**111550130 李慕庭 – Quiz1**

**Problem 1**

1. 一張含有 文字, 螢幕擷取畫面, 數字, 字型 的圖片

   AI 產生的內容可能不正確。Frequency Analysis & Fill the table
2. a=17, b=45
3. If the encryption is based on substitution alphabets (for example, as 1-(b) ), then the word “created” includes two “e”, so we can find all patterns in ciphertext form as ABCDECF (A, B, C, D, E, F are mutually different alphabets), assume it is a correct mapping and try to decryption. Besides, we know “e” is most frequent alphabets in usual (by Table 2 in 1-(a) ), so we can reduce to a smaller possible mapping space. This method is frequency analysis with pattern matching.
4. *a* need to coprime with 95, therefore, number of possible *a*

*b* need to within range [0, 94], therefore, number of possible *b* = 95

Total size of key space = 72 \* 95 = 6840

In terms of nowadays’ computational ability, 6840 is a very small size.

Moreover, by frequency analysis as we did in problem 1-(a), we can fix some mapping and therefore reduce the size of key space significantly. By enumerating all possible keys and observing decryption result, we can find correct key easily.

1. The size of key space of Monoalphabetic Substitution Cipher is the number of possible permutations over [32, 126] alphabets = 95!

95! , approximately equal to . Even, we can compute possibles in a second, we still need around years to enumerate them all !

1. Two steps encryption

Step 1. Choose integers such that and

. Then, given plaintext , we encrypt it in first step by

Step 2. Use pseudo random generator to generate a key stream , we

encrypt output of first step by where are

-bit of respectively and the symbol is bitwise XOR.

is ciphertext of .

Criteria 1: This encryption consists of two steps encryption with different

method.

Criteria 2: In the first step of encryption, the frequency doesn’t change.

However, in the second step, the same alphabet might be XOR by different bits and thus change the frequency of each alphabet.

In this way, make frequency analysis attacks more difficult.

Criteria 3: Decryption

Step 1:

Step 2:

We can fully reverse ciphertext if we know and

**Problem 2**

1. *a* is valid if a is coprime with *n* . →Number of valid *a =*

*b* has to within range [0, n-1] → Number of possible *b* = *n*

The total number of possible keys =

1. Use the following table to list all elements

|  |  |
| --- | --- |
| Elements have multiplicative inverse | Multiplicative inverse |
| 1 | 1 |
| 7 | 13 |
| 11 | 11 |
| 13 | 7 |
| 17 | 23 |
| 19 | 19 |
| 23 | 17 |
| 29 | 29 |

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

AI 產生的內容可能不正確。(Calculating Process)1

1. 一張含有 文字, 螢幕擷取畫面, 字型 的圖片

   AI 產生的內容可能不正確。a=37, b=58, n=97

(Searching Process)

1. The way to decrypt affine encryption

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

AI 產生的內容可能不正確。Therefore,

(Calculating Process)

1. a = 17, b = 5, n = 83

一張含有 文字, 螢幕擷取畫面, 軟體, 字型 的圖片

AI 產生的內容可能不正確。Missing digits are 3 and 4 in first and second row respectively.

(searching process)