資訊安全導論HW1

B10815044 謝鈞曜 加密

B10815057 廖聖郝 解密

### 加密

#### Caesar

先把key轉成整數，再將char根據key做位移



## Playfair

先將Key Table建出



對明文進行基本處理



根據字母相對的位置，做不同的加密，最後輸出結果



## Vernam

先生成Autokey，生成完畢之後再將key與plaintext做XOR運算



## RailFence

一開始先分配空間，並全部都用空白初始化，之後開始將明文填入陣列中，一開始會向下填，碰到row的最底層之後會開始反轉向上填，最後填完之後將陣列不是空格的元素輸出即是密文



## RowTransition

根據key的長度來決定col、row的大小，依據key的順序輸出row，但可以透過一定規律產生密文，就不需要配置儲存空間了



### 解密

#### **Caesar**

先將key值mod 26，然後將密文中的每個值減去此值，若超出A~Z的範圍，就加或減26，使其回到A~Z之範圍

#### **Playfair**

利用bool array紀錄每個字元有沒有出現過，並同時將重複字元去除，產生5x5 table



將輸入密文分成兩個一組



對每個組去查表，進行解密



#### **Vernam(autokey)**

掃過每個密文中的字元，若key的長度小於密文長度，則每次解密後的字元，須補到key最後面



#### **RailFence**

計算單個fence有多少個element (fence\_len)，利用fence\_len與key值(rail\_count) 來計算密文index對應到的明文index，一共分為三種情形，頂端、底部、中間進行處理



#### **RowTransition**

處理密文不足以形成完整長方形的狀況，會將每個直排的row數紀錄於col\_to\_rows



將每個每個數字字元於key中對應的index紀錄於order\_to\_col\_index



依序將密文中的每個字元放到其對應於明文的位置，完成解密

