (8), we have  $a$  is negative, so

$$\begin{aligned} (m^{e_A} \pmod{n})^a &= c_A^a \\ &= (c_A^{-1})^{-a} \end{aligned}$$

where  $c_A^{-1}$  is the inverse of  $c_A \pmod{n}$ .

**Question 6** Solution:

### 6.1.

$$\begin{aligned} p - q &= 2v \\ p^2 - pq &= 2pv \\ p^2 - 2pv &= n \\ p^2 - 2pv + v^2 &= n + v^2 \\ (p - v)^2 &= n + v^2 \\ p - v &= \sqrt{n + v^2} \quad (p \gg v) \\ p &= v + \sqrt{n + v^2} \end{aligned}$$

Then we try all the possible values of  $v$ . If we guess  $v$  correctly,  $\sqrt{n + v^2}$  should be an integer.

### 6.2. $p = v + \sqrt{n + v^2}$

Try  $v = 1, 2, 3, \dots, 9$ , when  $v = 9$ ,

$$\begin{aligned} p &= 9 + \sqrt{2189284635403183 + 9^2} \\ &= 46789801 \\ q &= n/p \\ &= 46789783 \end{aligned}$$

**Question 7** Solution:

1.  $m = \lfloor \sqrt{n} \rfloor = 506, Q(x) = (m + x)^2 - n$
2. set  $B = 31$ , the factor base is  $\{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$

3.

$$x = -3 \rightarrow Q(x) = -3952 = (-1) \times 2^4 \times 13 \times 19$$

$$x = -2 \rightarrow Q(x) = -2495 = (-1) \times 5 \times 19 \times 31$$

$$x = -1 \rightarrow Q(x) = -1936 = (-1) \times 2^4 \times 11^2$$

$$x = 1 \rightarrow Q(x) = 88 = 2^3 \times 11$$

$$x = 5 \rightarrow Q(x) = 4160 = 2^6 \times 5 \times 13$$

$$x = 10 \rightarrow Q(x) = 9295 = 5 \times 11 \times 13^2$$

$$x = 13 \rightarrow Q(x) = 12400 = 2^4 \times 5^2 \times 31$$

4. Take  $A = \{x = -3, -2, 5, 13\}$

$$5. y^2 = Q(-3) \times Q(-2) \times Q(5) \times Q(13) = (-1)^2 \times 2^{14} \times 5^4 \times 13^2 \times 19^2 \times 31^2$$

$$\Rightarrow y = (-1) \times 2^7 \times 5^2 \times 13 \times 19 \times 31 = -91105 \bmod 256961$$

$$6. z = (m - 3) \times (m - 2) \times (m + 5) \times (m + 13) = 75319 \bmod 256961$$

$$\gcd(75319 + 91105, 256961) = 293$$

$$\gcd(75319 - 91105, 256961) = 877$$

$$\text{So } n = 293 \times 877$$

**Question 8** Solution:

We have  $c_1 = 10, c_2 = 159$ . We use extended Euclidean Algorithm to find  $c_1^{-1}$ .

$$\begin{aligned} 227 &= 22 \times 10 + 7 \\ 10 &= 1 \times 7 + 3 \\ 7 &= 2 \times 3 + 1 \\ 1 &= 7 - 2 \times 3 \\ &= 7 - 2 \times (10 - 1 \times 7) \\ &= -2 \times 10 + 3 \times 7 \\ &= -2 \times 10 + 3 \times (227 - 22 \times 10) \\ &= -68 \times 10 + 3 \times 227 \end{aligned}$$

$$\text{So } 10^{-1} = -68 \bmod 227 = 159$$

To decrypt  $(c_1, c_2)$ , we compute

$$\begin{aligned} m &= c_1^{-x} \cdot c_2 \bmod p \\ &= 10^{-15} \cdot 159 \bmod 227 \\ &= 159^{15} \cdot 159 \bmod 227 \\ &= 7 \end{aligned}$$

The plaintext is 7.