

此程式輸入 8 字元的明文與 8 字元的金鑰，輸入後會將明文與金鑰的最後 1 位元翻轉，並對原始加密後的結果作比較，加密模式使用 CBC，另外在實作過程中發現，若加密模式使用 ECB，key 最後 1 位做翻轉在大部分情況下與原始加密後結果一樣。

執行結果：

```
請輸入明文(8字元): abcdefgh
請輸入金鑰(8字元): 12345678
原始加密結果: b'4b54144c0a6c40c9'
明文差 1 bit 結果: b'bd5f473cf8c462ed'
bit差異數量: 28 (43.75%)

key 差 1 bit 結果: b'd116928dba839d3e'
bit差異數量: 35 (54.69%)
```

範例程式

<https://github.com/sunnysoun/2024-NCKU-INFORMATION-SECURITY/tree/main/HW3/sample>