Homework One

潘亦晟
515021910384

March 23, 2018

Problem 1.

Solution Cipher text: LFDPHLVDZLFRQTXHUHG
We can easily get the character frequency of the cipher text:

$$H:3, L:3, D:2, F:2, L:2, P:1, V:1, Z:1, R:1, Q:1, T:1, X:1, U:1, G:1$$

Since the two most frequent characters of the ciphertext are "H" and "L", we infer that "H" and "L" represents "E" and "I" in the plaintext correspondingly,Therefore,the shift method is

$$C = (M + 3) \mod 26$$

We can get the plaintext:

$$ICAMEISAWICONQUERED$$

Problem 2.

Solution (a) ciphertext : FSKWPYTJUMB
(b) plaintext: csfivetwoeightfive
(c) h

Problem 3.

Solution a)Encryption : $ciphertext = plaintext \oplus key$
Plaintext:

$$H(00111), E(00100), L(01011), L(01011), O(01110)$$

KEY:

$$X(10111), M(01100), C(00010), K(01010), L(01011)$$

Ciphertext:

$$Q(10000), I(01000), J(01001), B(00001), F(00101)$$

(b)Decryption: $plaintext = ciphertext \oplus key$
Ciphertext:

$$Q(10000), I(01000), J(01001), B(00001), F(00101)$$

KEY:

$$T(10011), Q(10000), U(10100), R(10001), I(01000)$$

Plaintext:

$$D(00011), Y(11000), D(11101), Q(10000), N(01101)$$

(c) We can get

$$M_1 \oplus KEY = C_1, M_2 \oplus KEY = C_2$$

Therefore,

$$(M_1 \oplus KEY) + (M_2 \oplus KEY) = M_1 \oplus M_2 = C_1 \oplus C_2$$

Problem 4.

Solution e can compute L_0,R_0 :

1. $L_2 = R_3 + f(K, L_3), R_2 = L_3$
2. $L_1 = R_2 + f(K, L_2), R_1 = L_2$
3. $L_0 = R_1 + f(K, L_1), R_0 = L_1$

Problem 5.

Solution a)The number of keys we have to try on average is

$$2^{56} \times 2^{56} \div 2 = 2^{111}$$

(b)If $K_1 = K_2$, 3DES will covert to DES

Problem 6.

Solution onvert the plaintext into binary form:

$$P = P_0P_1P_2P_3P_4P_5 = I(1000)A(0000)M(1100)B(0001)O(1110)B(0001)$$

Then

$$C_0 = E(K, P_0 \oplus IV) = P_0 \oplus IV + 1 = 1011(L)$$
$$C_1 = E(K, P_1 \oplus C_0) = C_0 \oplus P_1 + 1 = 1100(M)$$
$$C_2 = E(K, P_2 \oplus C_1) = C_1 \oplus P_2 + 1 = 0001(B)$$
$$C_3 = E(K, P_3 \oplus C_2) = C_2 \oplus P_3 + 1 = 0001(B)$$
$$C_4 = E(K, P_4 \oplus C_3) = C_3 \oplus P_4 + 1 = 0000(A)$$
$$C_5 = E(K, P_5 \oplus C_4) = C_4 \oplus P_5 + 1 = 0010(C)$$

Therefore, the ciphertext is

$$C = LMBBAC$$