암호화(AES-128-CBC)

C소스 및 알고리즘 보고서

20208 김승호

차 례

1. 암호화 알고리즘 분석

2. 암호화 소스 분석

1. 암호화 알고리즘 분석

1) 전체적인 알고리즘

Initial round - 평문을 입력 받은 키 값과 XOR연산

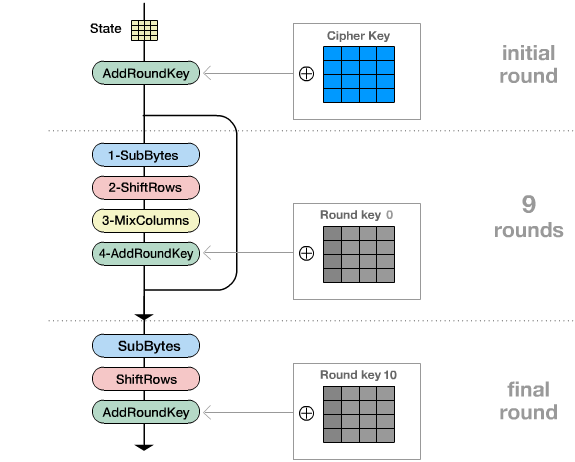
0 ~ 9 rounds - sbox에 대입하여 SubBytes 알고리즘 수행

- 정해진 규칙에 따라 행을 이동하여 ShiftRows 알고리즘 수행

- 정해진 규칙과 rcon을 통하여 연산하여 MixColumns 알고리즘수행

- key 스케줄링을 통하여 생성된 키와 XOR 연산

final round - Mixcolumns를 제외하고 위의 단계 수행

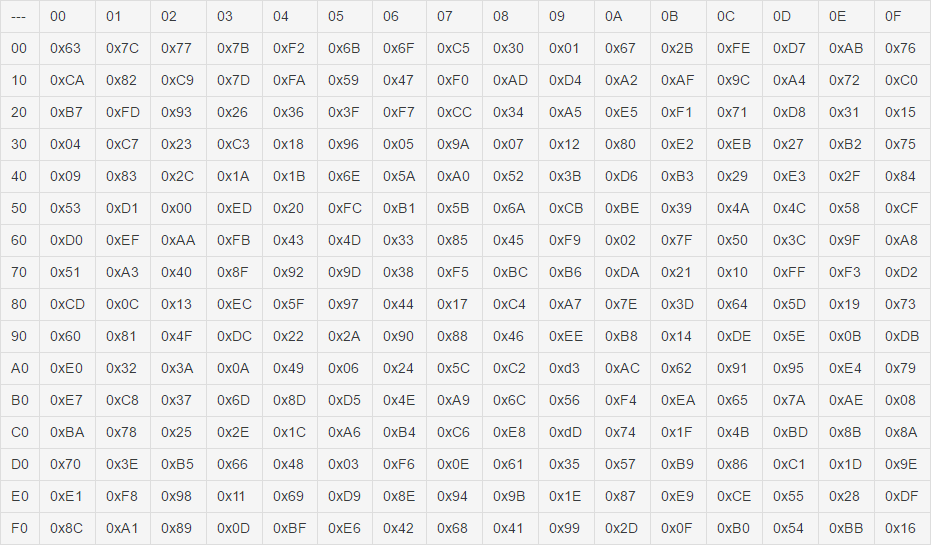


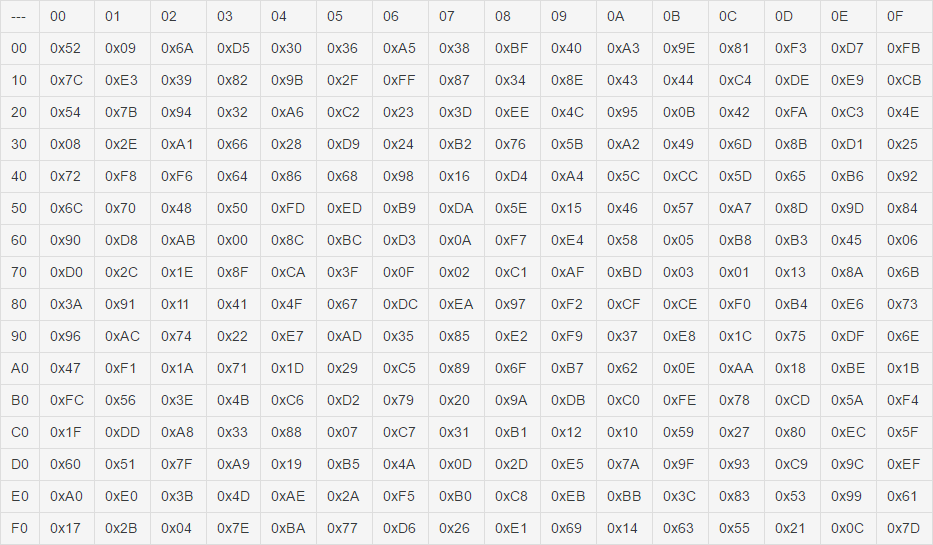
2) Subbytes

- 문자를 0x00형태로 변환해서 s-box에 해당 좌표의 값으로 치환

- ex : 0x7A = 0xDA

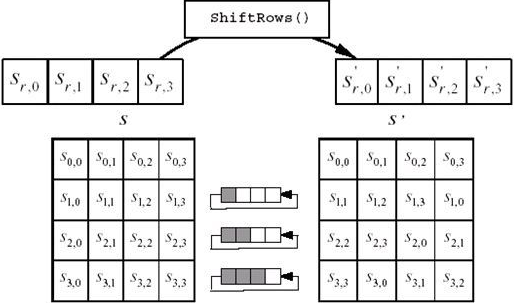
- s-box, inv s-box

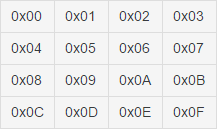
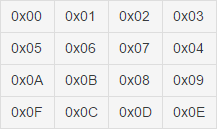




3) ShiftRows

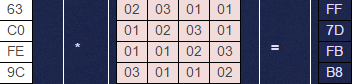
- 4 x 4 배열의 값을 정해진 규칙으로 치환하는 과정

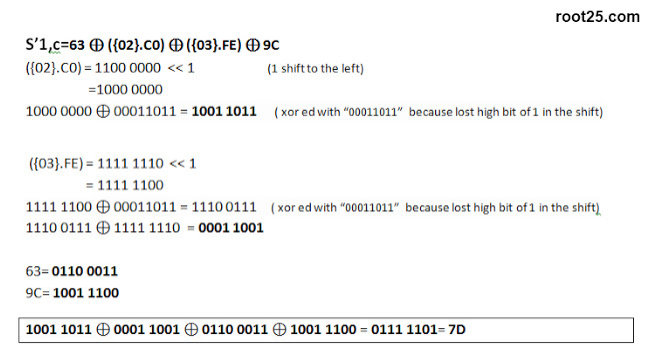


 -> 

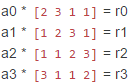
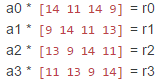
4) MixColumns

- 아래의 예시와 같이 4 x 4 배열의 모든 값 치환





- MixColumns 표

(encode) (decode)

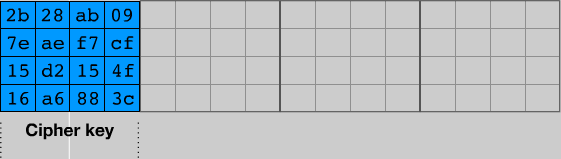
5) RoundKey

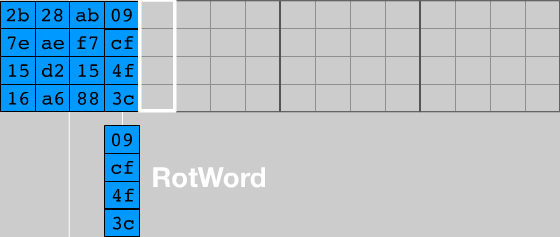
- 키 스케줄링은 두 가지로 나뉘어진다.

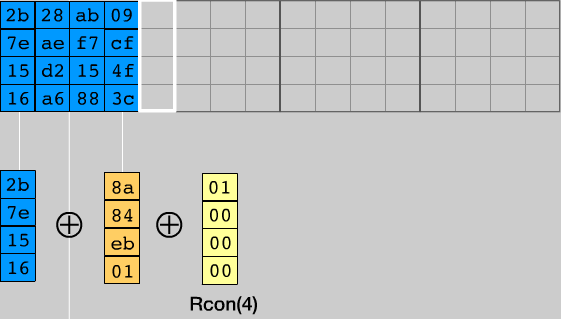
- W4, W8, … , W40에서 쓰이는 스케줄링(Rcon 필요)과 그 외의 스케줄링

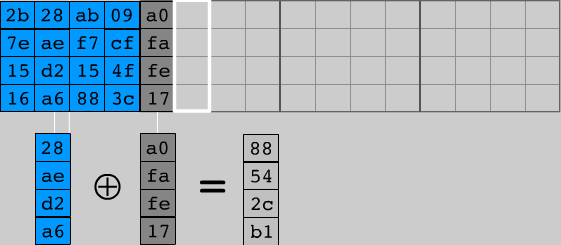
-  Rcon

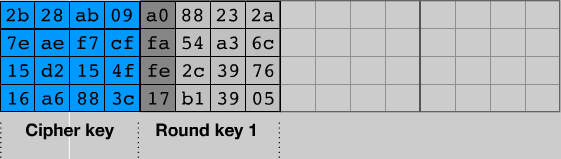
- 순서

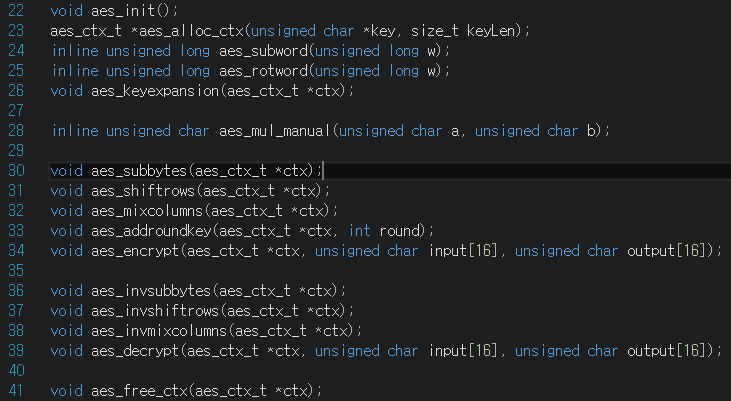
1 - 

2 - 

3 - 

4 - 

5 - 

2. 암호화 소스 분석 

- 22, 28 : s-box, inv s-box 생성 함수 및 연산 함수

- 23 : key의 길이의 따른 bit변경 및 라운드 변경 함수(만들어 두긴 했지만 16bit 버전에 초점을 둠)

- 24 ~ 26 : 라운드 키 연산 함수

- 30 ~ 33 : 암호화 라운드 별 필요 알고리즘 함수

- 34 : 암호화 필요 알고리즘 호출 함수

- 36 ~ 38 : 복호화 라운드 별 필요 알고리즘 함수

- 39 : 복호화 필요 알고리즘 호출 함수

- 41 : 메모리 정리 함수