資訊安全　作業二

F84086171 黃盈盛

演算法說明:

加密:

步驟一:將明文以及給定金鑰轉換成 ASCII code
步驟二:將明文與金鑰轉換結果做 XOR
步驟三:將步驟二結果以 4 個 bit 為單位拆分，並以 0~15 對應 A~P 的形式轉換為密文

解密:

步驟一:將密文以 A~P 對應 0~15 轉為 binary 形式，並將金鑰轉換為 ASCII code
步驟二:將步驟一結果以 8 bit 為單位拆分並與轉換後的金鑰做 XOR
步驟三:以 ASCII code 將拆分結果還原回明文

範例:

明文 : HELLO
金鑰 : SECRET

加密:

步驟一:

明文轉換	密文轉換
H : 01001000	S : 01010011
E : 01000101	E : 01000101
L : 01001100	C : 01000011
L : 01001100	R : 01010010
O : 01001111	E : 01000101

步驟二:

```
        01001000 01000101 01001100 01001100 01001111
XOR     01010011 01000101 01000011 01010010 01000101
Result: 00011011 00000000 00001111 00011110 00001010
```

步驟三:

0001 1011 0000 0000 0000 1111 0001 1110 0000 1010

⇨ 1 11 0 0 0 15 1 14 0 10

⇨ BLAAAPBOAK

密文: BLAAAPBOAK

解密:

步驟一:

密文轉換		金鑰轉換
B : 1	=> 0001	S : 01010011
L : 11	=> 1011	E : 01000101
A : 0	=> 0000	C : 01000011
A : 0	=> 0000	R : 01010010
A : 0	=> 0000	E : 01000101
P : 15	=> 1111	
B : 1	=> 0001	
O : 14	=> 1110	
A : 0	=> 0000	
K : 10	=> 1010	

步驟二:

	00011011 00000000 00001111 00011110 00001010
XOR	01010011 01000101 01000011 01010010 01000101
Result:	01001000 01000101 01001100 01001100 01001111

步驟三:

01001000 : H

01000101 : E

01001100 : L

01001100 : L

01001111 : O

明文:HELLO