과제: 변형된 AES-128

AES-128(128-bit 키를 사용하는 Advanced Encryption Standard)은 $GF(2^8)$ 상에서 수행되는 산술 연산들(덧셈, 뺄셈, 곱셈, 곱셈역원)을 사용하고, 이때 사용되는 irreducible polynomial f(x)은 아래와 같다.

$$f(x) = x^8 + x^4 + x^3 + x + 1$$

Irreducible polynomial g(x)가 아래와 같이 주어질 때,

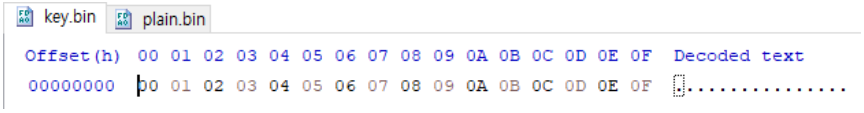
$$g(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$$

본 과제에서는 f(x) 대신에 g(x) 를 사용하여 변형된 AES-128을 구현한 프로그램(예: aes.exe)을 작성한다.

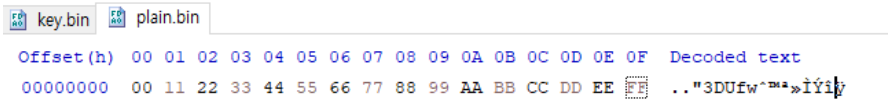
[Specification]

1. 입력 파일

(1) key.bin (16바이트 바이너리 파일)



(2) plain.bin (크기가 16바이트의 배수인 바이너리 파일. Encryption 모드에서 사용)
cipher.bin (plain.bin과 같은 크기인 바이너리 파일. Decryption 모드에서 사용)



* 단, cipher.bin은 ECB 모드로 암호화 됨
* 바이너리 파일을 보기 또는 편집하기 위해서는 위 그림과 같이 HxD 등의 hex editor 프로그램 사용 가능

2. 출력 파일

(1) Encryption 모드: cipher.bin
(2) Decryption 모드: plain2.bin

3. 실행 방법

- 사용자가 'e'(ncrypt) 또는 'd'(erypt) 중에 하나를 표준 입력
- 입력이 'e' 라면,
  "key.bin"을 사용하여 "plain.bin"을 암호화하고, 그 결과를 "cipher.bin"으로 출력
- 입력이 'd' 라면,
  "key.bin"을 사용하여 "cipher.bin"을 복호화하고, 그 결과를 "plain2.bin"으로 출력

* 블록 암호 운영 모드는 ECB로 함
* 단, BS 연산은 S-box 쓰지 말고 직접 $GF(2^8)$ 연산 이용해서 온라인으로 할 것

4. 수행 환경
- 프로그래밍 언어는 C 또는 C++ 만 사용 가능
- 표준 라이브러리만 사용 가능
(특히, 유한체 연산과 AES 연산을 구현한 외부 라이브러리 함수 사용 금지)
- command-line 인터페이스의 프로그램으로 작성. 예를 들어, 명령 프롬프트 창에서 aes.exe를 실행하였을 때, 명령 프롬프트 창에서 표준 입력 및 출력이 되어야함

5. 채점
- 채점 시, 보고서를 참고하여 조교 채점 환경(Windows 10 64bit, Visual Studio 2019)에서 소스코드 컴파일 및 실행할 예정
- 과제의 요구조건에 맞게 프로그램을 작성해야 함
- 주어진 “key.bin”에 대해, “plain.bin”과 “plain2.bin”이 일치해야 함
- 채점용 데이터(key.bin, plain.bin, cipher.bin)을 사용할 시,
  “cipher.bin”과 “채점용 cipher.bin”이 일치해야하고,
  “plain2.bin”과 “채점용 plain.bin”이 일치해야 함
- 보고서와 다르게 동작하거나 컴파일 및 실행에 에러가 있는 경우에 감점
- 채점용 데이터(key.bin, plain.bin, cipher.bin)을 사용할 시, 실행에 에러가 발생하거나 출력이 틀린 경우 감점

6. Hint
(1) $x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$ 은 0x01E7의 binary polynomial 표현 임
(2) f(x) 대신에 g(x)를 사용함에 따라 아래 부분이 수정되어야 함
  - Substitute bytes (BS)
  - Mix Columns
  - Key expansion algorithm의 RC
(3) 3~4 페이지의 [Test vectors]를 참고하여 중간 출력 결과들을 디버깅

7. 제출
(1) 보고서
- 커버 페이지: 이름, 학번, 연락처(전화번호, email, 등) 포함
  * 제출자 신원 확인 및 채점 오류 시 문의를 위함
- 프로그램 동작원리 및 설명 등을 포함
(2) 소스코드 (주석 포함)
(3) 실행 프로그램(aes.exe)
  * 제출자의 컴퓨터에서 컴파일된 프로그램
(4) 보고서, 소스코드, 실행 프로그램을 압축하여 i-class에 제출
(5) 제출 마감: 2021년 5월 27일. 마감일 이후 늦은 제출 시, 하루에 10%씩 감점 (단, 7일 경과 후 제출 불가함)
(6) no cheating

[Test vectors]

Plaintext:
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
Key:
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Ciphertext:
37 4D 03 95 C0 07 7B B6 61 B5 DD F6 EB 43 2B F6

expanded key:
k0: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
k1: 3B 5A B9 00 3F 5F BF 07 37 56 B5 0C 3B 5B BB 03
k2: 50 67 88 14 6F 38 37 13 58 6E 82 1F 63 35 39 1C
k3: 4E B1 03 A8 21 89 34 BB 79 E7 B6 A4 1A D2 8F B8
k4: A0 1E 08 67 81 97 3C DC F8 70 8A 78 E2 A2 05 C0
k5: F2 14 89 C9 73 83 B5 15 8B F3 3F 6D 69 51 3A AD
k6: F3 0D E8 A1 80 8E 5D B4 0B 7D 62 D9 62 2C 58 74
k7: 63 B7 42 FE E3 39 1F 4A E8 44 7D 93 8A 68 25 E7
k8: D1 31 1C E1 32 08 03 AB DA 4C 7E 38 50 24 5B DF
k9: 0D 58 28 04 3F 50 2B AF E5 1C 55 97 B5 38 0E 48
k10: 33 03 67 FB 0C 53 4C 54 E9 4F 19 C3 5C 77 17 8B

Starting state:
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
AR: 00 10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0
1st round
BS: 63 C5 C4 01 44 E5 A6 59 F0 75 20 7B 81 CB 8A B9
SR: 63 E5 20 B9 44 75 8A 01 F0 CB C4 59 81 C5 A6 7B
MC: 97 97 EA F5 9C D6 C1 31 20 73 BF 4A 90 9A 62 F1
AR: AC CD 53 F5 A3 89 7E 36 17 25 0A 46 AB C1 D9 F2
2nd round
BS: 16 A2 B4 D1 07 06 E0 AB 54 86 23 E4 96 7F 27 2E
SR: 16 06 23 2E 07 86 27 D1 54 7F B4 AB 96 A2 E0 E4
MC: 2B 51 24 43 95 54 5B ED 36 3A BE 86 CE 16 D8 30
AR: 7B 36 AC 57 FA 6C 6C FE 6E 54 3C 99 AD 23 E1 2C
3rd round
BS: B1 AB 16 C9 9D F3 F3 93 67 D5 DB 3E 61 85 41 D0
SR: B1 F3 DB D0 9D D5 41 C9 67 85 16 93 61 AB F3 3E
MC: 7C EA 84 5B CD DA 76 A1 23 23 9C FB 15 1C 89 87
AR: 32 5B 87 F3 EC 53 42 1A 5A C4 2A 5F 0F CE 06 3F
4th round
BS: 5C 69 6F 5D BE B4 53 CF 83 7D 0E EC BB 2F 4A 8D
SR: 5C B4 0E 8D BE 7D 4A 5D 83 2F 6F CF BB 69 53 EC

MC: 00 4C 84 A3 0B C7 B0 A8 30 A3 C4 5B 95 70 A7 2F
AR: A0 52 8C C4 8A 50 8C 74 C8 D3 4E 23 77 D2 A2 EF
5 th round
BS: 20 2C A0 7D 1F E5 A0 AA AC 28 ED 85 84 E6 42 E1
SR: 20 E5 ED E1 1F 28 42 7D AC E6 A0 AA 84 2C A0 85
MC: 84 3C 3C 4D 79 F4 34 B1 78 2A F4 E6 BE 5E 67 0A
AR: 76 28 B5 84 0A 77 81 A4 F3 D9 CB 8B D7 0F 5D A7
6 th round
BS: D8 87 FF 8F 23 84 C3 30 5D 27 6E 15 78 BB CD C2
SR: D8 84 6E C2 23 27 CD 8F 5D BB FF 30 78 87 C3 15
MC: 90 47 21 06 6D 52 0F 76 5F 1A AF C3 48 26 A1 E6
AR: 63 4A C9 A7 ED DC 52 C2 54 67 CD 1A 2A 0A F9 92
7 th round
BS: BC 65 F7 C2 9A 95 2C 35 D5 12 A2 CF 0E 23 05 A5
SR: BC 95 A2 A5 9A 12 05 C2 D5 23 F7 35 0E 65 2C CF
MC: C0 D5 82 B9 22 73 23 3D EA 58 A0 26 50 7F 85 22
AR: A3 62 C0 47 C1 4A 3C 77 02 1C DD B5 DA 17 A0 C5
8 th round
BS: 07 5F 81 37 7F 65 DB 84 18 8B D7 FF 25 54 20 7A
SR: 07 65 D7 7A 7F 8B 20 37 18 54 81 84 25 5F DB FF
MC: 0C 29 A5 4F 93 D9 ED 44 C9 50 C2 12 8F EE CD F2
AR: DD 18 B9 AE A1 D1 EE EF 13 1C BC 2A DF CA 96 2D
9 th round
BS: D7 A7 B7 36 51 92 64 E1 E8 8B 48 0E 34 1E 79 4B
SR: D7 92 48 4B 51 8B 79 36 E8 1E B7 E1 34 A7 64 0E
MC: 1B 87 08 D2 97 1D 72 6D 43 0B BB 53 0C 3F 49 83
AR: 16 DF 20 D6 A8 4D 59 C2 A6 17 EE C4 B9 07 47 CB
10 th round
BS: 04 34 C4 E2 CC 4E 3C 35 88 54 64 7D B7 FA 37 6E
SR: 04 4E 64 6E CC 54 37 E2 88 FA C4 35 B7 34 3C 7D
AR: 37 4D 03 95 C0 07 7B B6 61 B5 DD F6 EB 43 2B F6