# Assignment 1

QUESTION 1

Gen: the Key-Generation algorithm choose a key from the permutation of alphabet according to the uniform distribution.

Enc: given a key k is the permutation of alphabet, and a string of the letter. The encryption algorithm outputs the ciphertext by replace the letter with mapping letter in key.

Dec: given a key k is the permutation of alphabet and a ciphertext, the decryption algorithm outputs the plaintext by replacing the letter with the mapping letter in opposite way.

## QUESTION 2

For shift scheme, we just need one character of plaintext, we can calculate the number of shift, so we get the key.

For substitution scheme, we need a plaintext , which is a ASCII alphabet permutation. Then we can deduce the mapping relationship, which is the key.

For Vigenere scheme, we need a plaintext which the length is bigger than period of Dec. Then we can deduce the mapping relationship, which is the key.

## QUESTION 3

(a)

<1> shift:

Gen: the Key-Generation algorithm choose a key from [0 ,127] according to the uniform distribution. So k<= 127 and k>=0 .

Enc: given a key k and a string m from ASCII alphabet, the encryption algorithm outputs the ciphertext c = m + k mod 128.

Dec: given a key k and a ciphertext c, the decryption algorithm outputs the plaintext m = c – k mod 128.

<2> substitution:

Gen: the Key-Generation algorithm choose a key from the permutation of ASCII alphabet according to the uniform distribution.

Enc: given a key k is the permutation of ASCII alphabet, and a string of the letter. The encryption algorithm outputs the ciphertext by replace the letter with mapping letter in key.

Dec: given a key k is the permutation of alphabet and a ciphertext, the decryption algorithm outputs the plaintext by replacing the letter with the mapping letter in opposite way.

<3> Gen: the Key-Generation algorithm define the length of key t randomly. Then choose a string, which length is t, formed by the character from ANCSII alphabet according to the uniform distribution.

Enc: given a key k is the permutation of ASCII alphabet, and a string of the letter. For every t character, means that the period is t, the encryption algorithm outputs that c =m + k mod 128

Dec: given a key k is the permutation of ASCII alphabet, and a string of the letter. For every period t, the encryption algorithm outputs that plaintext

m = c - k mod 128

(B)

There is not essential difference with the ASCII alphabet and English alphabet, just the space is bigger. So the attack for scheme by English alphabet is almost same as the scheme by ASCII alphabet. We can using COA to break them.

For shift scheme, we just need one character of plaintext, we can calculate the number of shift, so we get the key.

For substitution scheme, we need a plaintext of ASCII alphabet permutation. Then we can deduce the mapping relationship.

For Vigenere scheme, we need a plaintext which the length is bigger than period. But we don`t know the period. So we need try to find the period.

## QUESTION 4

I think redefining the key space means that old key maps to the new key. So I set a function nGen, which give a key w uniformly. Then I set a function nEnc,

nEnc(w) = k. So

## QUESTION 5

(a) scheme is not perfectly secret. because:

Pr( M = m | C = c) = Pr(EncK (m) = c )

when m = 0 and c = 0, we can deduce k = 0 or 5

so Pr(EncK (0) = 0 ) = 2/6

because Pr(M = m) = 1/5

so Pr( M = m | C = c) Pr(M = m)

(a) is not perfect secret.

(b) scheme is perfect secret. According to Shannon`s Theorem, we can proof it.

At first, we can know |M| = |K| = |C| = 2l-1,

Second, because Enck(m) = m ⊕ (k || 0) = c ,so for any m, c ,there are unique (key || 0) = m⊕c

So (b) scheme is perfect secret.

## QUESTION 6

(a) if t = 1, every character int plaintext use the same key to encrypt, so

if t = 2 and t = 3, because A just use the first and second character, so the result when m=2 and m=2 is same. so

if the character of 1st ≠ 2nd and 1st – 2nd ≠ 1,the probability of correct is 1/2.

if the character of 1st = 2nd , the probability of correct is 1.

if 1st ≠ 2nd and 1st – 2nd = 1, the probability of correct is 0.

In a word,

(b) A` outputs m0 = aaa, m1 = abb, when given a ciphertext c, it outputs 0 if the first character = the third character or the first character = the second character of c.

in A`, if t = 1：

if t = 2, because the first and third character use the same key to encrypt, means that shift the same number. So the probability of correct is 0.

if t = 3: it is a perfect secret, So

In a word, the success probability of A` is:

## QUESTION 7

(a) <1> |K| = |M| = |C|=26 (alphabet)

<2> Pr(K=k) = 1/|K| = 1/26

<2> for any c,m ,the key = c – m mod 26.

so according to Shannon`s theorem and <1> <2> and <3>, the shift cipher under this condition is perfect secret.

<b> 26!

Accord to the perfect secret theorem , when |K| < |M| ,the scheme is not perfect secret.

The key space |K| = 26! When |K| >= |M|, (for the largest space, let |K| = |M|):

We can compute that the cipher space = 26! (the permutation of alphabet)

so

so

so this scheme is perfect secret.

<c> for each period t ,obviously, it is perfect secret. because:

<1> |M| = |K| = |K| = 26t

<2> Pr(K=k) = 1/26t

<3> for any m ,c , k = c – m

So according to Shannon`s theorem, it is perfect secret.

## QUESTION 8

According to the question, we can know that this scheme is perfect secret. So

So

Because scheme is perfect secret, K,C is independent.

So

According to the question:

So

In a word,