

정보보호

- HW03 : XOR Cipher, Brute Force-

제 출 일	2018년 09월 22일
담당교수	류재철
학 과	컴퓨터공학과
학 번	201302423
이 름	신종욱

1. XOR 암호(XOR Cipher)

■ 과제해결 과정

시저암호에서 복호화할때 암호화할 때 사용한 +대신 - 했듯이 Xor의 역연산을 알아야 한다.

Xor 함수표

입력 \ Key	Key	
	0	1
0	0	1
1	1	0

원편이 원래 값 윗 값이 킷값이라고 할시

복호화를 할때 암호화된값 \oplus 키 = 원래 값이 되야한다 \oplus (특수한 연산)

$0 \oplus 0 = 0$, $1 \oplus 1 = 0$, $1 \oplus 0 = 1$, $0 \oplus 1 = 1$ 이 되어야한다.

만족하는 연산은 그대로 Xor이다.

코드는 이전과제에 했던 getsize를 이용하였고 그 외는 그대로 사용하였다.

바뀐 부분만 주석을 추가했다.

```
shin@shin: ~/Desktop/homework/2
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
47
48     for(i=0;i<fileSize;i++)
49     {
50         fread(&buff,sizeof(char),1,input_FD);
51
52         len = i % strlen(key); //키값이 반복되야 하기때문에 나머지 계산을 이용
53         key_modified=key[len]; //나온 나머지값의 인덱스값이 암호,복호화에 사용될
진짜 값이다
54         if(mode==0)
55         {
56             enc(&buff,key_modified);
57         }
58         else if(mode==1)
59         {
60             dec(&buff,key_modified);
61         } //암복호화 진행
62
63         fwrite(&buff,sizeof(char),1,output_FD);
64     }
65     fclose(output_FD);
66     fclose(input_FD);
67 }
68
```

킷값 반복을 위한 나머지연산 사용

```

81 void enc(char *buff,int key){
82     *buff = *buff^key;
83 }
84
85 void dec(char *buff,int key){
86     *buff = *buff^key;
87 }

```

//XOR의 경우에는 역원의 경우에도 XOR이기 때문에 암호,복호화 과정이 둘다 XOR로 같다.

암,복호화 과정이다 사실 하나의 함수로 작성하여도 문제가 없다.

■ XOR 암호

```

shin@shin: ~/Desktop/homework/2
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
shin@shin:~/Desktop/homework/2$ ./xor
>> Input file name : plain.txt
>> Input mode [ 0 : ENC , 1: DEC ]0
input key : sky
FILE Size = 15
shin@shin:~/Desktop/homework/2$ cat encrypt.txt
;[...Y .....s
shin@shin:~/Desktop/homework/2$ xxd plain.txt
00000000: 4865 6c6c 6f20 5365 6375 7269 7479 0a    Hello Security.
shin@shin:~/Desktop/homework/2$ xxd encrypt.txt
00000000: 3b0e 151f 0459 200e 1a06 1910 0712 73    ;[...Y .....s
shin@shin:~/Desktop/homework/2$ ./xor
>> Input file name : encrypt.txt
>> Input mode [ 0 : ENC , 1: DEC ]1
input key : sky
FILE Size = 15
shin@shin:~/Desktop/homework/2$ cat decrypt.txt
Hello Security
shin@shin:~/Desktop/homework/2$ xxd encrypt.txt
00000000: 3b0e 151f 0459 200e 1a06 1910 0712 73    ;[...Y .....s
shin@shin:~/Desktop/homework/2$ xxd decrypt.txt
00000000: 4865 6c6c 6f20 5365 6375 7269 7479 0a    Hello Security.
shin@shin:~/Desktop/homework/2$

```

2. 무차별 대입 공격(Brute Force)

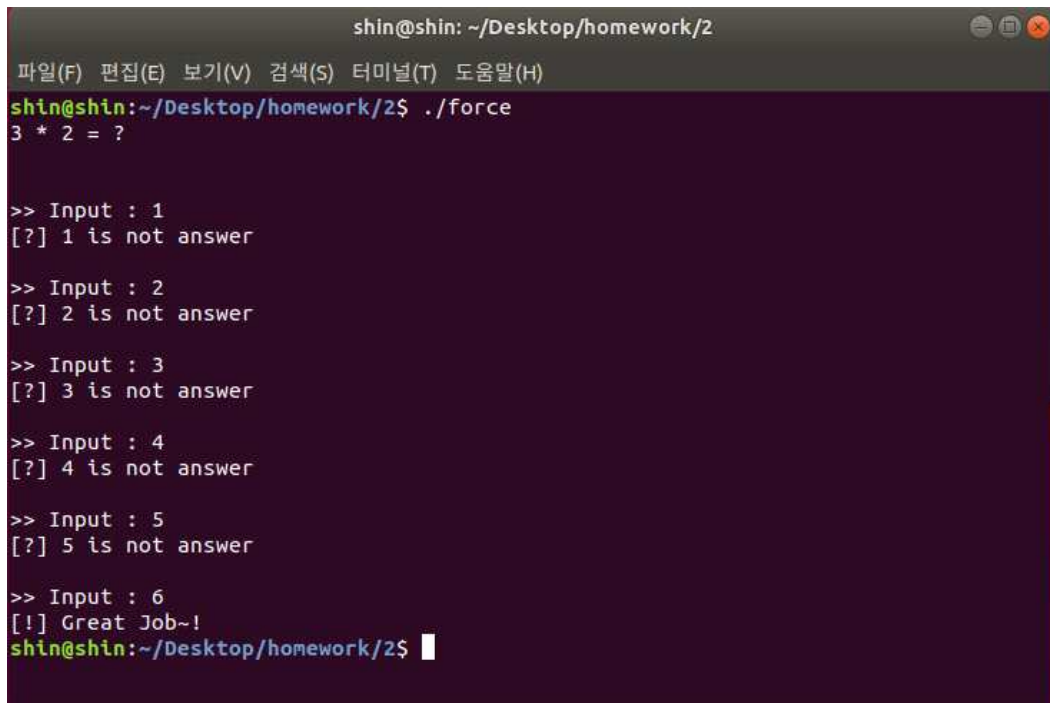
■ 과제해결 과정

while문 형태로 원하는 답이 나올때까지 입력을 반복하게 된다면
원하는 형태가 나올 것 같아서 구현하였다.

정답값은 나중에 수정하기 편하게 define으로 지정하여서 사용하였다.

```
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4 #define CORRECT 6//정답값 지정
5 void main()
6 {
7     int answer=0;
8     printf("3 * 2 = ?\n\n");//문제 제시
9     while(answer!=CORRECT){//정답이 아닐경우 무한 반복
10        printf(">> Input : ");
11        scanf("%d",&answer);
12        if(answer==CORRECT)
13        {
14            printf("[!] Great Job~!\n");//정답일 경우 메세지
15        }
16        else{
17            printf("[?] %d is not answer\n\n",answer);
18        }//정답이 아닐경우 메세지
19    }
20 }
21 exit(1);
22 }
```

■ 무차별 대입 공격 결과



```
shin@shin: ~/Desktop/homework/2
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
shin@shin:~/Desktop/homework/2$ ./force
3 * 2 = ?

>> Input : 1
[?] 1 is not answer

>> Input : 2
[?] 2 is not answer

>> Input : 3
[?] 3 is not answer

>> Input : 4
[?] 4 is not answer

>> Input : 5
[?] 5 is not answer

>> Input : 6
[!] Great Job~!
shin@shin:~/Desktop/homework/2$
```

느낀점 : Xor의 복호화 연산이 무엇인지 몰랐는데 똑같은 Xor인걸 알아서 신기했다.