Homework 2 & 3

111061548 游鎮遠

1. (a) $p = 83$, $g = 16$, Z_{83}^*, public key $= (p, g, 59)$,
secret key $= (p, g, 29)$

Encrypt $m = 25$:

choose a random number k, $1 \le k \le p-2$, let $k = 2$,

$C = (C_1, C_2) = (g^k, my^k) \bmod 83 = (16^2, 25 \cdot 59^2) \bmod 83$

$= (7, 41)$ #

Decrypt $C = (56, 13)$:

$m = C_1^{-x} C_2 \bmod 83 = 56^{-29} \cdot 13 \bmod 83$

$= 56^{53} \cdot 13 \bmod 83 = 16$ #

1. (b) $p = 83$, $g = 16$, secret key $= (p, g, 29)$, $m = 25$, $k = 23$

$r = g^k \bmod p = 16^{23} \bmod 83$

$= 28$

$S = k^{-1}(m - rx) \bmod p-1$

$= 23^{-1}(25 - 28 \cdot 29) \bmod 83-1$

$= 23^{-1}(-787) \bmod 82$

$= 25 \cdot 33 \bmod 82$

$= 5$

#

2. (a) Compute the signature of $m = 9876543210$

$H(9876543210) = 9876543210^{31} \bmod 37 = 1$,

let $k = 2$.

$$r = (g^k \bmod p) \bmod q$$
$$= (41^2 \bmod 149) \bmod 37$$
$$= 42 \bmod 37$$
$$= 5$$

$$s = k^{-1}(h(m) + rx) \bmod q$$
$$= 2^{-1}(1 + 5 \cdot 26) \bmod 37$$
$$= 2^{35}(131) \bmod 37$$
$$= 19 \cdot 20 \bmod 37$$
$$= 10$$

for $m = 9876543210$, (r, s) is $(5, 10)$ #

2. (b) The condition $1 \le 12, 25 \le q-1$ holds.

$$t = s^{-1} \bmod q$$
$$= 25^{-1} \bmod 37$$
$$= 25^{35} \bmod 37$$
$$= 3$$

$$v = ((g^{h(m)} y^r)^t \bmod p) \bmod q$$
$$= ((41^{31} \cdot 144^{12})^3 \bmod 149) \bmod 37$$
$$= 65 \bmod 37$$
$$= 28.$$

since $v \neq r$, $(12, 25)$ isn't a valid signature of $m = 3248$ #

3.

In the "sequential" DL interactive proof system, the prover cannot obtain any information before interacting with the verifier, and is therefore considered a zero-knowledge system.

In contrast, in the "parallel" Fs interactive proof system, the prover can obtain information by monitoring the verifier's output, which violates the zero-knowledge property.

4.

To achieve this assurance, the authorities can use a technique called "proof of consistency."
Here's explanation of how it works:

① Before the voting scheme begins, all authorities, including A_i and A_j, agree on a common reference string or a public key that will be used in the scheme.

② Authority A_i computes their share $s_{i,j} = f_i(x_j)$ based on their secret value x_j and their function f_i. The share $s_{i,j}$ represents the partial result of the vote encryption or decryption process.

③ Authority A_i generates a proof of consistency to show that their share s_{ij} is consistent with all other shares sent to the other authorities. This proof is based on the cryptographic operations performed by A_i during the vote processing.

④ Authority A_i sends the share s_{ij} and the corresponding proof of consistency to A_j. The proof of cosistency provides evidence that A_i's share is derived correctly and is consistent with the shares generated by other authorities.

⑤ Aj verifies the proof of consistency provid by Ai. By using the common reference string or public key agreed upon earlier, Aj can perform the necessary cryptographic operations to validate that the share s_{ij} is indeed consistent with the shares received from other authorities.

⑥ If the proof of consistency is valid, Aj accepts the share s_{ij} as consistent and proceeds with their own computations. Otherwise, if the proof fails to validate, Aj can reject the share and take appropriate actions, such as requesting a new share from Ai or taking measures to ensure the integrity and consistency of the voting process.