MAS 433 Tutorial 7

Wang Xueou (087199E16)

November 9, 2011

Question 1 Solution:
Let $m' = m + k \cdot n$, then

$$(m')^d \bmod n = (m + k \cdot n)^d \bmod n = (m^d + \sum_{i=1}^{d-1} m^{d-i}(k \cdot n)^i + (k \cdot n)^d) \bmod n = m^d \bmod n = s$$

Thus, without hashing, m can be modified to be $m' = m + k \cdot n, \forall k \in Z$

Question 2 Solution:
2.1
If $s = 0$, then

$$(H(M) - xr)K^{-1} \bmod p - 1 = 0$$

Since K^{-1} is not zero, $H(M) - xr \bmod p - 1 = 0, \Rightarrow H(M) \equiv xr (\bmod p - 1)$. If $r, H(M)$ is known, we can compute x. If x is coprime to $p - 1$, we have a unique solution; otherwise, we try several solutions.

2.2
Let $r = g^k \bmod p$, then

$$s_1 = (H(m_1) - xr)k^{-1} \bmod p - 1$$
$$s_2 = (H(m_2) - xr)k^{-1} \bmod p - 1$$

In this linear system, we have 2 unknowns: x, k and 2 equations. So this system can be solved and we can get

$$s_2 H(m_1) - s_1 H(m_2) = xr(s_2 - s_1) \bmod p - 1$$

2.3
We have

$$\begin{aligned} r_i &= g^{k_i} \bmod p \\ r_{i+1} &= g^{k_{i+1}} \bmod p \end{aligned}$$

Then

$$\begin{aligned} k_{i+1} &= k_i + a \\ s_i &= ((H(m_i) + xr_i)k_i^{-1}) \bmod p - 1 \\ s_{i+1} &= ((H(m_{i+1}) + xr_{i+1})k_{i+1}^{-1}) \bmod p - 1 \end{aligned}$$

We now have 3 unknowns, k_i, k_{i+1}, x and 3 equations, so we can solve the system and get x.

2.4
We have

$$\begin{aligned} r_i &= g^{k_i} \bmod p \\ r_{i+1} &= g^{k_{i+1}} \bmod p \\ r_{i+2} &= g^{k_{i+2}} \bmod p \end{aligned}$$

Then

$$\begin{aligned} s_i &= ((H(m_i) + xr_i)k_i^{-1}) \bmod p-1 \\ s_{i+1} &= ((H(m_{i+1}) + xr_{i+1})k_{i+1}^{-1}) \bmod p-1 \\ s_{i+2} &= ((H(m_{i+2}) + xr_{i+2})k_{i+2}^{-1}) \bmod p-1 \\ k_{i+1} &= k_i + a \\ k_{i+2} &= k_i + 2a \end{aligned}$$

We now have 5 unknowns, $k_i, k_{i+1}, k_{i+2}, a, x$ and 5 equations, so we can solve the system and get x.

Question 3 Solution:
3.1
If the secret integer k is reused, then

$$r = (g^k \bmod p) \bmod q$$

Then we have

$$\begin{aligned} s_1 = (k^{-1}(H(m_1) + xr)) \bmod q \\ s_2 = (k^{-1}(H(m_2) + xr)) \bmod q \end{aligned}$$

We have 2 unknowns, k, x and 2 equations, so we can solve the linear system to get x.

3.2
If $s = k^{-1}(H(m) - xr) \bmod q$, then the signature verification can be modified as:

$$\begin{aligned} \text{Calculate } u1 &= H(m)s^{-1} \bmod q \\ \text{Calculate } u2 &= rs^{-1} \bmod q \\ \text{Calculate } v &= ((g^{u1}y^{-u2}) \bmod p) \bmod q \end{aligned}$$

Then we check $v \stackrel{?}{=} r$

3.3
Let $t = aq + b$, i.e., $b = t \bmod q$, and let $p - 1 = k \cdot q$, then

$$g^t \bmod p = h^{\frac{p-1}{q} \cdot t} \bmod p = h^{k \cdot t} \bmod p = h^{k\cdot(aq+b)} \bmod p = h^{a(k\cdot q)+kb} \bmod p = h^{p-1}h^{kb} \bmod p = h^{kb} \bmod p = g^b \bmod p$$

$$g^{t \bmod q} \bmod p = g^b \bmod p$$

Thus, $g^t \bmod p = g^{t \bmod q} \bmod p$

Question 4 Solution:
4.1
If the attacker does not have the capability to modify the internet traffic, it is secure. If the attacker can modify the internet traffic, he or she can launch the man-in-the-middle attack to modify the public key.

4.2
If the public key certificate is invalid, the keys are no longer secure anymore. The attacker may launch the man-in-the-middle attack to decrypt the communication between users.

Question 5 Solution:
There is no unconditionally secure public key cryptosystem. In public key cryptosystem, everyone knows the public key. So if the computing power is unlimited, we can always recover the private key.

Question 6 Solution:
6.1.
Let $C = (c_1, c_2)$, then after receiving C:

- S_1 computes $w_1 = (c_1)^{x_1} \bmod p$
- S_2 computes $w_2 = (c_2)^{x_2} \bmod p$
- S_3 computes $w_3 = (c_3)^{x_3} \bmod p$
- The message is decrypted as: $(w_1 \cdot w_2 \cdot w_3)^{-1} \cdot c_2 \bmod p = m$

6.2.

- x_1, x_2 are given to server S_1
- x_2, x_3 are given to server S_2
- x_1, x_3 are given to server S_3

Let $C = (c_1, c_2)$, then after receiving C:

- If only S_1, S_2 are available, then
  - S_1 computes $w_1 = (c_1)^{x_1} \bmod p$
  - S_2 computes $w_2 = (c_1)^{x_2} \bmod p; w_3 = (c_1)^{x_3} \bmod p$
  - The message is decrypted as: $(w_1 \cdot w_2 \cdot w_3)^{-1} \cdot c_2 \bmod p = m$
- If only S_1, S_3 are available, then
  - S_1 computes $w_1 = (c_1)^{x_1} \bmod p; w_2 = (c_1)^{x_2} \bmod p$

- S_3 computes $w_3 = (c_1)^{x_3} \bmod p$
- The message is decrypted as: $(w_1 \cdot w_2 \cdot w_3)^{-1} \cdot c_2 \bmod p = m$

- If only S_2, S_3 are available, then
  - S_2 computes $w_2 = (c_1)^{x_2} \bmod p; w_3 = (c_1)^{x_3} \bmod p$
  - S_3 computes $w_1 = (c_1)^{x_1} \bmod p$
  - The message is decrypted as: $(w_1 \cdot w_2 \cdot w_3)^{-1} \cdot c_2 \bmod p = m$

Question 7 Solution:

7.1.

The entropy of each key bit is

$$-(0.95 \times \log_2 0.95 + 0.05 \times \log_2 0.05) = 0.286396957$$

7.2

The entropy of the key is

$$0.286396957 \times 64 = 18.3294052$$

7.3

The probability that 64 bits in a key with values '1' is

$$0.95^{64} = 0.0375241392$$

7.4

The probability that at least 63 bits in a key with values '1' is

$$\binom{64}{63} 0.95^{63} \times 0.05 + 0.95^{64} = 0.16392124$$

7.5

The probability that at least 62 bits in a key with values '1' is

$$\binom{64}{62} 0.95^{62} \times 0.05^2 + \binom{64}{63} 0.95^{63} \times 0.05 + 0.95^{64} = 0.373474328$$

7.6

The probability that at least 61 bits with values '1' is

$$\binom{64}{61} 0.95^{61} \times 0.05^3 + \binom{64}{62} 0.95^{62} \times 0.05^2 + \binom{64}{63} 0.95^{63} \times 0.05 + 0.95^{64} = 0.601409265$$

7.7

The number of keys having at least 61 bits with values'1' is

$$\binom{64}{61} + \binom{64}{62} + \binom{64}{63} + 1 = 43745 \approx 2^{15.4168305}$$

7.8

After trying $2^{15.4168305}$ keys, the probability to recover the secrete key is 0.601409265. The entropy of the key is $18.3294052 \sim \log_2 2^{15.4168305}$. This means the entropy of the secrete key is close to the complexity of brute force attack.