Problem 1. Lamport one-time signature scheme

1. Lamport signature scheme can be built from any cryptographically secure one-way function, usually a hash function. It can be divided into three parts.

   (a) **Key pair generation:**
   Let k be a positive integer and let $P = \{0,1\}^k$ be set of messages. Let $f : Y \to Z$ be a one-way function. For $1 \leq i \leq k$ and $j \in \{0,1\}$ the signer chooses $y_{i,j} \in Y$ randomly and computes $z_{i,j} = f(y_{i,j})$. The private key K consists of $2k$ values $y_{i,j}$, and the public key consists of values $z_{i,j}$.

   (b) **Signature:**
   Let $m = m_1, m_2, ..., m_k \in \{0,1\}^k$ be a message. The signature is

   $$sig(m_1, ..., m_k) = (y_{1,m_1}, ..., y_{k,m_k}) = (s_1, ..., s_k)$$

   (c) **Verification:**
   The verifier validates a signature by checking that $f(s_i) = z_{i,m_i}$ for all $1 \leq i \leq k$

2. Benefits:

   (a) Based on Grover's algorithm, Lamport signatures would be secure in quantum secure system.

   (b) Lamport signatures can be built from any secure one-way function.

   Drawbacks:

   (a) The security of Lamport signatures is based on one way hash function, the length of its output and the quality of the input.

   (b) In practical cases, Lamport signatures needs to select larger element sizes and stronger hash functions to improve security, which is quite expensive.

3. According to the set up, for every time the same private key is used, k values out of $2k$ values of private key K is known. Therefore, the attackers can collect the knowledge of the private key until he can recover all $2k$ values of private key K.

4. Merkle tree, aka hash tree, is a tree data structure which every non-leaf node is labeled with the hash of the labels or values (in case of leaves) of its child nodes. Merkle tree allows efficient and secure verification of the contents of large data structures.

   Merkle tree can be used to serve as form of the public key of Lamport signature, so user can sign the message using root instead of generating key pairs every time. Compare to the original set up, this is more efficient because user can verify any future signatures with the knowledge of only one master hash.

Problem 2. Chaum-van Antwerpen signatures

1. (a) For each $r \equiv s^{e_1}\beta^{e_2} \mod p$, first e_1 has q different choices, then for e_2, it needs to satisfy

$$\beta^{e_2} \equiv \alpha^{xe_2} \equiv rs^{-e_1} \mod p$$

α is a generator of G, which is a subgroup of F_p^*, at least one value e_2 can be determined according to the above formula. Therefore, at least q ordered pairs $\langle e_1, e_2\rangle$ can be considered.

(b) Given

$$\begin{cases} r \equiv \alpha^i \equiv \alpha^{le_1+xe_2} \mod p \\ t \equiv \alpha^j \equiv \alpha^{ke_1+e_2} \mod p \end{cases}$$

Using little fermat's theorem, we can write as

$$i \equiv le_1 + xe_2 \mod p-1$$

$$j \equiv ke_1 + e_2 \mod p-1$$

Since $s \not\equiv m^x \mod p$, we can get $l \not\equiv kx \mod p-1$, so $(l-kx)^{-1}$ is unique. We can find a unique solution by solving equations below.

$$e_1 \equiv (i-xj)(l-kx)^{-1} \mod p-1$$

$$e_2 \equiv (ki-lj)(kx-l)^{-1} \mod p-1$$

(c) We've known that at least q pairs of $\langle e_1, e_2\rangle$, and Alice can only verify one of them, thus the probability of Alice accepts an invalid signature is less than $1/q$.

2. (a) On a valid signature we have

$$t_1 \equiv r_1^{x^{-1}} \equiv s^{e_1x^{-1}}\alpha^{e_2} \mod p$$

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv s^{e_1f_1x^{-1}} \mod p$$

(b) Using the same method from (a), we have

$$t_2 \equiv r_2^{x^{-1}} \equiv s^{f_1x^{-1}}\alpha^{f_2} \mod p$$

$$\left(t_2\alpha^{-f_2}\right)^{e_1} \equiv s^{e_1f_1x^{-1}} \mod p$$

We can find that

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$$

Since $s \not\equiv m^x \mod p$, we know

$$t_1 \equiv r^{x^{-1}} \equiv s^{e_1x^{-1}}\beta^{e_2x^{-1}} \not\equiv m^{e_1}\alpha^{e_2} \mod p$$

$$t_2 \not\equiv m^{f_1}\alpha^{f_2} \mod p$$

Therefore, only if Bob can show

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$$

ensures Alice that he is not trying to disavow a valid signature.

3. (a) Suppose that

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$$

This assumption is true with a possibility of $1/q$ when

$$s \equiv m^x \bmod p$$

$$t_1 \not\equiv m^{e_1}\alpha^{e_2} \text{ and } t_2 \not\equiv m^{f_1}\alpha^{f_2}$$

Therefore, we know the probability of the following is $1 - 1/q$.

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \not\equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$$

(b) Yes, if Bob doesn't follow the protocol, the probability of him recognized by Alice is $1 - 1/q$.

(c) Yes, Bob can convince Alice by showing

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$$

Since when q is large, the equality of two term can proves the forgery.

Problem 3. Simple Questions

1. Given $q = 101, p = 7879, \alpha = 170, x = 75, \beta = 4567, m = 52$

   (a) To sign the message with $k = 49$,

   $$r \equiv (170^{49} \bmod p) \bmod q \equiv 1776 \bmod 101 \equiv 59 \bmod 101$$
   $$s \equiv 49^{-1}(52 + 75 \times 59) \bmod q \equiv 79 \bmod 101$$

   (b) To verify, we have the triple $< m, r, s >=< 52, 59, 79 >$, compute

   $$v \equiv (170^{79^{-1}\times 52 \bmod 101} 4567^{79^{-1}\times 59 \bmod 101} \bmod 7879) \bmod 101 \equiv 59 \bmod 101$$

   Since $v = r$, we verified the signature.

2. First we need to find k, and then it's simple to recover x. Knowing

   $$\beta^r r^{s_1} \equiv \alpha^{m_1} \mod p$$
   $$\beta^r r^{s_2} \equiv \alpha^{m_2} \mod p$$

   Dividing two equations, we have

   $$\alpha^{m_1 - m_2} \equiv \alpha^{k(s_1 - s_2)} \mod p$$
   $$m_1 - m_2 \equiv k(s_1 - s_2) \mod p - 1$$
   $$-22425 \equiv 10915k \mod 31846$$
   $$k = 1165$$

   Since $gcd(r, p - 1) = 2$, we use

   $$s_1 \equiv k^{-1}(m_1 - xr) \bmod p - 1$$
   $$31396 \equiv 27855(8990 - 23972x) \bmod 31846$$
   $$8142 \equiv 7874x \bmod 31846$$
   $$x \equiv 7459 \bmod 31846$$