2023/01/12, 2023 겨울방학 보안기초 세미나

Network Security Essential

- Chapter 2.1 ~ Chapter 2.3 -

강 민 채(minchae@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

목 차

대칭 암호 원리

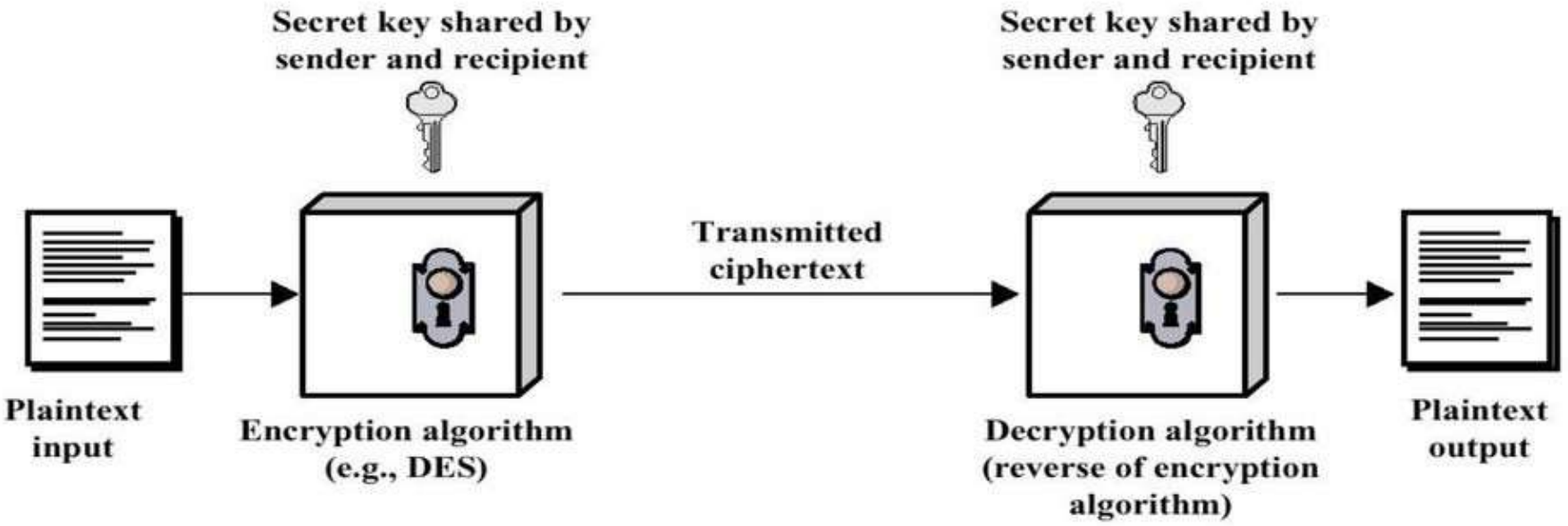
- 대칭 암호
  - 정의
    - 암호화 시 사용하는 키와 복호화 시 사용하는 키가 동일한 암호 알고리즘
  - 특징
    - 관용 암호, 비밀 키 암호, 단일 키 암호라고도 불림
    - 키 크기가 상대적으로 작고 알고리즘 내부 구조가 단순하여 암호화와 복호화 속도가 상대적으로 빠른 편임

대칭 암호 원리

- 대칭 암호 요소
  - 평문(Plaintext)
    - 알고리즘의 입력으로 이용되는 원문
  - 비밀 키(Secret Key)
    - 공개되지 않고 송수신자가 비밀리에 사용하는 키
  - 암호 알고리즘(Encryption Algorithm)
    - 입력으로 들어온 평문을 치환, 변환하는 알고리즘
  - 암호문(Ciphertext)
    - 암호 알고리즘으로 암호화 된 메시지
  - 복호 알고리즘(Decryption Algorithm)
    - 암호화 시 사용했던 동일한 키를 이용하여 암호 알고리즘을 역수행하여 원문을 복구하는 알고리즘

대칭 암호 원리

- 대칭 암호 모델



대칭 암호 원리

- 대칭 키 암호를 안전하게 사용하기 위한 조건
  - 강한 암호 알고리즘이 있어야 한다
    - 강한 암호 알고리즘이란, 공격자가 암호문과 알고리즘을 알고 있어도 위험이 적을 만큼 안전하게 설계된 알고리즘을 뜻함
  - 송수신자는 공유하는 비밀 키를 안전하게 획득, 보관해야 한다
    - 공격자에게 비밀 키가 노출되면 그 키를 이용한 모든 통신은 노출될 수 있음

대칭 암호 원리

- 암호 시스템 구분 기준
  - 평문을 암호문으로 전환하는데 사용되는 연산 유형
    - 대체
      - 평문의 각 요소를 다른 요소로 바꾸는 것
    - 치환
      - 요소의 순서를 재조정하는 것
  - 평문 처리 방법
    - 블록 암호
      - 한 번에 한 블록씩 입력하여 처리하고 한 블록씩 출력하는 것
    - 스트림 암호
      - 입력 요소를 연속적으로 처리하여 입력 요소가 끝날 때까지 한 번에 한 요소씩 출력하는 것

대칭 암호 원리

- 암호 해독
  - 정의
    - 데이터를 암호화한 암호문을 원문으로, 즉 원래의 형태로 복구하는 것
- 전수 공격
  - 정의
    - 모든 가능한 경우의 수를 다 시도하는 공격 기법
  - 특징
    - 모든 경우의 수를 다 시도할 경우, 공격에 성공할 확률이 100%임
    - 가능한 경우의 수의 크기에 따라 실용성이 달라짐
    - 암호를 해독하는데 드는 시간과 비용을 정량화 할 수 있는 공격임
    - 암호문을 통해 평문을 알아내고자 하는 공격일 경우, 평문이 의미 있는 평문인지 구별해 내는 기술이 중요함

대칭 암호 원리

- 암호 해독 공격 유형

공격 유형	암호 해독가가 알고 있는 정보
암호문만 알고 있는 공격 * 전수 공격 이용 가능	- 암호 알고리즘 - 해독해야 할 암호문
알려진 평문 공격 * 예측되는 단어 공격	- 암호 알고리즘 - 해독해야 할 암호문 - 비밀 키로 만들어진 한 쌍 혹은 여러 쌍의 평문-암호문
선택 평문 공격	- 암호 알고리즘 - 해독해야 할 암호문 - 해독가가 선택한 평문 메시지와 비밀 키로 그 평문을 암호화 한 암호문
선택 암호문 공격	- 암호 알고리즘 - 해독해야 할 암호문 - 해독가가 목적을 갖고 선택한 암호문과 비밀 키로 그 암호문을 복호화한 평문
선택문 공격	- 암호 알고리즘 - 해독해야 할 암호문 - 해독가가 선택한 평문 메시지와 비밀 키로 그 평문을 암호화 한 암호문 - 해독가가 목적을 갖고 선택한 암호문과 비밀 키로 그 암호문을 복호화한 평문

대칭 암호 원리

- 암호 구조의 안전 조건
  - 암호문을 깨는데 드는 비용이 암호화된 정보의 가치보다 클 경우
  - 암호문을 깨는데 걸리는 시간이 행당 정보의 수명보다 길 경우

- 모든 키를 시도해보는 데 걸리는 평균 시간

키 길이 (비트)	암호	키의 종류 수	10^9 복호화/초 속도로 처리할 경우 소요시간	10^{13} 복호화/초 속도로 처리할 경우 소요시간
56	DES	2^{56}	1.125년	1시간
128	AES	2^{128}	5.3×10^{21}년	5.3×10^{17}년
168	삼중 DES	2^{168}	5.8×10^{33}년	5.8×10^{29}년
192	AES	2^{192}	9.8×10^{40}년	9.8×10^{36}년
256	AES	2^{256}	1.8×10^{60}년	1.8×10^{56}년

대칭 암호 원리

- 페이스텔 암호 구조
  - 정의
    - 데이터를 두 부분으로 나누어 좌, 우 두 부분에 교대로 비선형 변환을 적용시키는 구조

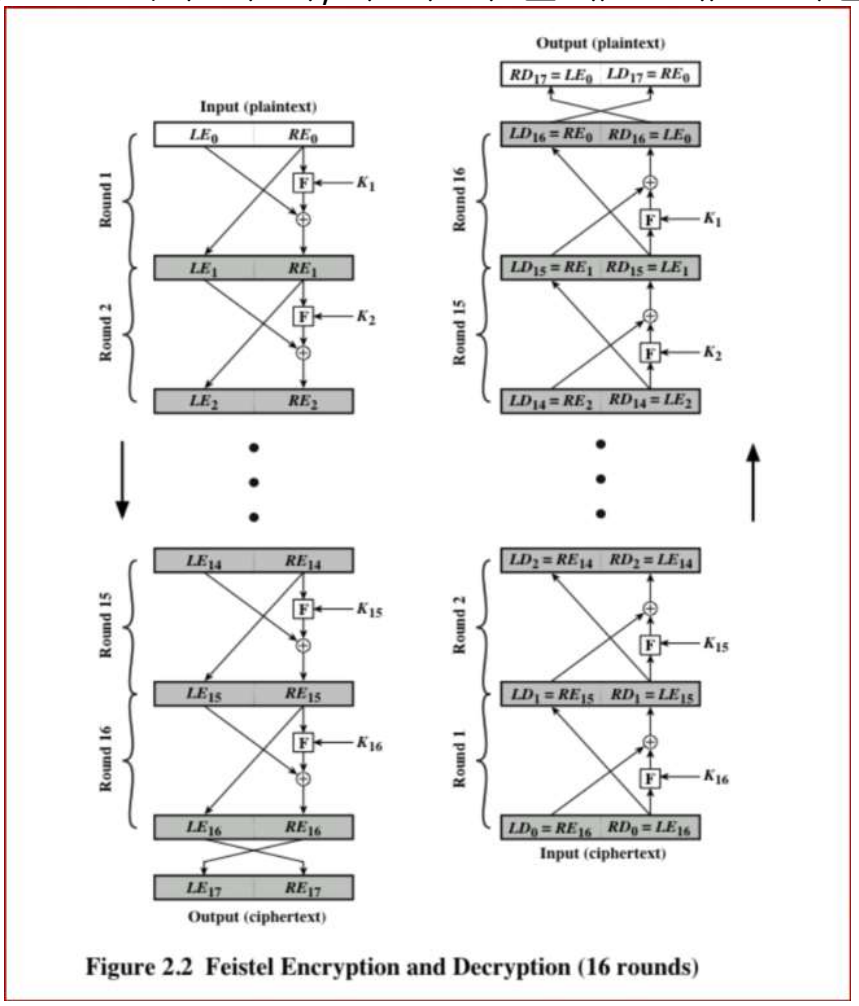
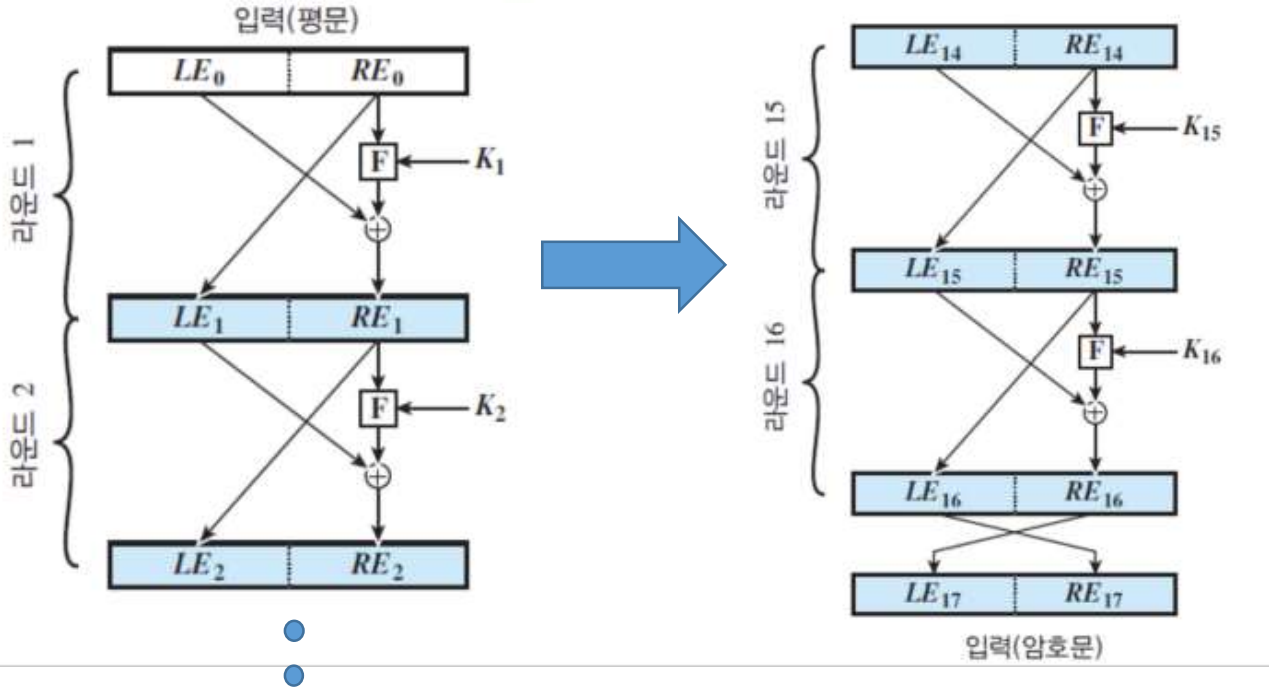


Figure 2.2 Feistel Encryption and Decryption (16 rounds)

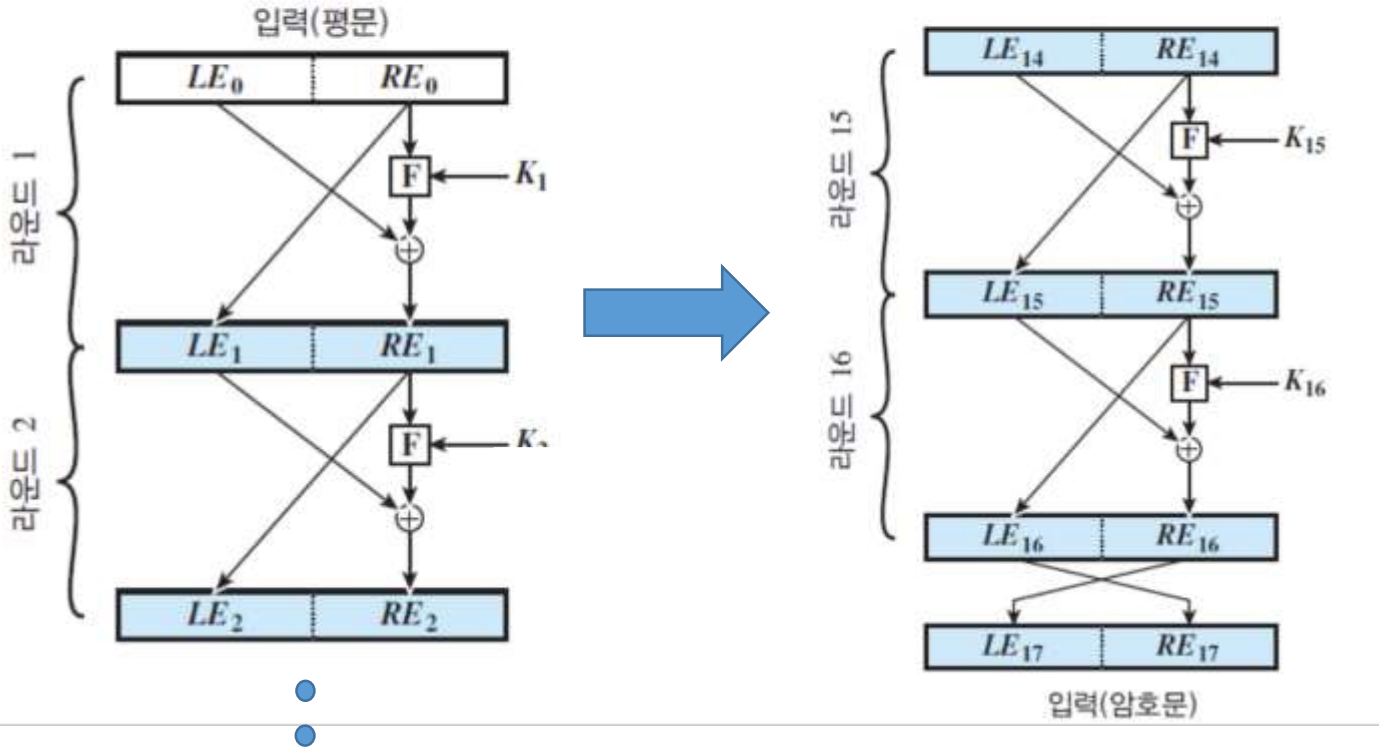
대칭 암호 원리

- 페이스텔 암호 구조
  - 암호화 과정
    - 평문 블록을 두 조각으로 나눈다
    - 왼쪽 반의 데이터를 오른쪽 반의 데이터에 라운드 함수를 적용한 것과 XOR한 것으로 대체한다
      - 라운드 함수를 이용 시, 매 과정 다른 라운드 서브키를 사용한다
    - 두 개의 반쪽짜리 데이터를 치환한다



대칭 암호 원리

- 페이스텔 암호 구조
  - 복호화 과정
    - 근본적으로 암호 과정과 동일하지만, 서브키의 순서를 거꾸로 적용한다



대칭 암호 원리

- 페이스텔 암호에서의 매개변수와 설계 특성
  - 블록 길이
    - 길수록 보안이 강하지만, 암호화/복호화 속도가 떨어짐
    - 64비트 블록 길이가 합리적임
  - 키 길이
    - 길수록 보안이 강하지만, 암호화/복호화 속도가 떨어짐
  - 라운드 수
    - 라운드 수가 증가할수록 보안이 강함
    - 전형적인 라운드 수는 16
  - 서브키 생성 알고리즘
    - 복잡할수록 해독이 어려움
  - 라운드 수
    - 복잡할수록 해독이 어려움

대칭 암호 원리

- 대칭 블록 암호 설계 시 고려 사항
  - 빠른 소프트웨어 암호화/복호화
    - 하드웨어적인 구현이 아닌, 응용 프로그램이나 유틸리티 함수에 암호화를 내장하여 알고리즘의 실행 속도를 고려
  - 용이한 해독
    - 알고리즘 구조를 단순하게 만들어 암호 해독적 취약점을 찾기 쉽게 만듦

목 차

대칭 암호 알고리즘

- DES(Data Encryption Standard)
  - 정의
    - 페이스텔 구조의 대칭 블록 암호 알고리즘의 일종으로, 미국 NBS(National Bureau of Standards, 현재 NIST)에서 국가 표준으로 정한 암호
  - 특징
    - 평문의 길이가 64비트
    - 키 길이가 56비트
    - 16개 서브키 사용
    - 복호화 과정이 암호화 과정과 동일

대칭 암호 알고리즘

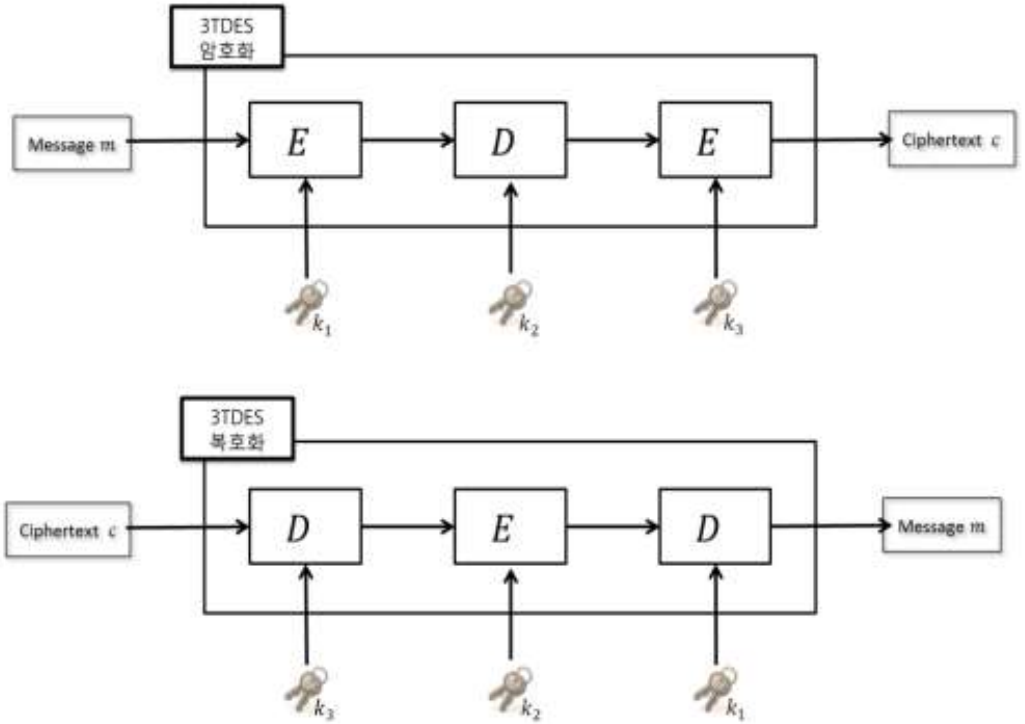
- DES의 강도
  - DES는 수많은 시도에도 취약점이 발견되지 못함
    - 알고리즘의 구조 면에서 보안이 강하다고 볼 수 있음
  - 하지만, 키의 길이가 56비트

➡ 전수 공격 시 일반 컴퓨터로도 몇시간 만에 암호를 해독할 수 있음

즉, 다른 암호 알고리즘 필요

대칭 암호 알고리즘

- 3중 DES
  - 정의
    - DES 알고리즘을 세번 수행한 알고리즘



암호화: 암호-복호-암호

$$C = E(K_3, D(K_2, E(K_1, P)))$$

복호화: 복호-암호-복호

$$P = D(K_1, E(K_2, D(K_3, C)))$$

대칭 암호 알고리즘

- 3중 DES
  - 장점
    - 유효 키 길이가 168비트이므로 전수공격의 위협이 적음
  - 단점
    - DES보다 라운드 수가 3배나 많기 때문에 소프트웨어 구현속도가 상대적으로 느림
    - 64비트 블록을 사용하므로 보안이나 효율성 측면에서 떨어짐

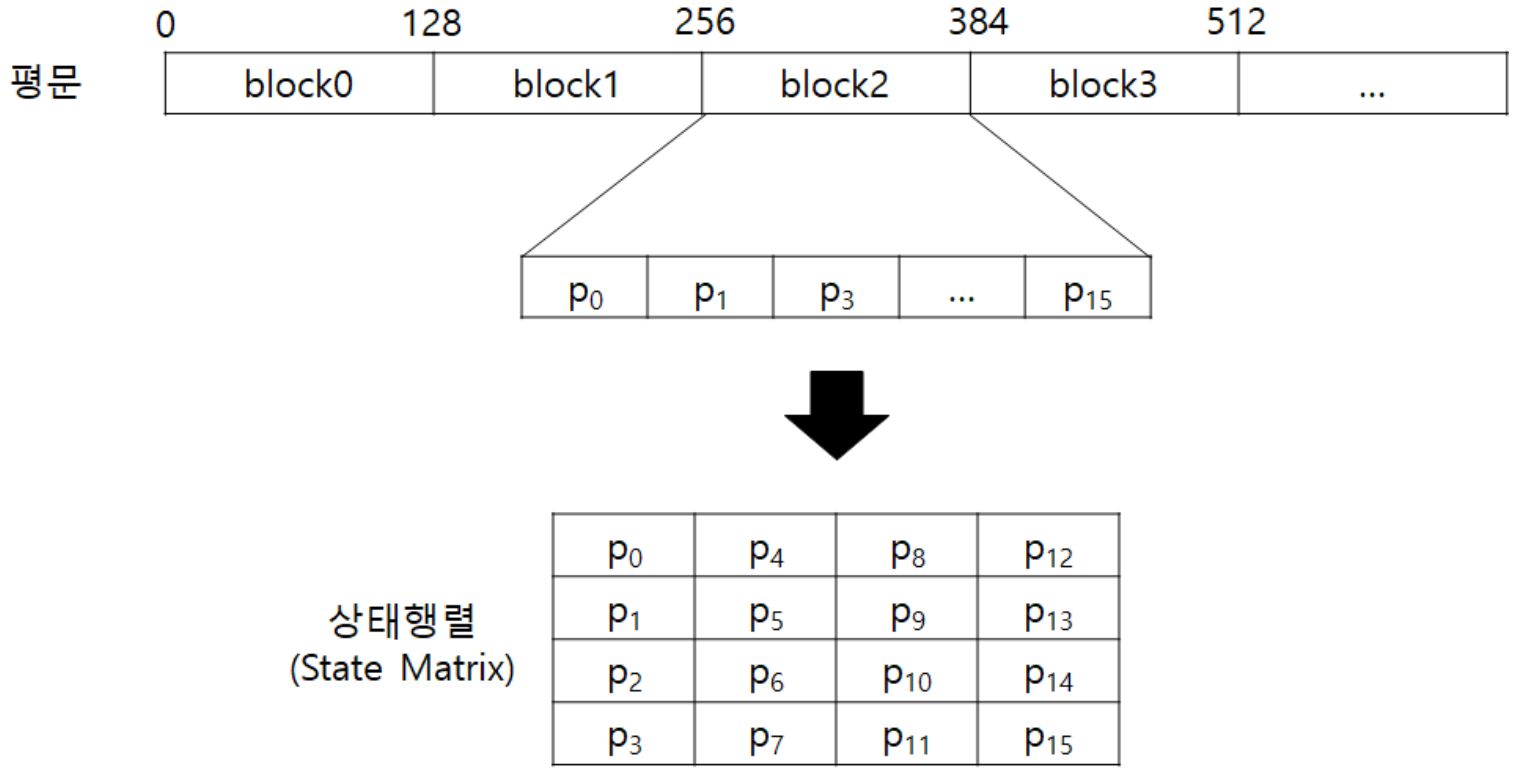
장기적으로 사용될 표준이 되기엔 부적합

대칭 암호 알고리즘

- AES(Advanced Encryption Standard)
  - 정의
    - 미국 NIST에서 DES를 대체하기 위해 공모했던 암호 알고리즘으로, Rijndael이 개발한 알고리즘
  - 특징
    - 페이스텔 구조가 아님
    - 블록 길이가 128비트
    - 키의 길이는 128, 192, 256비트를 지원함
    - 라운드 수
      - 키가 128비트일때 10개
      - 키가 192비트일때 12개
      - 키가 256비트일때 14개

대칭 암호 알고리즘

- AES 암호화 과정
  - 상태행렬(State Array)에 복사

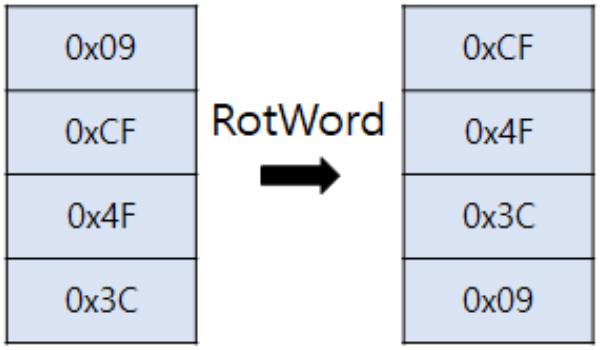


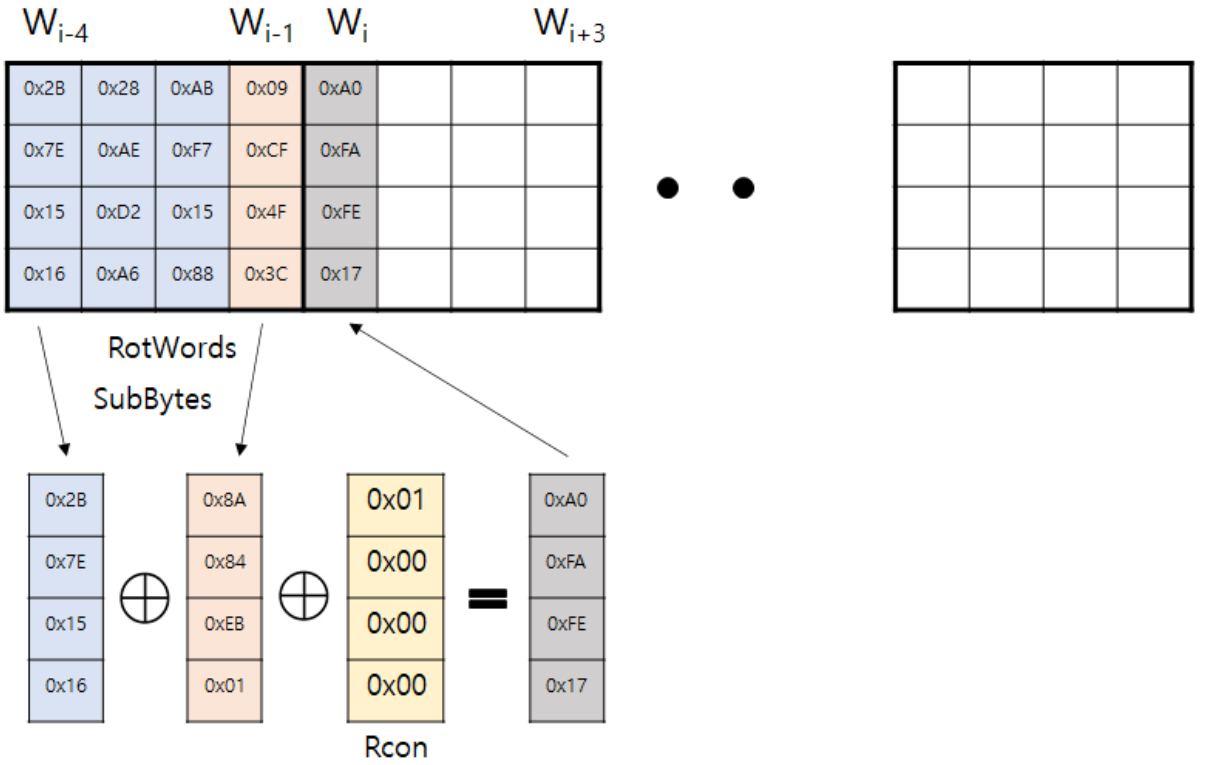
대칭 암호 알고리즘

- AES 암호화 과정
  - 라운드 키 확장
    - 첫번째 열 확장방법

0x01	0x02	0x04	0x08	0x10	0x20	0x40	0x80	0x1B	0x36
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00

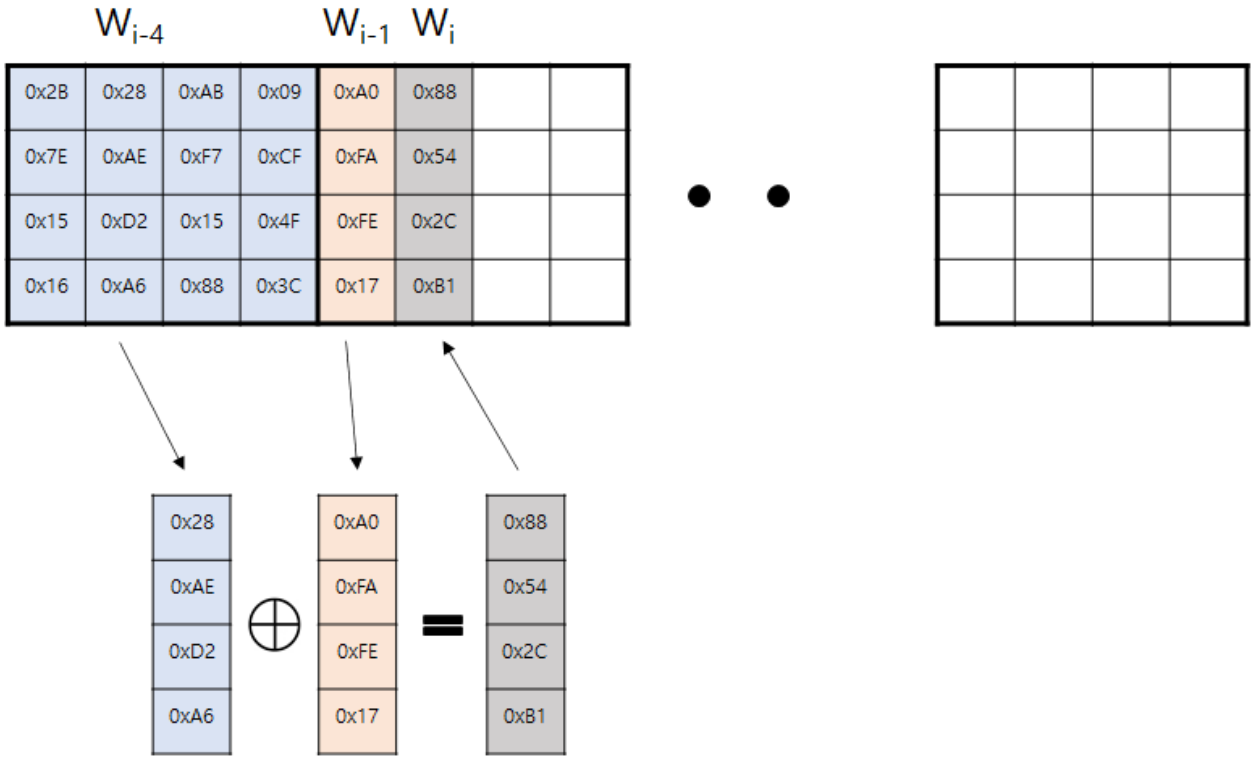
rcon





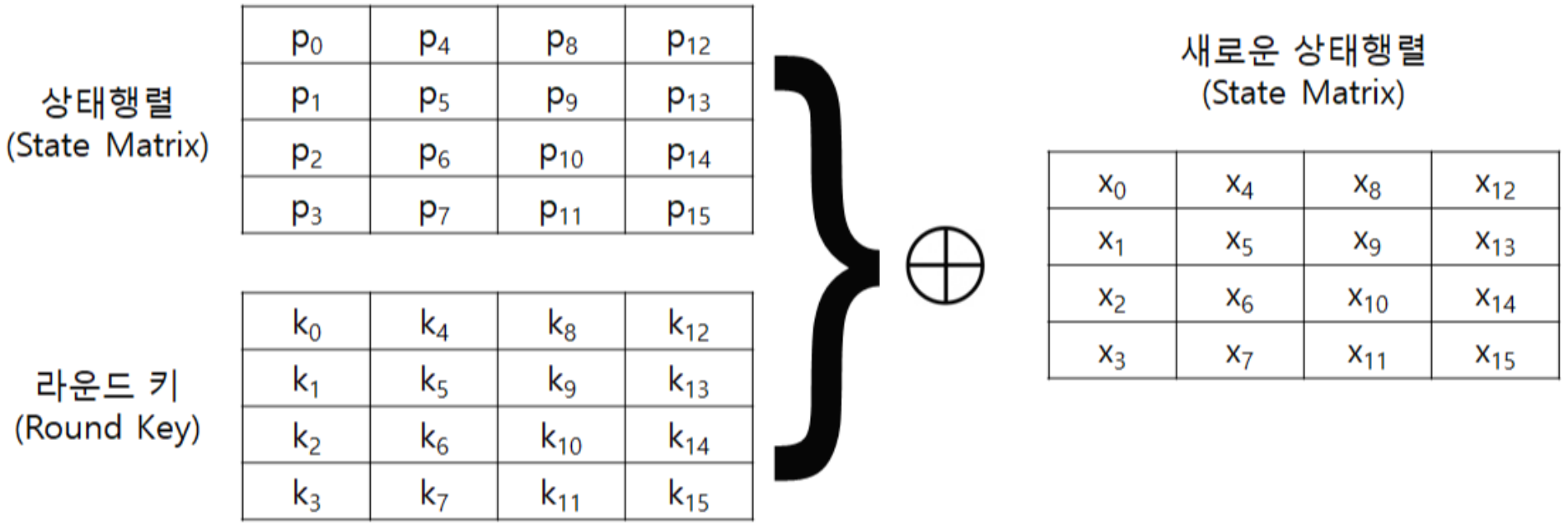
대칭 암호 알고리즘

- AES 암호화 과정
  - 라운드 키 확장
    - 두번째, 세번째, 네번째 열 확장방법



대칭 암호 알고리즘

- AES 암호화 과정
  - 라운드 키 더하기(Add Round Key)
    - 확장된 키와 현재 블록을 XOR 한다



대칭 암호 알고리즘

- AES 암호화 과정
  - 바이트 대체(Substitute Bytes)
    - S-box라는 표를 이용해 블록 교환

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

0x19	0xA0	0x9A	0xE9
0x3D	0xF4	0xC6	0xF8
0xE3	0xE2	0x8D	0x48
0xBE	0x2B	0x2A	0x08

SubBytes

0xD4	0xE0	0xB8	0x1E
0x27	0xBF	0xB4	0x41
0x11	0x98	0x5D	0x52
0xAE	0xF1	0xE5	0x30

대칭 암호 알고리즘

- AES 암호화 과정
  - 행 이동(Shift rows)
    - 첫번째 위치부터 각 행의 위치가 증가되는 수만큼 각 행을 왼쪽으로 이동

0xD4	0xE0	0xB8	0x1E
0x27	0xBF	0xB4	0x41
0x11	0x98	0x5D	0x52
0xAE	0xF1	0xE5	0x30

ShiftRows

0xD4	0xE0	0xB8	0x1E
0xBF	0xB4	0x41	0x27
0x5D	0x52	0x11	0x98
0x30	0xAE	0xF1	0xE5

대칭 암호 알고리즘

- AES 암호화 과정
  - 열 섞기(Mix columns)
    - 열을 고정 행렬과 섞음

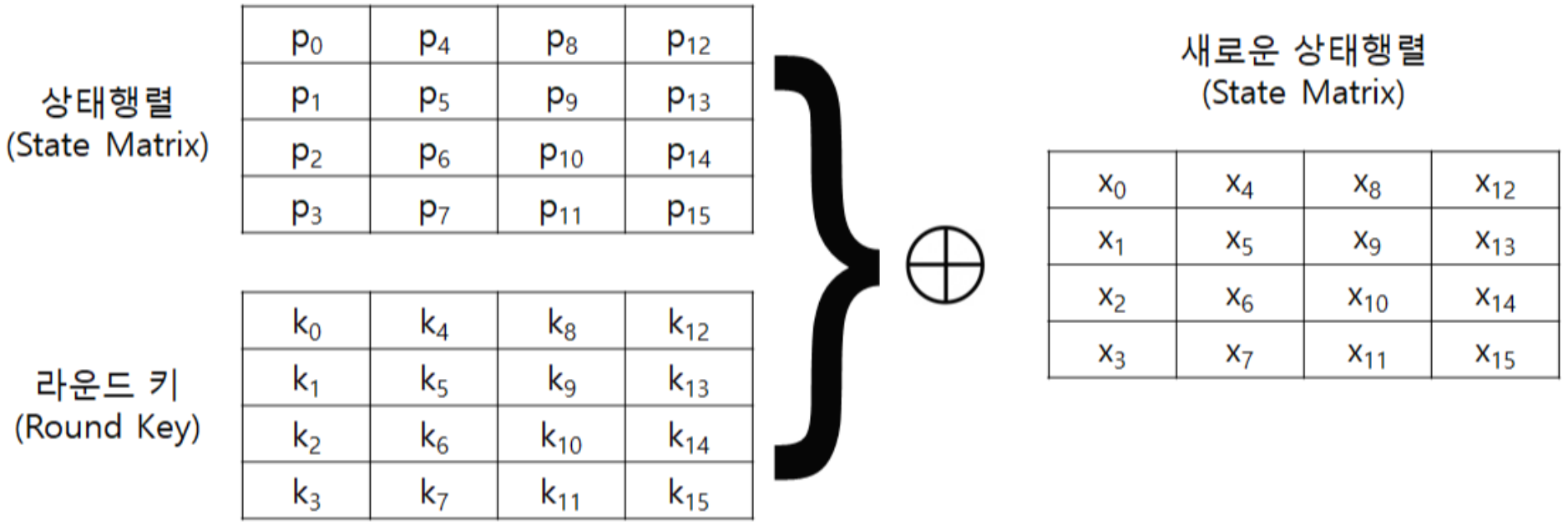
0xD4	0xE0	0xB8	0x1E
0xBF	0xB4	0x41	0x27
0x5D	0x52	0x11	0x98
0x30	0xAE	0xF1	0xE5

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \bullet \begin{bmatrix} 0xD4 \\ 0xBF \\ 0x5D \\ 0x30 \end{bmatrix} = \begin{bmatrix} 0x04 \\ 0x66 \\ 0x81 \\ 0xE5 \end{bmatrix}$$

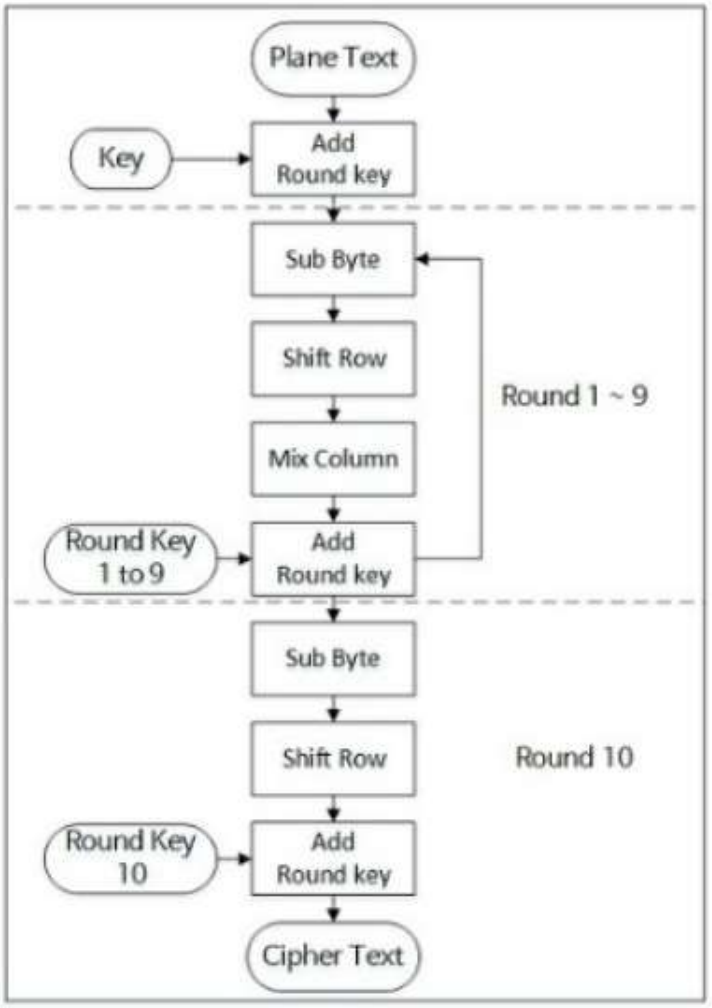
단, 마지막 라운드에서는 이 단계를 건너뜀

대칭 암호 알고리즘

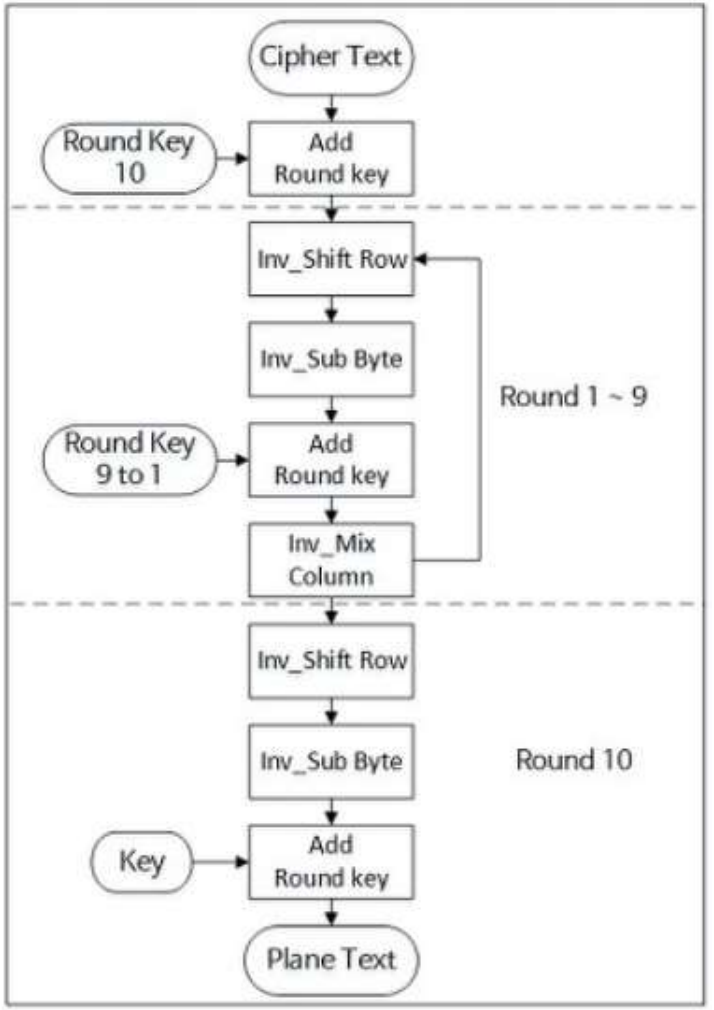
- 라운드 키 더하기(Add round key)
  - 확장된 키의 일부와 현재 블록을 XOR한다



대칭 암호 알고리즘



AES 암호화 알고리즘



AES 복호화 알고리즘

복호화:
A xor B xor B = A
라는 것을 이용하여 같은 라운드 키를 블록에 수행하여 역을 계산

목 차

난수와 의사난수

- 진성난수
  - 정의
    - 정의된 범위내에서 무작위로 선택된 수

- 난수열의 두 가지 조건
  - 무작위성
    - 균등 분포
      - 수열의 비트 분포가 균등해야 함
    - 독립성
      - 수열에서 추출한 어떠한 부분수열도 다른 수열로부터 추론할 수 없어야 함

  - 예측 불가성
    - 수열의 일부를 보고 이어지는 수를 예측할 수 없어야 함

난수와 의사난수

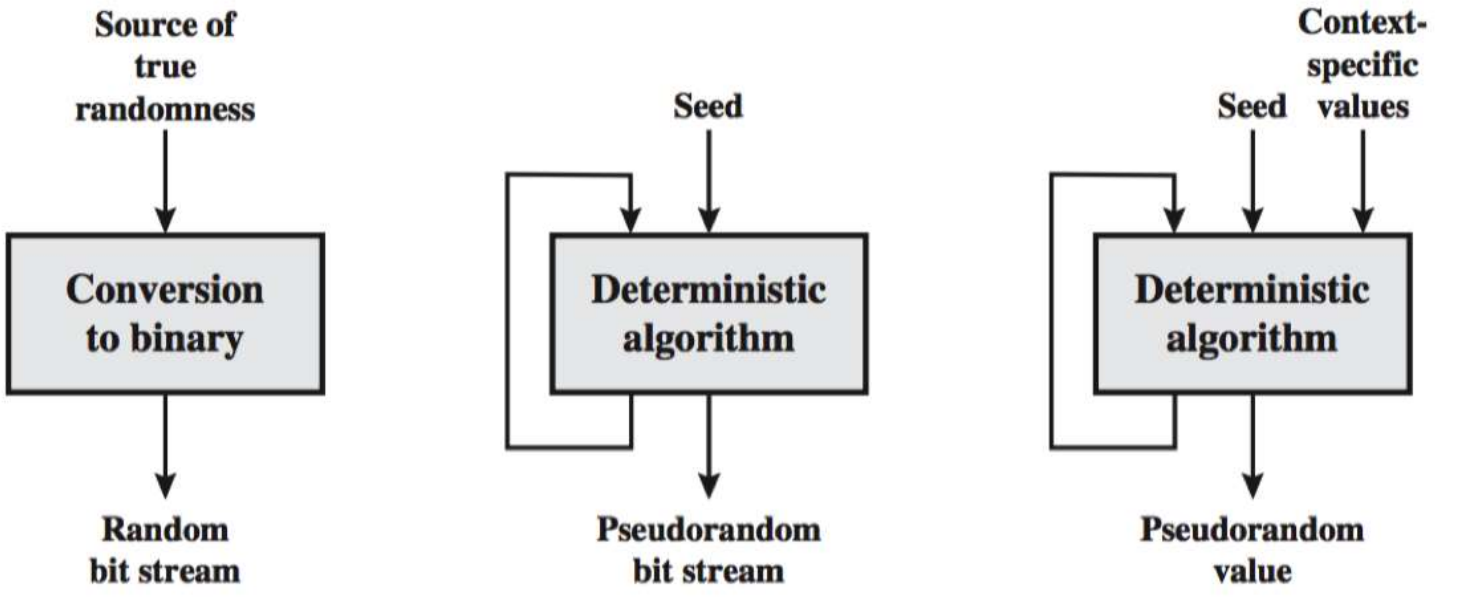
- 의사난수
  - 정의
    - 컴퓨터 알고리즘으로 만들어 낸 난수
  - 특징
    - 무작위해 보이지만 정해진 알고리즘으로 만들기 때문에 진성 난수와 구분됨
    - 잘 만들어진 알고리즘이라면, 무작위성 테스트를 무사히 통과해 실제 사용에 문제가 없음

난수와 의사난수

- 진성난수 생성기(TRNG)
  - 컴퓨터의 물리적 환경에서 얻은 엔트로피 소스(키 입력 타이밍 패턴, 디스크 전기 작용, 마우스 움직임 등)를 입력 값으로 사용
- 의사난수 생성기(PRNG)
  - 무한 비트열을 생성하기 위해 사용되는 알고리즘
- 의사난수 함수(PRF)
  - 고정된 길이 의사난수 비트열을 생성하기 위해 사용되는 함수

난수와 의사난수

- 난수 생성기와 함수



TRNG = true random number generator
PRNG = pseudorandom number generator
PRF = pseudorandom function

Figure 7.1 Random and Pseudorandom Number Generators

난수와 의사난수

- 의사난수 생성기의 알고리즘 종류
  - 기존 암호 알고리즘을 이용한 알고리즘
    - 난수화된 입력 효과를 가지고 있음
  - 특정 목적 알고리즘
    - 의사난수 비트 스트림을 생성하기 위해 특정하게 그 목적만을 위해 설계된 알고리즘

Thanks!

강 민 채 (minchae@pel.sejong.ac.kr)