hw1 write-up - Computer Security

學號：b04902053

姓名：鄭淵仁

write-up

`disassemble` 程式之後，觀察到程式會從 `main()` 輸入字串，再呼叫 `encrypt()` 來寫出結果到 `flag`。

接著用 `gdb` 觀察變數，發現：一直到進入 `encrypt()` 之前，輸入的字串都沒被改動。而 `encrypt()` 會把輸入的字串經過一連串操作後，再 `fwrite()` 到檔案 `flag` 上。所以關鍵在於程式如何「加密」輸入的字串。

接下來觀察輸入和輸出的關係，發現輸入的字串中的每一個字元都會被獨立轉成 4 個 byte ，不會和其他字元有關係，但是和字元的前後位置有關係。在這個時候其實我有想要寫一個 python 檔去一個字母一個字母拼出答案，不過我還不是很確定我觀察到的這個特性是不是正確的，所以我就先試著直接翻譯 `encrypt()` function 看看。（我翻譯完 `encrypt()` 之後就確認這個方法是可行的）

總之我就從 assembly code 整理出原始的 `encrypt()` 的 code，並且寫一個 python script 模擬加密的流程，實際跑跑看結果是否相同。確認加密的流程是正確的之後，就反著做程式的流程就可以把檔案 `flag` 轉換回輸入的 flag string 了。

> 可以輸出和 `hw1` 一樣的結果的 python 檔：`translate.py`
>
> 把 `flag` 檔案的內容轉回輸入的 flag string 的 python 檔：`inv_translate.py`