Programming Assignment: Modified AES-128

[과제 목표]

Modified AES-128 프로그램 구현 (블록 암호 운용 모드는 ECB이며, 표준과 일부 기능이 다름을 주의하여야 함)

[Specification]

1. input files

- 입력으로 주어지는 파일은 key 128비트를 순서대로 기록한 파일(key.bin)과 평문이 담긴 파일(pt.bin)이다.
- encrypt 모드에서 입력으로 사용되는 파일은 키 파일(key.bin)과 평문이 담긴 파일(pt.bin)이며 encrypt 결과인 암호문을 ct.bin 파일로 출력하여야 한다.
- decrypt 모드에서 필요한 파일은 키 파일(key.bin)과 암호문(ct.bin)이며, decrypt 결과를 pt2.bin 파일로 출력하여야 한다.
- 모든 입력 파일은 실행 파일과 같은 폴더(디렉토리)에 위치한다.

(1) key.bin (16-byte binary file)
(2) pt.bin: plaintext binary file (multiple of 16-bytes) - encrypt 모드에서 사용하는 input
(3) ct.bin: ciphertext binary file (multiple of 16-bytes) - decrypt 모드에서 사용하는 input

2. output files

AES encrypt와 decrypt를 각각 수행하며 결과 값을 아래와 같은 파일 이름으로 출력한다.
(1) encrypt mode : ct.bin (multiple of 16-bytes) - encrypt 모드에서 출력하는 output
(2) decrypt mode : pt2.bin (multiple of 16-bytes) - decrypt 모드에서 사용하는 output

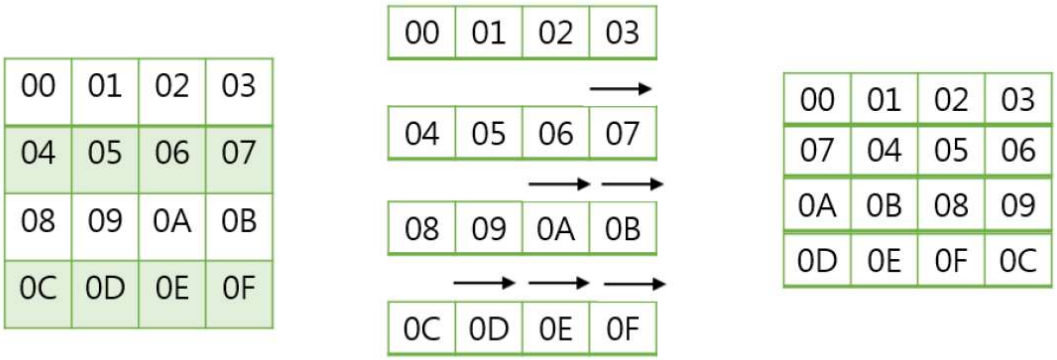
3. Modify AES

작성해야하는 AES 프로그램은 표준 AES를 일부 수정한 버전이다. 표준 AES와 다른 점은 크게 2가지이다.

[차이점 1] 본 과제에서는 아래와 같이 정의된 S Box를 이용하여 AES를 수행한다.
(즉, SBox를 이용하여 inverse S Box를 구해야 하며, S Box의 변경으로 Key Scheduling에도 영향이 있음을 주의하여야 함)

```
static const unsigned char SBox[256] ={
        0xD4, 0xAD, 0x82, 0x7D, 0xA2, 0x59, 0xF0, 0xAF, 0x9C, 0xA4, 0x72, 0xC0, 0xCA, 0xC9, 0xFA, 0x47,
        0xA5, 0x34, 0xFD, 0x26, 0xE5, 0x3F, 0xCC, 0xF1, 0x71, 0xD8, 0x31, 0x15, 0xB7, 0x93, 0x36, 0xF7,
        0xD3, 0xC2, 0x32, 0x0A, 0xAC, 0x06, 0x5C, 0x62, 0x91, 0x95, 0xE4, 0x79, 0xE0, 0x3A, 0x49, 0x24,
        0x12, 0x07, 0xC7, 0xC3, 0x80, 0x96, 0x9A, 0xE2, 0xEB, 0x27, 0xB2, 0x75, 0x04, 0x23, 0x18, 0x05,
        0x01, 0x30, 0x7C, 0x7B, 0x67, 0x6B, 0xC5, 0x2B, 0xFE, 0xD7, 0xAB, 0x76, 0x63, 0x77, 0xF2, 0x6F,
        0x1E, 0x9B, 0xF8, 0x11, 0x87, 0xD9, 0x94, 0xE9, 0xCE, 0x55, 0x28, 0xDF, 0xE1, 0x98, 0x69, 0x8E,
        0xCB, 0x6A, 0xD1, 0xED, 0xBE, 0xFC, 0x5B, 0x39, 0x4A, 0x4C, 0x58, 0xCF, 0x53, 0x00, 0x20, 0xB1,
        0xB6, 0xBC, 0xA3, 0x8F, 0xDA, 0x9D, 0xF5, 0x21, 0x10, 0xFF, 0xF3, 0xD2, 0x51, 0x40, 0x92, 0x38,
        0xA7, 0xC4, 0x0C, 0xEC, 0x7E, 0x97, 0x17, 0x3D, 0x64, 0x5D, 0x19, 0x73, 0xCD, 0x13, 0x5F, 0x44,
        0x56, 0x6C, 0xC8, 0x6D, 0xF4, 0xD5, 0xA9, 0xEA, 0x65, 0x7A, 0xAE, 0x08, 0xE7, 0x37, 0x8D, 0x4E,
        0x99, 0x41, 0xA1, 0x0D, 0x2D, 0xE6, 0x68, 0x0F, 0xB0, 0x54, 0xBB, 0x16, 0x8C, 0x89, 0xBF, 0x42,
        0xEE, 0x46, 0x81, 0xDC, 0xB8, 0x2A, 0x88, 0x14, 0xDE, 0x5E, 0x0B, 0xDB, 0x60, 0x4F, 0x22, 0x90,
        0xDD, 0xE8, 0x78, 0x2E, 0x74, 0xA6, 0xC6, 0x1F, 0x4B, 0xBD, 0x8B, 0x8A, 0xBA, 0x25, 0x1C, 0xB4,
        0x35, 0x61, 0x3E, 0x66, 0x57, 0x03, 0x0E, 0xB9, 0x86, 0xC1, 0x1D, 0x9E, 0x70, 0xB5, 0x48, 0xF6,
        0xF9, 0x45, 0xEF, 0xFB, 0x02, 0x4D, 0x85, 0x7F, 0x50, 0x3C, 0x9F, 0xA8, 0xD0, 0xAA, 0x43, 0x33,
        0x3B, 0x52, 0x83, 0x1A, 0xD6, 0x6E, 0xA0, 0xB3, 0x29, 0xE3, 0x2F, 0x84, 0x09, 0x2C, 0x1B, 0x5A };
```

[차이점 2] ShiftRow는 아래와 변형된 형태로 수행한다.



3) 이외 Add Round Key와 Mix Column은 표준 및 강의 자료와 동일한 방법으로 진행한다.

4. execution

[STEP 1]

구현한 프로그램의 실행파일(예를 들어 aes.exe)를 실행 시, 자동으로 키(key.bin)와 평문(pt.bin) 을 읽어온다. bin 파일로부터 읽은 키(16바이트)와 평문(16의 배수 바이트)을 콘솔창(stdout)에 출력한 후 암호화를 수행한다. 이때 AES의 각 라운드를 수행할 때마다 중간 결과들을 콘솔창 (stdout)에 출력하여야 한다. 예를 들어, 라운드 1번에서 출력해야 하는 결과 값은 SubByte를 수행한 직후의 결과 값 1, ShiftRow를 수행한 직후의 결과 값 2, MixColumn을 수행한 직후의 결과 값 3, AddRoundKey를 수행한 직후의 결과 값 4이며, 총 4가지를 출력해야한다. 라운드 0번의 경우 Add Round Key 직후의 결과 값만 출력하면 되며 마지막 라운드의 경우 3가지를 출력하면 된다. 암호화를 수행하여 최종적으로 얻은 결과 값을 콘솔창(stdout)과 ct.bin 파일에 각각 출력한다.

(※ 자세한 각 라운드별 출력 형태는 아래 테스트벡터를 참고)

[STEP 2]

Step 1이 끝나면 자동으로 생성한 ct.bin을 읽어온 후, 복호화를 수행한다. 이때 암호화와는 다르게 매 라운드 수행과정을 출력하지 않는다. 복호화의 경우 최종적으로 얻은 복호화 결과 값을 콘솔창(stdout)과 pt2.bin 파일에 각각 출력한다. 이때 주의하여야 할 점은 올바르게 암/복호화가 진행되었다면 pt.bin과 pt2.bin의 값이 동일하여야 한다.

5. environment

- 언어는 C / C++를 사용할 것
- Windows의 Visual Studio 환경을 권장 (Linux환경에서 개발 시, gcc 사용)
- GUI 사용 금지, 프로그램은 CLI(Command-line interface)에서 동작할 것.

6. submission

실습 시간에 보고서 직접 제출 및 보고서와 프로젝트를 압축한 파일 온라인 제출.

(1) Report 요구사항
a. 한글 또는 MS 워드 또는 PDF로 작성
b. cover page: 이름, 학번, 연락처 포함
c. 개발 환경에 대한 명확한 명시 (OS, Visual Studio 버전, GCC 컴파일러 버전 등등)
d. 작성한 program에 대한 description (자세히)
e. 실제 수행 화면

(2) project 요구사항
a. Visual Studio 환경 혹은 Linux 환경의 gcc 컴파일러 사용
b. source code에 적절한 주석 포함
c. build 가능해야 함
(과제 제출자가 제출한 디렉토리/프로젝트를 그대로 빌드 할 예정)

[Test vector]

```
[+] key: 000102030405060708090a0b0c0d0e0f
[+] Input plaintext : 00112233445566778899aabbccddeeff

ROUND 0
        AR : 00102030405060708090a0b0c0d0e0f0
ROUND 1
        SB : d4a5d312011ecbb6a75699eedd35f93b
        SR : d43599b601a5f9eea71ed33bdd56cb12
        MC : c3b809bce1ae64989fce4949822530c5
        AR : 0b434c752d5027565b39008c4adf770f
ROUND 2
        SB : c07b639d3a1e6294df27d4cdabf62147
        SR : c0f6d4943a7b21cddf1e6347ab27629d
        MC : dac4224a15624f95a301ce89dbdef482
        AR : 3f14ecc83c4cc2d94ed80a00fefd77c1
ROUND 3
        SB : 05e5d04b046378c1f28672d41b2c21e8
        SR : 052c72c104e521d4f263d0e81b86784b
        MC : cd0a95c8c962c47b62b7097594cfb045
        AR : 2636204c0b70fcb34d7cf5349e27cf47
ROUND 4
        SB : 5c9ad363c0b609dc77516e808d62b42b
        SR : 5c626edcc09ab48077b6d32b8d510963
        MC : acf69d4b1aa8b26ed74501aa98576b12
        AR : 1ff2aabd6bbebd508998f2d5cc62e76f
ROUND 5
        SB : f783bb4fcf224f1e5d658303bad17fb1
        SR : f7d1831ecf837f035d22bbb1ba654f4f
        MC : 00ce196c6750b7b0d67eda07c0ee9061
        AR : 35076e1d238fcfffcc7c51378ed9972c
ROUND 6
        SB : 96af20930a44b45aba519be25fc1eae0
        SR : 96c19b5a0aafeae2ba4420e05f51b493
        MC : aee3944ff688578463b2856a6aa9d339
        AR : 598594cc45312f48ca0976968d252788
ROUND 7
        SB : 5597f4ba6b0724fe8ba4f5a913066264
        SR : 5506f5fe6b9762a98b07f46413a424ba
        MC : aba3bbebbf51d80194e6d3bd4f962ada
        AR : d113fd177658e631f4541e71c8a813a7
```

```
ROUND 8
        SB : 61262cf1f5ce8507d68736bc4bb0260f
        SR : 61b03607f52626bcd6ce2c0f4b8785f1
        MC : 3847b42b016f4067dd2a519d703bd526
        AR : dad0b2ea2af178969606a4a0bc291966
ROUND 9
        SB : 1d35819fe45210a9a9f02d996095d85b
        SR : 1d952da9e435d899a952815b60f0109f
        MC : 1af232d6cd64caf365ce0f8544340a65
        AR : 1edf35ade2d7f5790151c532ecb90c92
ROUND 10
        SB : 36f69689efb96effad9ba6c7d05ecac8
        SR : 365ea6ffeff6cac7adb996c8d09b6e89
        AR : 17831234e1984186c748d73e12e72988

[+] Result Encryption: 17831234e1984186c748d73e12e72988
[+] Result Decryption: 00112233445566778899aabbccddeeff
```

(참고 : 과제 명세서와 함께 업로드 한 pt.bin과 key.bin 파일은 위의 테스트벡터의 key, pt와 동일한 값입니다.)

[주의사항]

-deadline: 2017.11.17.(금) 오전 9시 마감
(보고서 오프라인 제출은 2017년 11월 17일 실습시간)

-no cheating