**Introduction to Information Security - HW1**

**分工:**

B10615036 黃泰明 : Encrypt

B10615045 陳尚富 : Decrypt

**開發環境**

macOS High Sierra Python3 using Visual Studio Code

**使用套件:**

sys, numpy, math

**程式說明:**

在處裡cipher前，先將輸入格式遵照作業一說明規定處理，並也只會處理符合規定長度格式的輸入。建立一個陣列裡面存放英文字母a~z，方便後續的解碼工作。

1. **Caesar cipher**

**Input:**

*Key*: 5

*Ciphertext*: ITDTZWGJXYFSIYMJSQJYLT

**Output:**

*Decrypt*: doyourbestandthenletgo

**說明**:

預先建立一個list alpha，裡面有a~z總共26個英文字母，這樣我們只需要取得字母的index再減去Key，就可以知道是移動到哪個index，這樣再利用預先建立的alpha就可以知道是哪一個字母。之後只需要再模26讓index維持再-25 ~25，就可以達到解碼的功能。

1. **Playfair cipher**

**Input:**

*Key*: 5

*Ciphertext*: IDWPQSDFTUGUFRKBHNFSDA

**Output:**

*Decrypt*: doyourbestandthenletgo

**說明:**

開一個一維陣列，先將沒有重複的Key字母加入。再利用26英文字母陣列，將沒有出現過的字母依序加入(不使用j)，再將此陣列重新塑形成5\*5的二微陣列。

之後就可以開始解碼。利用try, except來處理ciphertext只有基數的問題。

使用numpy的where來取得字母再playfair方陣中的位置。再來只要依照上課教過的規則就可以達成解碼。

1. **Vernam proposed the autokey system**

**Input:**

*Key*: 5

*Ciphertext*: QK[N[JPQDSE`QTKH\_MA\_NK

**Output:**

*Decrypt*:

**說明**:

這邊無法輸出任何東西，因為Ciphertext中有符號 “ ` “。假如將輸入改成 :

**Input:**

*key*: 5

*Ciphertext*: QK[N[JPQDSE

**Output**:

*Decrypt*: doyourbesta

就可以成功的解碼。程式邏輯部分，創建一個string將key加入，再利用這個string和Ciphertext互斥或 (Ciphertext的長度 – Key的長度) 個字母，就可以取得真正的Key。之後再利用這個string和Ciphertext互斥或，就可以解碼。

1. **Row transposition**

**Input:**

*Key*: 45362178

*Ciphertext*: ORGEEEUKGVENEPVPIGNI

**Output:**

*Decrypt*: keepgoingnevergiveup

**說明**:

先算出row transposition所需的陣列的col和row。Row的部分再做除法時需要無條件進位，所以import math來使用ceil函式。由於考慮到row的陣列可能不回填滿的問題，所以我先將陣列依照Ciphertext的長度，依序將row陣列會用到的位置填上’0’，填不滿的部分填上’1’。為了後續方便使用row陣列上的index，所以使用numpy的transpose，將其transpose再利用dictionary將其依照Key標上index。再來就只需要依照標好的index陸續填上Ciphertext，就將row的陣列做好了。由於標上index的dict是使用=，會直接更改到row陣列，所以只要將row陣列依照規則輸出，就可以解碼。

1. **Rail fence cipher**

**Input:**

*Key*: 2

*Ciphertext*: KEGIGEEGVUEPONNVRIEP

**Output:**

*Decrypt*: keepgoingnevergiveup

**說明**:

由於數學不太好，所以建一個陣列，裡面的內容先依照rail fence的形狀填好，我的話是字母的位置標上\*，其餘的標上1。假設key為3，會產生一個:

\* 1 1 1 \* 1 1

1 \* 1 \* 1 \* 1

1 1 \* 1 1 1 \*

的陣列。再來只要將\*字號的部分，將Ciphertext依照規則填入就得到了rail fence的陣列。再來就只需要依照規則再把填上的字母取出，就完成解碼。