Fundamentals of Cryptography

Homework 6

Sepehr Ebadi **9933243**

Question 1

To ensure Oscar's attack is successful, he needs to replace Bob's public key with his own private key. Once this substitution is done, Oscar can sign his message using his private key. During the verification process, Alice will not detect any issues with the message, as the signature will pass validation successfully due to the manipulated keys.

Question 2

1)

$$r = \alpha^{K_E} \bmod p, s = (x - d.r).{k_E}^{-1} \mod p-1, p = 97, \alpha = 23, \beta = 15, d = 67$$
$$t = \beta^r.r^s = \alpha^x \ ?$$
$$x = 17, k_E = 31\ , r = 23^{31} \bmod 97 = 87, s = (17 - 67.87).31 \bmod 96 = 20$$
$$t = 15^{87}.87^{20} \bmod 97 = 68 \rightarrow 23^{17} = 68 \rightarrow VALID$$

$$x = 17, k_E = 49\ , r = 23^{49} \bmod 97 = 74, s = (17 - 67.74).49 \bmod 96 = 3$$
$$t = 15^{74}.74^{3} \bmod 97 = 68 \rightarrow 23^{17} = 68 \rightarrow VALID$$

$$x = 85, k_E = 77\ , r = 23^{77} \bmod 97 = 84, s = (85 - 67.84).5 \bmod 96 = 29$$
$$t = 15^{84}.84^{29} \bmod 97 = 83 \rightarrow 23^{85} = 83 \rightarrow VALID$$

2)

$$\boldsymbol{(x1, r1, s1) = (22, 37, 33)}$$
$$t = 15^{37}.37^{33} \bmod 97 = 49, \alpha^{22} \bmod 97 = 49 \rightarrow 49 = 49 \rightarrow VALID$$

$$\boldsymbol{(x2, r2, s2) = (22, 37, 33)}$$
$$t = 15^{13}.13^{65} \bmod 97 = 54, \alpha^{82} \bmod 97 = 32 \rightarrow INVALID$$

Question 3

1)

$$r = (\alpha^{K_E} \bmod p) \bmod q, s = (h(x) + d.r).{K_E}^{-1} \bmod q$$
$$w = s^{-1} \bmod q, u1 = w.h(x) \bmod q, u2 = w.r \bmod q, v = (\alpha^{u1}.\beta^{u2} \bmod p) \bmod q$$
$$p = 59, q = 29, \alpha = 3, d = 23, \beta = 3^{23} \bmod p = 45\ , h(x) = 17, K_E = 25, r = 22, s = 7$$
$$w = 25, u1 = 19, u2 = 28, v = 22 \rightarrow VALID$$

2)

$$h(x) = 2, K_E = 13, r = 25, s = 2$$
$$w = 15, u1 = 1, u2 = 27, v = 25 \rightarrow VALID$$

3)

$$h(x) = 21, K_E = 8, r = 12, s = 19$$
$$w = 26, u1 = 24, u2 = 22, v = 12 \rightarrow VALID$$

Question 4

1)

To calculate the probability that at least two people share the same birthday, we can use the complementary probability approach. This involves first calculating the probability that no two people have the same birthday, and then subtracting this value from 1 to obtain the desired probability.

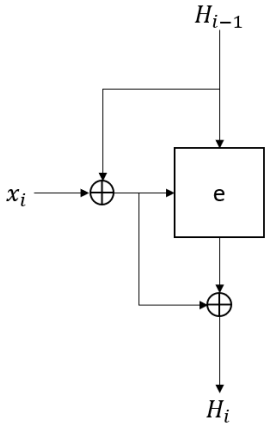
$$p'(k,n) = \left(1 - \frac{1}{n}\right) * \left(1 - \frac{2}{n}\right) * \ldots * \left(1 - \frac{k-1}{n}\right)$$
$$\prod_{i=1}^{t-1} e^{\frac{t}{n}} \rightarrow\ e^{\frac{k(k-1)}{2n}}$$
$$p(k,n) = 1 - p'(k,n)$$
$$p(k,n) = 1 - e^{\frac{k(k-1)}{2n}}$$

2)

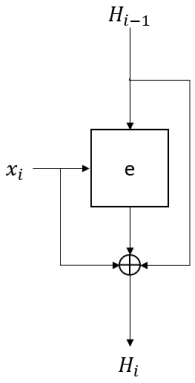
$$t = 2^{\frac{n+1}{2}} \sqrt{\ln\left(\frac{1}{1-\lambda}\right)}$$
$$n = 64 \rightarrow \approx\ 2^{32}\ inputs$$
$$n = 128 \rightarrow \approx\ 2^{64}\ inputs$$
$$n = 160 \rightarrow \approx\ 2^{160}\ inputs$$

Question 5

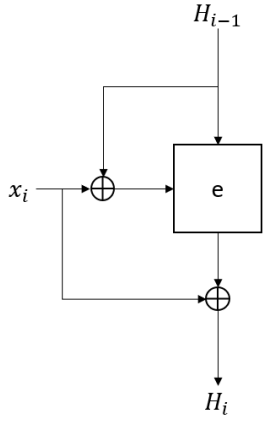
1)



2)



3)



Question 6

1)

In the Hirose algorithm, the output length is twice the block size of the block cipher. Therefore, the output length is 128 bits.

2)

Since the left and right halves are computed exactly the same way, the state space of the algorithm will be 2^{64}.

So to find one collision just need check 2^{64} states.

3)

check all possible states for xi so : brute-force and we can found a weak collision.

4)

When c≠0, the Hirose construction guarantees that the two halves of the hash output are generated differently. This minimizes the probability of them being identical and ensures that the full 128-bit entropy of the hash output is maintained.

Consequently, performing a second-preimage attack would require exploring the entire 128 space of potential outputs, which is beyond the reach of current computational capabilities. The robustness of the hash function relies on this high level of entropy to withstand such attacks effectively.