HW1 說明文件

分工

四資工三甲 B10632026 吳苡瑄 Encrypt + Decrypt

四不分三戊 B10630436 林玉庭 Decrypt-playfair

開發環境

Windows10 Python3

範例

Plaintext: doyourbestandthenletgo

1. **Caesar cipher:**

   Key: 5

   Ciphertext: ITDTZWGJXYFSIYMJSQJYLT

   只是簡單的 shift 和一些大小寫轉換。

2. **Playfair cipher:**

   Key: COMP

   Ciphertext: IDWPQSDFTUGUFRKBHNFSDA

   把 key 的 table 建出來以後，後面就只要檢查是不是同 row 或是同 column 再做對應的動作即可。

3. **Vernam proposed the autokey system:**

   Key: TEC

   Ciphertext: WSARIPPYJUEFWTUHGSIGRS

   先用 key 去加密，沒有 key 以後就用明文接著做。

   用了這個 tool 來對過答案: https://cryptii.com/pipes/vigenere-cipher

4. **Row transposition:**

   Key: 45362178

   Ciphertext: RTOUDGYAEDSNOTLONTBHEE

   把他們都先塞到幾個 array 裡面再去分出去，解密的時候要多考慮比較少東西的 row，就沒問題了。

5. **Rail fence cipher:**

   Key: 2

   Ciphertext: DYUBSADHNEGOORETNTELTO

   也是和 row 類似的作法用 array 來做，解密時則是一行一行來，還沒輪到的就先跳過。