정보보호론 lect8_first

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.

main.cpp

```cpp
#include "global.h"

void display_sentence(char *cipher){
   printf("cipher:\n");
   for(int i=0;i<64;i++)
      printf("%d ", cipher[i]);
   printf("\n");
}
int main(){
   char keys[17][48];
   char cipher[64]; // cipher text

   construct_key_schedule(K, keys); // K is original 64bit key
   des_encrypt(M, keys, cipher);
   display_sentence(cipher);
}
```

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