

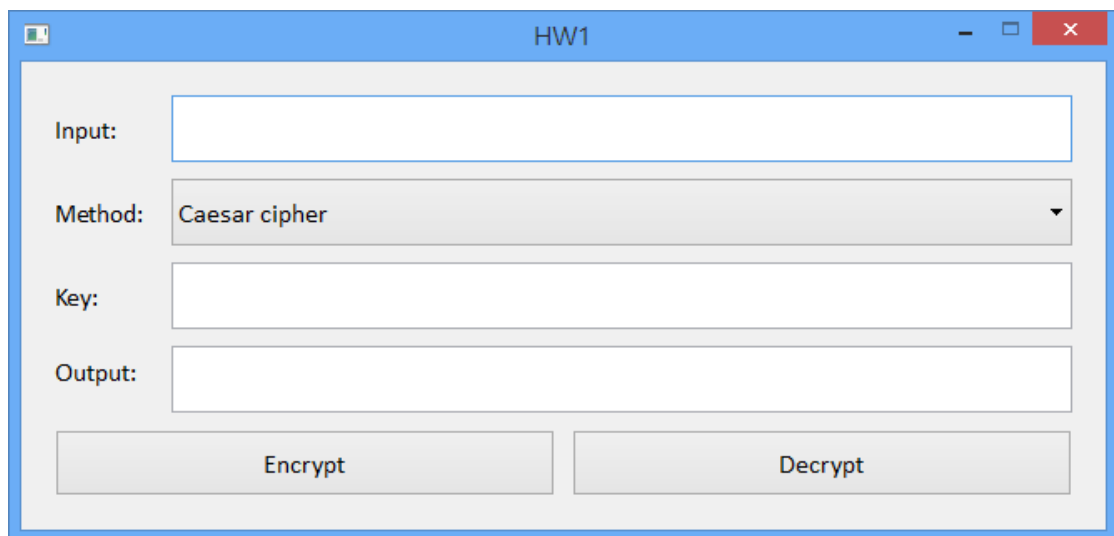
HW1 of Introduction to Information Security 2015

四電資三 B10232016 王奕棋

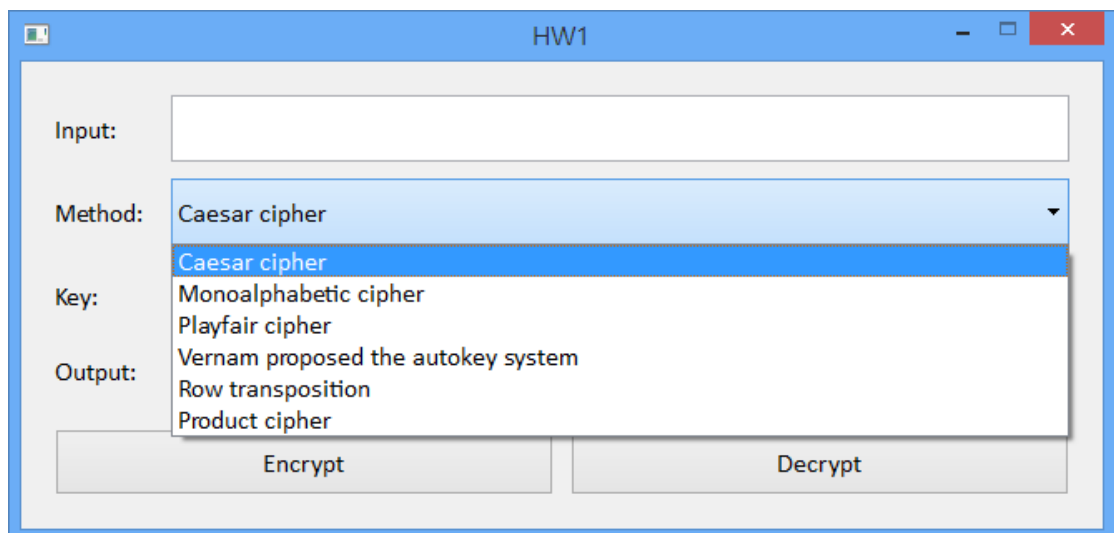
四電資三 B10232037 陳韋綱

0. UI design

使用 QT 進行視窗程式設計，使用者輸入 Input 和 Key 後可選擇想要加密或解密的方法，設計上將 Input 字串中的空白忽略，而 Key 必須輸入正確的格式，否則可能會造成結果錯誤或程式 Crash，Output 格式設計為大寫字母、每五個字母後加一個空格。



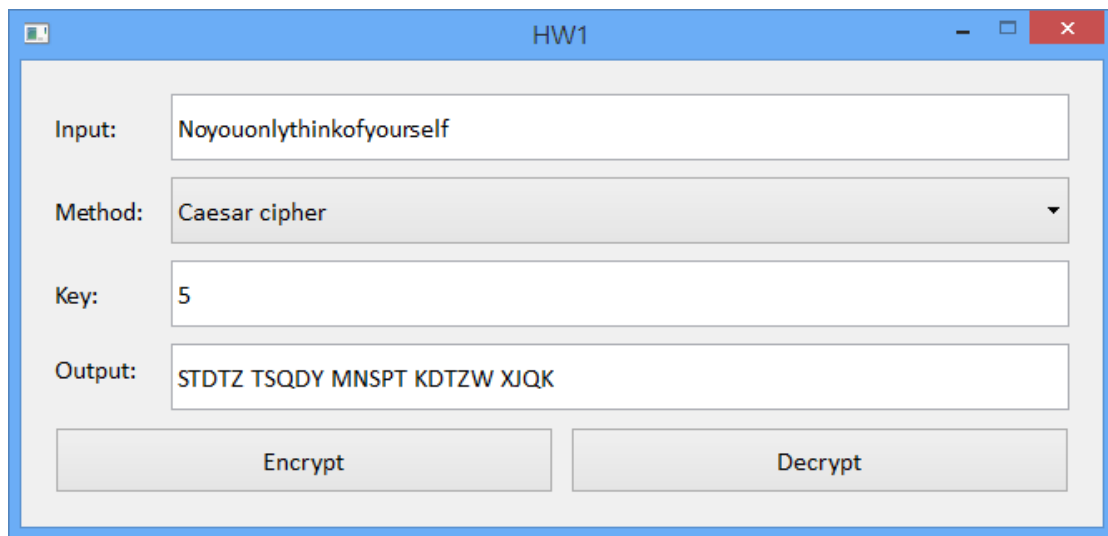
The screenshot shows a window titled "HW1" with a light blue border. Inside, there are four labels: "Input:", "Method:", "Key:", and "Output:". Each label is followed by a text input field. The "Method:" field is a dropdown menu currently showing "Caesar cipher". Below the input fields are two buttons: "Encrypt" and "Decrypt".



This screenshot shows the same "HW1" window, but the "Method:" dropdown menu is open, displaying a list of cipher options. The options are: "Caesar cipher" (highlighted in blue), "Monoalphabetic cipher", "Playfair cipher", "Vernam proposed the autokey system", "Row transposition", and "Product cipher". The "Input:", "Key:", and "Output:" fields remain empty, and the "Encrypt" and "Decrypt" buttons are still visible at the bottom.

1. Caesar cipher

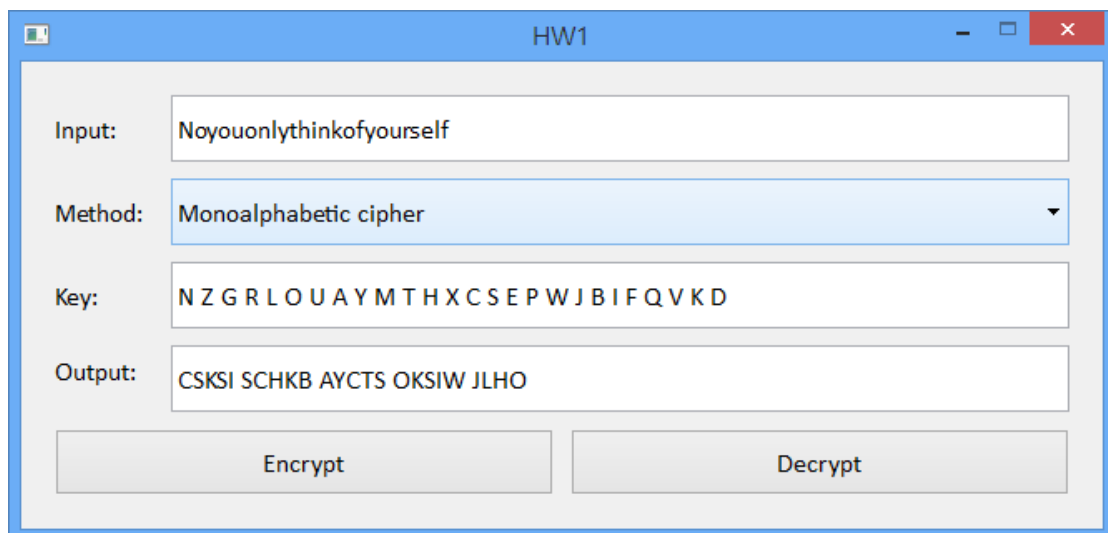
Key 的輸入為一個整數



The screenshot shows a window titled "HW1" with a light blue border. Inside, there are four input fields and two buttons. The "Input" field contains the text "Noyouonlythinkofyourself". The "Method" dropdown menu is set to "Caesar cipher". The "Key" field contains the number "5". The "Output" field displays the encrypted result "STDTZ TSQDY MNSPT KDTZW XIQK". At the bottom, there are two buttons: "Encrypt" and "Decrypt".

2. Monoalphabetic cipher

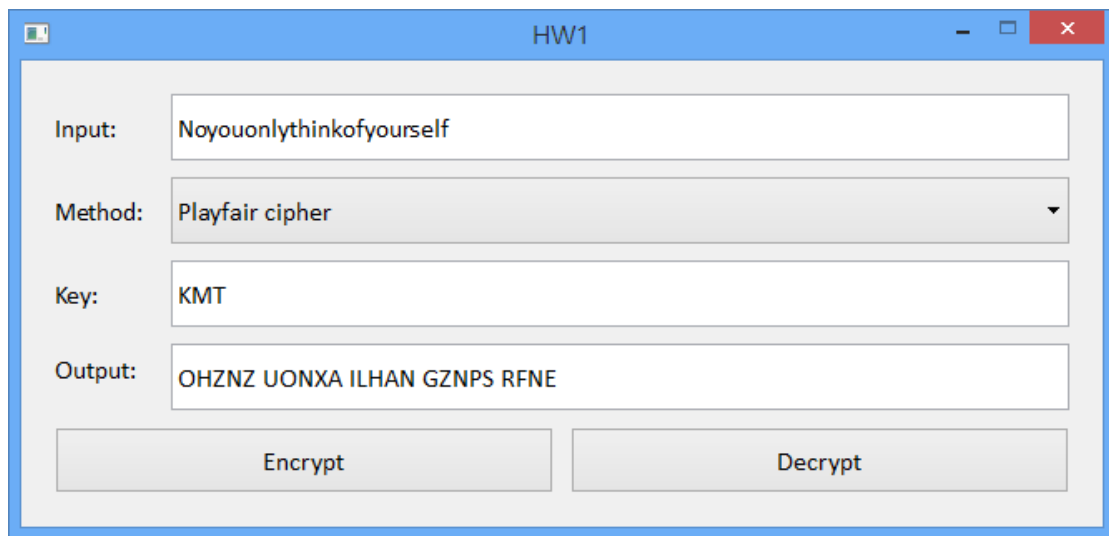
Key 的輸入為 26 個英文字母，字母間有無空格皆可



The screenshot shows the same "HW1" window, but with the "Method" dropdown menu set to "Monoalphabetic cipher". The "Input" field still contains "Noyouonlythinkofyourself". The "Key" field now contains a 26-letter string: "N Z G R L O U A Y M T H X C S E P W J B I F Q V K D". The "Output" field displays the encrypted result "CSKSI SCHKB AYCTS OKSIW JLHO". The "Encrypt" and "Decrypt" buttons remain at the bottom.

3. Playfair cipher

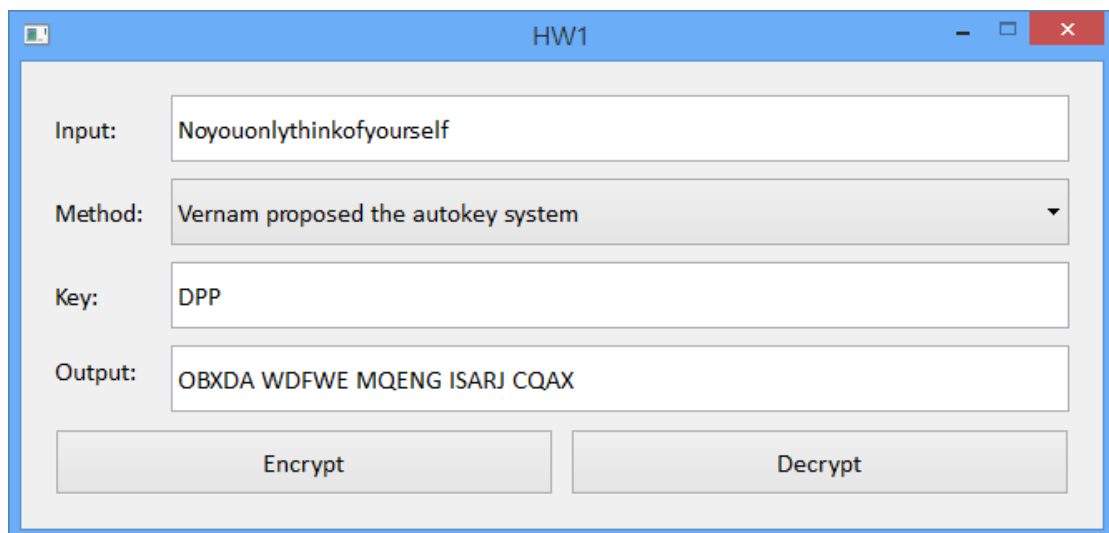
Key 的輸入為一個字串



The screenshot shows a software window titled "HW1" with a blue title bar. Inside, there are four input fields and two buttons. The "Input" field contains the text "Noyouonlythinkofyourself". The "Method" dropdown menu is set to "Playfair cipher". The "Key" field contains the text "KMT". The "Output" field displays the encrypted result "OHZNZ UONXA ILHAN GZNPS RFNE". At the bottom, there are two buttons labeled "Encrypt" and "Decrypt".

4. Vernam proposed the autokey system

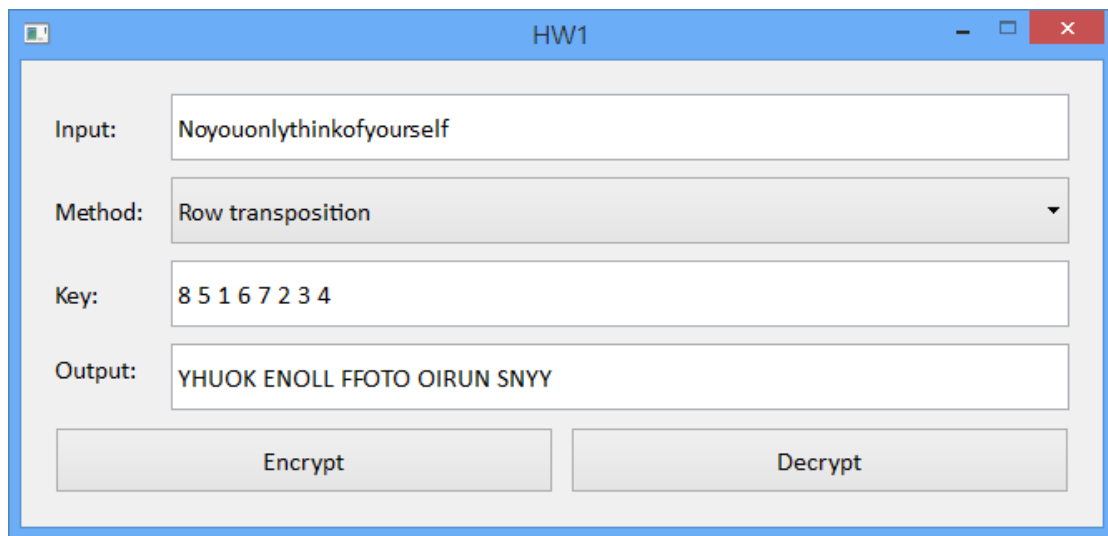
Key 的輸入為一個字串



The screenshot shows a software window titled "HW1" with a blue title bar. Inside, there are four input fields and two buttons. The "Input" field contains the text "Noyouonlythinkofyourself". The "Method" dropdown menu is set to "Vernam proposed the autokey system". The "Key" field contains the text "DPP". The "Output" field displays the encrypted result "OBXDA WDFWE MQENG ISARJ CQAX". At the bottom, there are two buttons labeled "Encrypt" and "Decrypt".

5. Row transposition

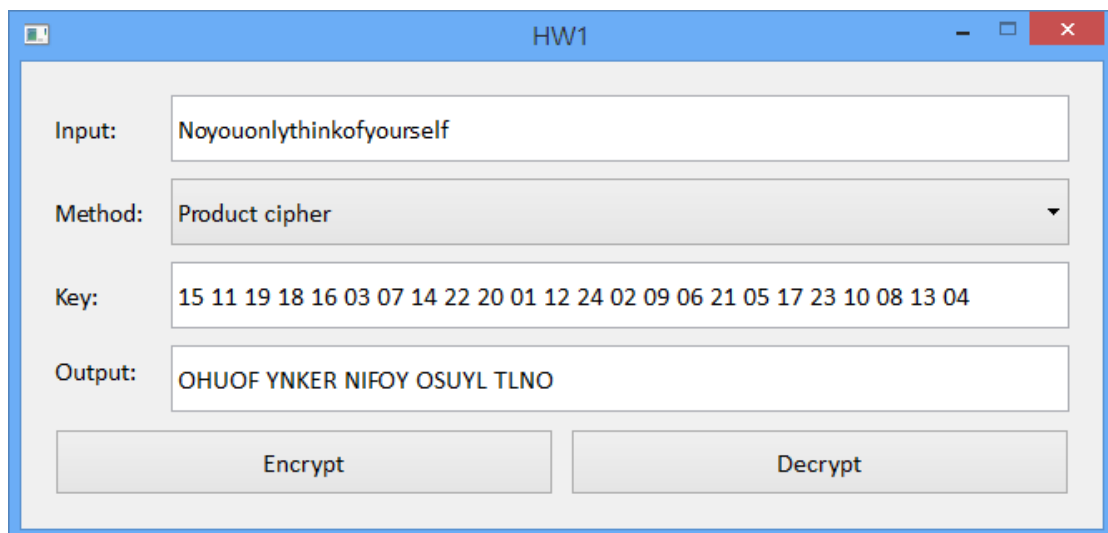
Key 的輸入為數個整數，整數中間必須要有一個空格，且字尾不可有空格



The screenshot shows a window titled "HW1" with a light blue border. Inside, there are four input fields and two buttons. The "Input" field contains the text "Noyouonlythinkofyourself". The "Method" dropdown menu is set to "Row transposition". The "Key" field contains the sequence "8 5 1 6 7 2 3 4". The "Output" field displays the result "YHUOK ENOLL FFOTO OIRUN SNYY". At the bottom, there are two buttons: "Encrypt" and "Decrypt".

6. Product cipher

Key 的輸入為數個整數，整數中間必須要有一個空格，且字尾不可有空格



The screenshot shows the same "HW1" window, but with the "Method" dropdown menu set to "Product cipher". The "Input" field remains "Noyouonlythinkofyourself". The "Key" field now contains a longer sequence of numbers: "15 11 19 18 16 03 07 14 22 20 01 12 24 02 09 06 21 05 17 23 10 08 13 04". The "Output" field displays the result "OHUOF YNKER NIFOY OSUYL TLNO". The "Encrypt" and "Decrypt" buttons are still present at the bottom.