정보보호론 lect8_second

12141163 이욱진

Homework
2) Implement DES
ref: "The DES Algorithm Illustrated" :
http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm

처음 강의자료에 올려주신 코드를 확인하는작업을 진행하였습니다 다음은 main문 입니다.

```
1 main.cpp
  1 #include "global.h"
  2
  3 void display_sentence(char *cipher){
  4    printf("cipher:\n");
  5    for(int i=0;i<64;i++)
  6       printf("%d ", cipher[i]);
  7    printf("\n");
  8 }
  9 int main(){
 10    char keys[17][48];
 11    char cipher[64]; // cipher text
 12
 13    construct_key_schedule(K, keys); // K is original 64bit key
 14    des_encrypt(M, keys, cipher);
 15    display_sentence(cipher);
 16 }
```

main문에서 construct_key_schedule함수를 호출하게되는데 이 함수는 keyshed.cpp 에서 찾을 수 있었습니다.

K값을 채워넣기위하여 코드를 다음과같이 구현하였고 출력문을확인해보았습니다.

```
 10    char keys[17][48];
~/De/정 /lect8/desCode-template  ./a.out                    ✓  11:11:07
K : 1
K : 3
K : 3
K : 4
K : 5
K : 7
K : 7
K : 9
K : 9
K : 11
K : 11
K : 12
K : 13
K : 15
K : 15
K : 1
after permute. dest (size:56) is
-94 -16 0 64 88 0 9 1 38 -27 0 -24 64 0 11 3 42 97 0 48 52 0 11 3 25 -30 0
25 0 0 0 0 0 0 15 7 0 127 0 0 0 0 15 7 1 -2 0 1 1 0 13 5 25 0 12 4
1101101111011011110110111101000000110100001111011011011after split KPlust
117799413100072-77-77-106-112700-1-1-1-1-1-1-1-10000
-62-41125-1005872284700001186l120-6678-1271270563839270000
1th CD
000064-2897-30-212700-4510677112-11270000000000
000048-2797-30-21270056-2797-30-212700-242315-70-484940-95
```

K를 10진수로 출력하였고 총 16개 각 1바이트이기에 64비트를 저장한다고생각하였습니다.

이후에 permut8_7 함수를 살펴보았고 index에해당하는값 즉 테이블에서가져오는 값이 64이하의 원소를 index로이용한다는 것을 코드를통해 확인해보았고 제가 K를 구현한것이 다르다는것을 알게되었습니다. 그래서K를 64개의 배열로 선언해주었고 처음에는 포인터를 이용하려고하였으나 값의대입이 불가능하여 64개의배열로선

언 후 133457799BB~ 값을 채워넣을생각입니다.