

分工

四資工三 B10615056 黃暉翔 Encrypt

開發環境

Visual Studio CPP

Encrypt:

Main:

字串判斷 call function and output.

1. Caesar :

將每個字元位移 key 值。

2. Playfair:

先用 c_table 紀錄每個字母，將 key 值填入 table 後再將 c_table 中剩下的字元依序填入，最後再依 plaintext 輸出正確 cipher text。

3. Vernam:

將 key 加在 plaintext 前產生 auto key，再跟 plaintext 做 XOR 運算。

4. Row:

將 plaintext 填入 table 後再依 key 順序產生 cipher text。

5. Rail_fence:

將 plaintext 填入 table 後產生 cipher text。

分工：

四資工三甲 B10615055 潘禎佑 Decrypt

開發環境：

Visual Studio C++

Decrypt：

Main：

輸入字串後格式判斷 call function and output

1. Caesar Decrypt

每個位元減去 key 值後回傳。

2. Playfair Decrypt

在 chars 這個陣列中填入所有字母，去掉 key 中出現的字母並加入 playfair table，key 處理完再將 chars 全部填入 table 完成建表。

掃描 ciphertext 兩兩一組，依照加密規則逆推完成解密後回傳 plaintext。

3. Vernam with Autokey Decrypt

將 key 與 ciphertext XOR 得到|key|長度的 plaintext，加到 key 後面繼續 XOR，持續做到 ciphertext 全部解密完成後回傳。

4. Row Transpotation Decrypt

計算所需變數後，將 ciphertext 逐一掃瞄填入 plaintext 對應位置完成解密後回傳。

5. Rail Fence Decrypt

計算所需變數後，將 ciphertext 逐一掃瞄填入 plaintext 對應位置完成解密後回傳。