

**CSCI971 Advance Computer Security:  
Homework #7**

**Mei Wangzhihui  
2019124044**

## Problem 1

AE-secure  $\Leftrightarrow$  semantically secure under CPA and CI.

For the first cipher, assume an attacker who can perform CPA. He intercept the ciphertext  $c = E_1(k, m) = (E(k, m), H_1(m))$ . He can perform as many as CPA. We assume in CPA attack game. Adversary  $\mathcal{A}$  first send  $m_0, m_0$  to challenger  $\mathcal{C}$ , he get the ciphertext  $c = (E(k_0, m_0), H_1(m_0))$ . Then  $\mathcal{A}$  send  $m_0, m_1$  to  $\mathcal{C}$ , as  $E$  is CPA secure, so key has to be changed.  $\mathcal{A}$  get the ciphertext  $c = (E(k_1, m_0), H_1(m_0))$  or  $c = (E(k_1, m_1), H_1(m_1))$  based on  $b$ . Then if  $b = 1$ ,  $\mathcal{A}$  can easily differ the plaintext from the tag  $H_1(m_b)$ . So  $Adv_{CPA}(\mathcal{A}, \mathcal{E}) = 1/2$  is not negligible. Cipher1 is not CPA-secure, so it's not AE-secure.

For the second cipher, attacker can intercept the ciphertext  $(c, H_2(c))$ , so he can learn the mapping model of  $H_2$  function. So in CI attack game, Adversary  $\mathcal{A}$  can easily generate an valid ciphertext-tag pair  $(c_{atk}, H_2(c_{atk}))$ . Then Decryptor  $D_2(k, (c_{atk}, H_2(c_{atk}))) \neq \perp$ . So  $Adv_{CI}(\mathcal{A}, \mathcal{E})$  is not negligible. Cipher2 does not satisfy CI, so it's not AE-secure.

## Problem 2

Addition  $\mathbb{Z}_6^*$  is a cyclic group.

$$\mathbb{Z}_6^* = \{0, 1, 2, 3, 4, 5, 6\}$$

1 generate  $\{0, 1, 2, 3, 4, 5\}$

2 generate  $\{0, 2, 4\}$

3 generate  $\{0, 3\}$

4 generate  $\{0, 2, 4\}$

5 generate  $\{0, 1, 2, 3, 4, 5\}$

So the generators of  $\mathbb{Z}_6^*$  are 1, 5, the subgroups are  $\{0, 1, 2, 3, 4, 5\}$ ,  $\{0, 2, 4\}$ ,  $\{0, 3\}$

## Problem 3

Group under multiplication  $\mathbb{Z}_{13}^*$  is a cyclic group.

$$\mathbb{Z}_{13}^* = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$\langle 1 \rangle = \{1\}$$

$$\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$\langle 3 \rangle = \{1, 3, 9\}$$

$$\langle 4 \rangle = \{1, 3, 4, 9, 10, 12\}$$

$$\langle 5 \rangle = \{1, 5, 8, 12\}$$

$$\langle 6 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$\langle 7 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$\langle 8 \rangle = \{1, 5, 8, 12\}$$

$$\langle 9 \rangle = \{1, 3, 9\}$$

$$\langle 10 \rangle = \{1, 3, 4, 9, 10, 12\}$$

$$\langle 11 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$\langle 12 \rangle = \{1, 12\}$$

So subgroups are  $\{1\}$ ,  $\{1, 12\}$ ,  $\{1, 3, 9\}$ ,  $\{1, 5, 8, 12\}$ ,  $\{1, 3, 4, 9, 10, 12\}$ ,  $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

python codes:

---

```
for i in range(2,13):
    num=1
    cset = set()
    for j in range(1,20):
        num*=i
        cset.add(num % 13)
    print(i, cset)
```

---