**Symmetric Encryption and Message Confidentiality 실습**

**[실습 목표] 수업 시간에 학습한 DES 소스 코드**를 실제 시스템에 활용할 때 사용되는 각 블록암호 동작모드(CBC, CFB, OFB, CTR)를 구현하고 동작 원리를 학습한다.

**[유의사항]** 아래 주어진 메인 함수를 활용하거나 별도의 메인 함수를 작성하여 소스 코드를 작성하시오. 동작 결과 화면은 full screen (사용자 실행환경 정보가 보이는 화면. 예: c://yhchoi/a.cpp)을 캡쳐하시오. 각 동작 모드의 동작을 검증하기 위해 아래 입력 값을 사용하시오.

* Plaintext: Computer Security
* Key: security
* IV: iloveyou

**[제출물]** 소스 코드, 소스 코드 동작 과정, 결과 값을 포함하는 보고서를 제출한다.

**[문제 1] 각 블록 모드 작업을 사용하여 DES 암호 알고리즘을 작성하시오.**

**(참고)** main() 함수

|  |
| --- |
| #include <stdio.h>  #include <stdlib.h>  #include <string.h>  #include "BlockCipherMode.h"  #define BLOCK\_MODE 1 /\* 1: CBC, 2: CFB, 3: OFB, 4: CTR \*/  int main()  {  int i;  BYTE p\_text[128]={0,};  BYTE key[9]={0,};  BYTE IV[9]={0,};  BYTE c\_text[128]={0,};  BYTE d\_text[128]={0,};  int msg\_len;  UINT64 ctr=0;  /\* 평문 입력 \*/  printf(“평문 입력: ");gets((char \*)p\_text);  /\* 비밀키 입력 \*/  printf(“비밀키 입력: ");scanf\_s("%s", key);  fflush(stdin);  #if(BLOCK\_MODE!=4)  /\* 초기화 벡터 입력 \*/  printf(“초기화 벡터 입력: ");  scanf\_s("%s", IV);  #else  /\* 카운터 입력 \*/  printf("ctr 입력: ");  scanf("%u", &ctr);  #endif  /\* 메시지 길이 계산 \*/  msg\_len=(strlen((char \*)p\_text) % BLOCK\_SIZE) ?  ((strlen((char \*)p\_text) / BLOCK\_SIZE +1)\*8):  strlen((char \*)p\_text);  #if(BLOCK\_MODE==1)  DES\_CBC\_Enc(p\_text, c\_text, IV, key, msg\_len);//DES-CBC 암호화  #elif(BLOCK\_MODE==2)  DES\_CFB\_Enc(p\_text, c\_text, IV, key, msg\_len);//DES-CFB 암호화  #elif(BLOCK\_MODE==3)  DES\_OFB\_Enc(p\_text, c\_text, IV, key, msg\_len);//DES-OFB 암호화  #else  DES\_CTR\_Enc(p\_text, c\_text, key, ctr, msg\_len);//DES-CTR 암호화  #endif  /\* 암호문 출력 \*/  printf("\n암호문: ");  for(i=0; i<msg\_len; i++)  printf("%c", c\_text[i]);  printf("\n");  #if(BLOCK\_MODE==1)  DES\_CBC\_Dec(c\_text, d\_text, IV, key, msg\_len);//DES-CBC 복호화  #elif(BLOCK\_MODE==2)  DES\_CFB\_Dec(c\_text, d\_text, IV, key, msg\_len);//DES-CFB 복호화  #elif(BLOCK\_MODE==3)  DES\_OFB\_Dec(c\_text, d\_text, IV, key, msg\_len);//DES-CFB 복호화  #else  DES\_CTR\_Dec(c\_text, d\_text, key, ctr, msg\_len);//DES-CTR 복호화  #endif  /\* 복호문 출력 \*/  printf("\n복호문: ");  for(i=0; i<msg\_len; i++)  printf("%c", d\_text[i]);  printf("\n");  return 0;  } |