CS411-HW4

Ahmet Furkan Ün

December 10, 2023

Question 1

The C that we want to decrypt is calculated by the sender as

$$C \equiv (M)^e \pmod{N}$$

where M is the message. If we choose a random number r that is coprime to N and calculate a new ciphertext $\bar{C}$ as

$$\bar{C} \equiv C \cdot r^e \pmod{N}$$

If we can find the decrypted value of this C' it will actually become

$$\bar{M} \equiv \bar{C}^d \pmod{N}$$

$$\bar{M} \equiv (C \cdot r^e)^d \pmod{N}$$

$$\bar{M} \equiv (M^e \cdot r^e)^d \pmod{N}$$

$$\bar{M} \equiv M^{ed} \cdot r^{ed} \pmod{N}$$

$$\bar{M} \equiv M^{ed} \cdot r^{ed} \pmod{N}$$

We know that $e \cdot d \equiv 1 \mathrm{mod} \phi(n)$

$$\bar{M} \equiv M \cdot r \pmod{N}$$

$$M \equiv \bar{M} \cdot r^{-1} \pmod{N}$$

By choosing $r = 3$ and performing these steps, I found

$$\bar{M} = 468159415484066292784991909769767374368182423276237998883003719023296699874793396956032885876320683693156445 0$$

$$M = 156053138494688764261663969923255791456060807758745999627667906341098899958264465653186776286254402278977188150$$

Decoded M: "Bravo! You found it. Your secret code is 75416"

Question 2

For this question, I decided to use brute force method since the keyspace is small. Since r is an 8-bit number, it ranges from 0 to 255. The possible number of PINS are $pin \in [1000, 9999]$ which means there can be 9000 different pins. So I need to check 256 random number for every 9000 pins. The key space is $256 \cdot 9000 = 2304000 \approx 2^{21}$. By trying all values I found that
Pin: 1308 and R: 206

Question 3

It is computationally infeasible to find the key s. However, when I inspect the encryption, I realized that the space for random key k is only 2^{16}. Since the space is small, I can try exhaustive search for discrete logarithm problem here.

$$r \equiv g^k \text{ mod p}$$

$$t \equiv h^k \cdot m \text{ mod p}$$

If we found the random key k, we can easily calculate message m as

$$m \equiv (h^k)^{-1} \cdot t \text{ mod p}$$

$$m \equiv (h^{-1})^k \cdot t \text{ mod p}$$

By doing exhaustive search, I found the random key k: 31659.
After applying the above formula I found

$$\begin{aligned}\text{Message} =& 23793265938149667774278838370488440701778278036200113477119695808\\ & 07839402328800310735083651740104432905774\end{aligned}$$

Decoded message: Be yourself, everyone else is already taken.

Question 4

When I looked at the question, I realized that the r_1 and r_2 values are the same. This means that the same random key k is used in the encryption of two messages. Therefore the corresponding ciphertexts are actually (r, t_1) and (r, t_2)

$$r \equiv g^k \text{ mod p}$$

$$t_1 \equiv h^k \cdot m_1 \text{ mod p}$$

$$t_2 \equiv h^k \cdot m_2 \text{ mod p}$$

$$h^k \equiv t_1 \cdot m_1^{-1} \text{ mod p}$$

$$m_2 \equiv t_2 \cdot (h^k)^{-1} \text{ mod p}$$

$$m_2 \equiv t_2 \cdot (t_1 \cdot m_1^{-1})^{-1} \text{ mod p}$$

$$m_2 \equiv t_2 \cdot t_1^{-1} \cdot m_1 \text{ mod p}$$

By calculating the above formula for m_2, I found:

$$\begin{aligned}m_2 =& 14649973832333132475064077137516748006344032866803958320445974163\\ & 97312573349068862772492909917628719523259524263786509544653220 0\\ & 27674685847369116208450902659061483 0\end{aligned}$$

Decoded m_2: A person can change, at the moment when the person wishes to change.

Question 5

$$s_1 \equiv k_1^{-1} \cdot (H(m_1) + a \cdot r_1) \bmod q$$
$$s_2 \equiv k_2^{-1} \cdot (H(m_2) + a \cdot r_2) \bmod q$$
$$k_1 \equiv s_1^{-1} \cdot (H(m_1) + a \cdot r_1) \bmod q$$
$$k_2 \equiv 3k_1 \equiv s_2^{-1} \cdot (H(m_2) + a \cdot r_2) \bmod q$$
$$3s_1^{-1} \cdot (H(m_1) + a \cdot r_1) \equiv s_2^{-1} \cdot (H(m_2) + a \cdot r_2) \bmod q$$
$$3s_2 \cdot H(m_1) + 3s_2 \cdot a \cdot r_1 \equiv s_1 \cdot H(m_2) + s_1 \cdot a \cdot r_2 \bmod q$$
$$3s_2 \cdot a \cdot r_1 - s_1 \cdot a \cdot r_2 \equiv s_1 \cdot H(m_2) - 3s_2 \cdot H(m_1) \bmod q$$
$$a \cdot (3s_2 \cdot r_1 - s_1 \cdot r_2) \equiv s_1 \cdot H(m_2) - 3s_2 \cdot H(m_1) \bmod q$$
$$a \equiv (s_1 \cdot H(m_2) - 3s_2 \cdot H(m_1)) \cdot (3s_2 \cdot r_1 - s_1 \cdot r_2)^{-1} \bmod q$$

By putting all known variables in the last equation, I can easily calculate secret key a:

$$a = 22476888247905612413097953963453670523390618116947138589103652264 53$$