과제1 : Modified AES 구현

- 수업시간에 배운 AES 암호화를 바탕으로 직접 AES 암호화, 복호화를 수행하는 프로그램을 구현한다.

**제출 기한**

* 11월 3일 일요일 23:59분

**구현 조건**

1. 구현 언어: C, C++로 구현
2. Irreducible Polynomials 변경:
3. S-Box 변경 : 아래에 따로 첨부
4. 컴파일 된 exe파일을 실행시키면 동일 폴더 내에 있는 ‘plain.bin’ 파일과 ‘key.bin’ 파일을 읽어들이고, 이를 암호화, 복호화함. 암호화 후 ‘cipher.bin’ 파일에 암호화 결과 저장, 복호화 후 ‘decrypt.bin’ 파일에 복호화 결과 저장.
5. 암호화, 복호화 과정은 수업시간에 배운 내용과 동일함
6. 아래 결과 출력 예시와 같이 콘솔 화면에 결과물 및 중간 단계 출력.

**제출물**

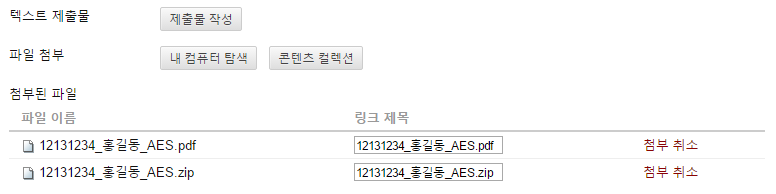
1. 보고서 (pdf 파일로 제출)
2. 압축파일
   1. 보고서 원본 파일(docx, hwp 등)
   2. exe 실행파일
   3. 소스코드 파일

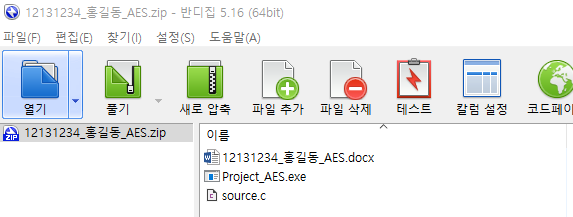
**과제 채점 기준**

* AES 암호화 복호화 구현 (70점)
  + Galois Field 덧셈, 곱셈, 역원 연산 함수 구현(5점)
    - 역원 연산 함수의 경우 S-Box를 직접 계산할 때에만 구현하면 되며, galois field 테이블을 미리 만들지 않고 Extended Euclidean Algorithm으로 구현할 시 추가 점수(+2점)
  + RC, Key Expansion 구현 (10점)
  + Inverse S-Box 구현 (10점)
    - 원본 S-Box를 통해 찾아서 계산하도록 짜면 변동 없음. 프로그램 실행 직후 미리 계산해서 행렬 등에 저장해두는것도 인정(+-0점)
    - Inverse S-box를 따로 계산한 후 코드에 0x12 식으로 하드코딩 시 감점(-3점)
    - S-box, inverse s-box 구현 시 모두 행렬 연산으로 값을 구하도록 구현 시 추가 점수(+5점)
      * 행렬 연산으로 구현하기 위해서는 S-Box를 만들 때에 사용하는 상수 0x63을 0x15로 바꾸면 됨
  + 암호화 구현: Substitute Bytes, Shift Rows, Mix Columns, Add Round Key (30점)
  + 복호화 구현: Inverse Substitute Bytes, Inverse Shift Rows, Inverse Mix Columns (15점)
* 보고서 (20점)
  + 구현 환경 및 구현 언어 기재
  + AES 암호화, 복호화 각 단계 설명 및 코드 설명 기재
* 코드 주석 및 제출 방법 숙지 (10점)

**제출방법**

* pdf파일과 압축 파일을 각각 올릴 것. **제출 방법 위반 시 감점 있음**.
* 보고서와 압축파일 이름을 ‘<학번>\_<이름>\_AES.\*’로 지정. (예. 12131234\_홍길동\_AES.pdf)





**참고자료**

* NIST Specification: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
* AES Wikipedia: <https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

**변경된 S-Box**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **00** | **01** | **02** | **03** | **04** | **05** | **06** | **07** | **08** | **09** | **0A** | **0B** | **0C** | **0D** | **0E** | **0F** |
| **00** | 15 | 0A | 3B | 21 | 02 | C7 | 0F | BC | 3F | 72 | DD | 8A | 18 | 99 | C1 | 5B |
| **10** | A1 | 2F | A6 | 4F | D0 | 01 | DA | 50 | 32 | 26 | 53 | 09 | 7F | 60 | 93 | 3A |
| **20** | EE | CE | A9 | BB | CC | C2 | 38 | F8 | F7 | CD | BE | FB | F2 | 20 | 16 | 22 |
| **30** | 86 | 91 | 2D | 03 | 97 | 23 | BA | 75 | 81 | 17 | AF | 44 | 56 | 04 | 82 | 19 |
| **40** | E8 | 11 | 59 | 05 | EA | D6 | E3 | E5 | 58 | C4 | FE | D5 | 83 | 1B | 42 | 9F |
| **50** | 64 | 88 | D8 | 69 | C0 | D9 | C3 | FD | 47 | 35 | 8F | FC | 94 | 9B | 8E | 07 |
| **60** | 7D | 54 | 57 | A3 | A8 | 4E | BF | 71 | F5 | B1 | 0E | D2 | 63 | 37 | 84 | A7 |
| **70** | 5F | C6 | 14 | CA | 48 | 10 | BD | 06 | B4 | E7 | 9D | A2 | DE | B0 | B2 | AC |
| **80** | 4A | 43 | B6 | D7 | 92 | F4 | 1D | 76 | 4B | 31 | 55 | 85 | CF | 87 | 6D | ED |
| **90** | 12 | 70 | 5C | 9A | E0 | 9E | D4 | 78 | 5E | 25 | B3 | 7A | 1F | 33 | F1 | E9 |
| **A0** | 0C | 89 | DB | 2A | F3 | 46 | 2B | 3E | FF | 08 | 73 | 6E | 7E | DC | 61 | E2 |
| **B0** | 3C | 7B | A4 | C8 | F9 | 8D | E1 | 0B | 74 | 0D | 52 | B7 | 79 | 96 | 1C | 39 |
| **C0** | 80 | 68 | B5 | 28 | 34 | 24 | EF | 2C | 6A | 45 | B8 | 8B | 40 | DF | 27 | AB |
| **D0** | 65 | AD | E6 | EB | 98 | 1E | F6 | D1 | 2E | 62 | A5 | 5A | 7C | AA | 4C | 3D |
| **E0** | 30 | E4 | 5D | 77 | 95 | D3 | FA | 90 | 1A | EC | 36 | CB | 41 | 8C | 9C | 49 |
| **F0** | C5 | B9 | 6C | A0 | F0 | 00 | 6F | 6B | 51 | 4D | 66 | 13 | 67 | 29 | C9 | AE |

**AES 결과 출력 예제**

|  |
| --- |
| RC: 01 02 04 08 10 20 40 80 4D 9A  PLAIN: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF  KEY: 00 10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0  <------ ENCRYPTION ------>  KEY EXPANSION  ROUND 0: 00 10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0  ROUND 1: 64 20 E5 B0 24 70 85 C0 A4 E0 25 70 64 30 C5 80  ROUND 2: E0 04 AF 18 C4 74 2A D8 60 94 0F A8 04 A4 CA 28  ROUND 3: 17 BC 58 1A D3 C8 72 C2 B3 5C 7D 6A B7 F8 B7 42  ROUND 4: 4E B7 01 11 9D 7F 73 D3 2E 23 0E B9 99 DB B9 FB  ROUND 5: 04 BA 12 34 99 C5 61 E7 B7 E6 6F 5E 2E 3D D6 A5  ROUND 6: 20 4C 54 22 B9 89 35 C5 0E 6F 5A 9B 20 52 8C 3E  ROUND 7: B8 83 D6 CC 01 0A E3 09 0F 65 B9 92 2F 37 35 AC  ROUND 8: 4D A0 A8 EE 4C AA 4B E7 43 CF F2 75 6C F8 C7 D9  ROUND 9: 51 8C CA 8D 1D 26 81 6A 5E E9 73 1F 32 11 B4 C6  ROUND 10: E4 75 25 A0 F9 53 A4 CA A7 BA D7 D5 95 AB 63 13  Round 0  AR: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Round 1  SB: 15 0A 3B 21 02 C7 0F BC 3F 72 DD 8A 18 99 C1 5B  SR: 15 C7 DD 5B 02 72 C1 21 3F 99 3B BC 18 0A 0F 8A  MC: A8 A7 C8 93 72 C9 DC F7 1F B1 59 D6 AB 97 DF 74  AR: CC 87 2D 23 56 B9 59 37 BB 51 7C A6 CF A7 1A F4  Round 2  SB: 40 76 20 BB C3 0D 35 75 B7 88 DE 2B AB 3E 53 F0  SR: 40 0D DE F0 C3 88 53 BB B7 3E 20 75 AB 76 35 2B  MC: B9 85 E1 BE F6 D0 6D E8 34 DE 56 60 9F 33 CA A5  AR: 59 81 4E A6 32 A4 47 30 54 4A 59 C8 9B 97 00 8D  Round 3  SB: 35 43 42 2B 2D F3 E5 86 C0 FE 35 6A 7A 78 15 87  SR: 35 F3 35 87 2D FE 15 2B C0 78 42 86 7A 43 E5 6A  MC: 80 46 68 DA 2B 88 84 CA 81 70 FB 76 BE F4 00 FC  AR: 97 FA 30 C0 F8 40 F6 08 32 2C 86 1C 09 0C B7 BE  Round 4  SB: 78 66 86 80 51 E8 6F 3F 2D F2 1D 7F 72 18 0B 1C  SR: 78 E8 1D 1C 51 F2 0B 80 2D 18 86 3F 72 66 6F 7F  MC: 84 DE 8E 45 72 65 78 47 CB E5 35 97 5E 70 4B 61  AR: CA 69 8F 54 EF 1A 0B 94 E5 C6 3B 2E C7 AB F2 9A  Round 5  SB: B8 B1 ED C0 49 53 8A E0 D3 EF 44 16 2C 6E 6C B3  SR: B8 53 44 B3 49 EF 6C C0 D3 6E ED E0 2C B1 8A 16  MC: 3F 61 FB B9 42 AE 73 95 54 95 47 36 5A C6 FE 63  AR: 3B DB E9 8D DB 6B 12 72 E3 73 28 68 74 FB 28 C6  Round 6  SB: 44 5A EC 87 5A D2 A6 14 77 CA F7 F5 48 13 F7 EF  SR: 44 D2 F7 EF 5A CA F7 87 77 13 EC 14 48 5A A6 F5  MC: AB 16 49 7A D7 50 F7 90 23 3C CD 4E 2D AE 41 83  AR: 8B 5A 1D 58 6E D9 C2 55 2D 53 97 D5 0D FC CD BD  Round 7  SB: 85 8F 60 47 84 62 B5 D9 20 69 78 1E 99 67 DF 96  SR: 85 62 78 96 84 69 DF 47 20 67 60 D9 99 8F B5 1E  MC: 0F 5F E0 B9 66 3D D7 F9 50 97 A1 98 08 46 13 E0  AR: B7 DC 36 75 67 37 34 F0 5F F2 18 0A 27 71 26 4C  Round 8  SB: 0B 7C BA 10 71 75 97 C5 07 6C 32 DD F8 C6 38 83  SR: 0B 75 32 83 71 6C 38 10 07 C6 BA C5 F8 7C 97 DD  MC: 38 34 D2 11 7E F1 5D E7 76 80 FA B2 73 29 CD 59  AR: 75 94 7A FF 32 5B 16 00 35 4F 08 C7 1F D1 0A 80  Round 9  SB: 10 E0 9D AE 2D FC DA 15 23 9F 3F 2C 3A AD DD 4A  SR: 10 FC 3F 4A 2D 9F DD AE 23 AD 9D 15 3A E0 DA 2C  MC: 1C AE 4C 67 C5 DA FA 24 74 CB C6 7F EF B8 57 2C  AR: 4D 22 86 EA D8 FC 7B 4E 2A 22 B5 60 DD A9 E3 EA  Round 10  SB: 1B A9 1D 36 2E 67 A2 42 BE A9 8D 7D AA 08 77 36  SR: 1B 67 8D 36 2E A9 77 36 BE 08 1D 42 AA A9 A2 7D  AR: FF 12 A8 96 D7 FA D3 FC 19 B2 CA 97 3F 02 C1 6E  CIPHER: FF 12 A8 96 D7 FA D3 FC 19 B2 CA 97 3F 02 C1 6E  <------ DECRYPTION ------>  Round 0  AR: 1B 67 8D 36 2E A9 77 36 BE 08 1D 42 AA A9 A2 7D  Round 1  SR: 1B A9 1D 36 2E 67 A2 42 BE A9 8D 7D AA 08 77 36  SB: 4D 22 86 EA D8 FC 7B 4E 2A 22 B5 60 DD A9 E3 EA  AR: 1C AE 4C 67 C5 DA FA 24 74 CB C6 7F EF B8 57 2C  MC: 10 FC 3F 4A 2D 9F DD AE 23 AD 9D 15 3A E0 DA 2C  Round 2  SR: 10 E0 9D AE 2D FC DA 15 23 9F 3F 2C 3A AD DD 4A  SB: 75 94 7A FF 32 5B 16 00 35 4F 08 C7 1F D1 0A 80  AR: 38 34 D2 11 7E F1 5D E7 76 80 FA B2 73 29 CD 59  MC: 0B 75 32 83 71 6C 38 10 07 C6 BA C5 F8 7C 97 DD  Round 3  SR: 0B 7C BA 10 71 75 97 C5 07 6C 32 DD F8 C6 38 83  SB: B7 DC 36 75 67 37 34 F0 5F F2 18 0A 27 71 26 4C  AR: 0F 5F E0 B9 66 3D D7 F9 50 97 A1 98 08 46 13 E0  MC: 85 62 78 96 84 69 DF 47 20 67 60 D9 99 8F B5 1E  Round 4  SR: 85 8F 60 47 84 62 B5 D9 20 69 78 1E 99 67 DF 96  SB: 8B 5A 1D 58 6E D9 C2 55 2D 53 97 D5 0D FC CD BD  AR: AB 16 49 7A D7 50 F7 90 23 3C CD 4E 2D AE 41 83  MC: 44 D2 F7 EF 5A CA F7 87 77 13 EC 14 48 5A A6 F5  Round 5  SR: 44 5A EC 87 5A D2 A6 14 77 CA F7 F5 48 13 F7 EF  SB: 3B DB E9 8D DB 6B 12 72 E3 73 28 68 74 FB 28 C6  AR: 3F 61 FB B9 42 AE 73 95 54 95 47 36 5A C6 FE 63  MC: B8 53 44 B3 49 EF 6C C0 D3 6E ED E0 2C B1 8A 16  Round 6  SR: B8 B1 ED C0 49 53 8A E0 D3 EF 44 16 2C 6E 6C B3  SB: CA 69 8F 54 EF 1A 0B 94 E5 C6 3B 2E C7 AB F2 9A  AR: 84 DE 8E 45 72 65 78 47 CB E5 35 97 5E 70 4B 61  MC: 78 E8 1D 1C 51 F2 0B 80 2D 18 86 3F 72 66 6F 7F  Round 7  SR: 78 66 86 80 51 E8 6F 3F 2D F2 1D 7F 72 18 0B 1C  SB: 97 FA 30 C0 F8 40 F6 08 32 2C 86 1C 09 0C B7 BE  AR: 80 46 68 DA 2B 88 84 CA 81 70 FB 76 BE F4 00 FC  MC: 35 F3 35 87 2D FE 15 2B C0 78 42 86 7A 43 E5 6A  Round 8  SR: 35 43 42 2B 2D F3 E5 86 C0 FE 35 6A 7A 78 15 87  SB: 59 81 4E A6 32 A4 47 30 54 4A 59 C8 9B 97 00 8D  AR: B9 85 E1 BE F6 D0 6D E8 34 DE 56 60 9F 33 CA A5  MC: 40 0D DE F0 C3 88 53 BB B7 3E 20 75 AB 76 35 2B  Round 9  SR: 40 76 20 BB C3 0D 35 75 B7 88 DE 2B AB 3E 53 F0  SB: CC 87 2D 23 56 B9 59 37 BB 51 7C A6 CF A7 1A F4  AR: A8 A7 C8 93 72 C9 DC F7 1F B1 59 D6 AB 97 DF 74  MC: 15 C7 DD 5B 02 72 C1 21 3F 99 3B BC 18 0A 0F 8A  Round 10  SR: 15 0A 3B 21 02 C7 0F BC 3F 72 DD 8A 18 99 C1 5B  SB: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  AR: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF  DECRYPTED: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF |