7. AES(Advanced Encryption Standard)

AES는 DES를 대신한 새 표준이다. - 미국표준기술연구소(NIST)

// AES 기본 사양

AES 종류	암호키	라운드	평문/암호문	라운드 키	라운드 키 수
AES-128	128bit	10	128bit	128bit	11
AES-192	192bit	12	128bit	128bit	13
AES-256	256bit	14	128bit	128bit	15

- AES는 암호키 크기에 따라 라운드 수가 결정된다.
- 라운드 키 크기는 마스터키(암호키) 크기와 무관하게 128비트로 같다.
- AES의 라운드 키 크기는 **평문과 암호문 블록 크기와 같은 128bit**이다.
- 라운드 키 수는 라운드 수 보다 하나 더 많이 필요하다.
  → Pre-round 변환에서 라운드 키가 하나 필요하기 때문이다.
  → Pre-round 변환은 라운드가 시작되기 전에 평문과 xor 연산하는 것이다.

〈AES 특징〉

① AES는 **바이트 기반 암호**이다.
→ 평문 128비트는 16바이트로 간주되고, 바이트 단위의 수학적 변환이 수행된다.

② AES 알고리즘은 **SPN**(Substitution Permutation Network) 구조이다.
→ 암호 알고리즘과 복호 알고리즘은 **유사**하다.**(암복호 알고리즘이 똑 같지는 않다)**
→ 차이점은 **복호** 알고리즘은 **키가 거꾸로 적용**된다.**(Forouzan 암호학 194쪽)**

③ AES의 **S-box**는 내부적으로 **테이블 참조** 또는 **유한체 GF(2^8)**를 사용한다. - **혼돈**
→ 외부 공격으로부터 안전성 확보

// 레인달(Rijndael)

① 미국표준기술연구소(NIST)에서 DES를 대체할 암호를 공모하였다.
→ 공모에 제안된 여러 후보 중에서 레인달(Rijndael)이 최종 선정되었다.

② 레인달(Rijndael)은 벨기에 암호학자인 존 대먼과 빈센트 라이먼에 의해서 개발되었다.
→ AES는 처음에는 두 사람의 이름을 합해서 만든 이름 "레인달"을 사용했다.

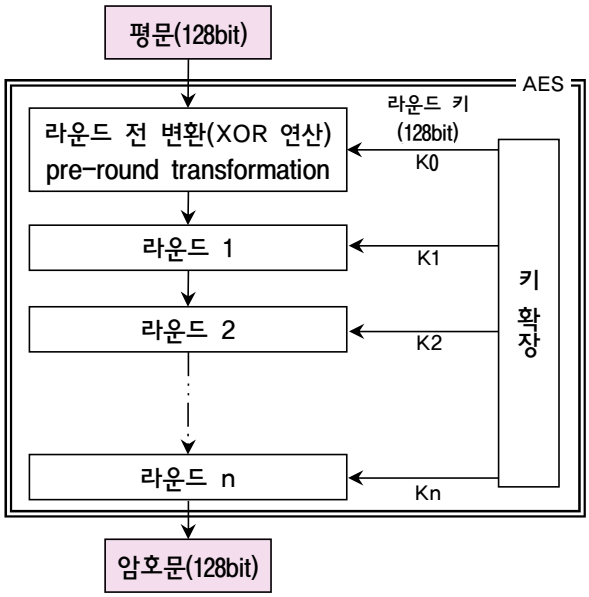
③ 암호의 정식 명칭은 1997년 9월 AES(Advanced Encryption Standard)로 정해졌다.

④ AES 후보 알고리즘들은 다음 3가지 조건을 만족해야 했다.

안전성(security)	전수조사공격, 선형공격과 차분공격에 대한 안전성
비용(cost)	계산 효율성(속도 및 메모리 요구량)
구현(implementation)	알고리즘의 유연성(flexibility)과 단순성(simplicity)

2 http://cafe.daum.net/pass365(홍재연)

// AES 암호 구조도



종류	암호키	라운드	라운드 키 수
AES-128	128bit	10	11
AES-192	192bit	12	13
AES-256	256bit	14	15

- AES는 각 라운드에서 사용할 **라운드 키**를 생성하기 위해 **키 확장** 과정을 거친다.
- **라운드 키**는 **암호키(128bit)**를 이용하여, **키 확장** 과정을 통해 생성된다.
- **라운드 수**가 n이면, **n+1**개의 **라운드 키**를 생성한다.
- **처음** 생성한 **라운드 키(k0)**는 첫 번째 라운드를 **수행하기 전**에 **평문**과 XOR 연산한다.
- 나머지 **라운드 키**는 각 라운드의 마지막 단계에서 XOR 연산한다.

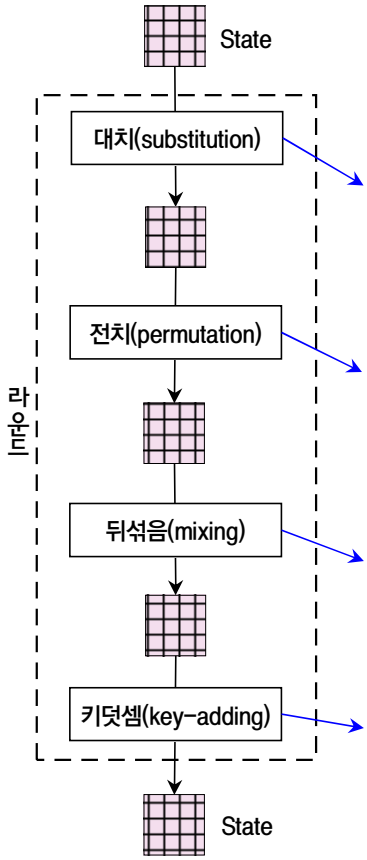
// AES 라운드 함수

AES 암호 알고리즘은 안전성을 위해 각 라운드는 다음 **4가지 단계의 변환**을 적용한다.

① **바이트 치환(substitute byte)**	S-box 표를 이용하여 바이트 단위로 블록 교환**(대치)**
② **행 이동(shift row)**	P-box, 단순히 행과 행을 이동**(전치)**
③ **열 혼합(mix column)**	행렬 곱셈 연산(행렬을 사용하여 열의 각 바이트를 **대치**)
④ **라운드 키 더하기(add round key)**	확장된 키의 일부와 현재 블록을 XOR 연산(**대치**)

- **각 라운드**는 **마지막**을 **제외**하고 **4개의 변환**을 사용한다.
- 암호의 **마지막 라운드**는 MixColumns을 제외한 **3의 변환**을 사용한다.
- 4단계 모두 역 계산이 가능하므로 복호화를 하면 평문을 얻을 수 있다

// AES 라운드 함수의 상태 변환



- **바이트 치환** : 16개의 독립된 **바이트**에 대해 적용(**대치, s-box**)
- 모든 **바이트** 변환은 **하나의 테이블**만 사용한다.
- 변환은 **테이블** 참조 또는 GF(2^8) 상의 수학적 연산으로 정의
- AES는 **역연산**이 가능한 2개의 변환 **테이블**을 사용한다.

- **행 이동**(shift row) : 단순히 행과 행을 이동(**전치, p-box**)
- **확산 계층(diffusion layer)을 의미한다.**
- **확산**은 **암호문**과 **평문** 사이의 관계를 알기 어렵게 한다.

- **열혼합(mix column) : 뒤섞음**은 **행열곱** 연산에 의해 수행된다.
- **행열곱셈**을 이용하여 바이트들을 뒤섞는다.
- **뒤섞음**은 4개의 바이트를 가지고 수행한다.

- **키덧셈** : 라운드 키와 스테이트 각 열을 **xor** 연산한다.
- **라운드 키**를 생성하기 위해 AES는 **키확장** 과정을 적용

- **4단계** 모두 역 계산이 가능하므로 **복호** 과정에서는 **역변환**이 사용된다.

◈ **행 이동(shift row)**

11	12	13	14
21	22	23	24
31	32	33	34
41	42	43	44

[이동 전 상태]

11	12	13	14	→ 행 이동 없음
22	23	24	21	→ 1byte 좌측 이동
33	34	31	32	→ 2byte 좌측 이동
44	41	42	43	→ 3byte 좌측 이동

[이동 후 상태]

◈ **열 혼합(mix column)**

• 열 혼합 변환 단계에서는 다음처럼 **행렬 곱셈** 연산에 의해 수행된다.

• 128비트 블록을 4×4인 정방행렬로 나열해서 처리한다.

$$\begin{pmatrix} a1 & a2 & a3 & a4 \\ b1 & b2 & b3 & b4 \\ c1 & c2 & c3 & c4 \\ d1 & d2 & d3 & d4 \end{pmatrix} \times \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} a1\cdot 1 + a2\cdot 2 + a3\cdot 3 + a4\cdot 4 \\ b1\cdot 1 + b2\cdot 2 + b3\cdot 3 + b4\cdot 4 \\ c1\cdot 1 + c2\cdot 2 + c3\cdot 3 + c4\cdot 4 \\ d1\cdot 1 + d2\cdot 2 + d3\cdot 3 + d4\cdot 4 \end{pmatrix}$$

↓ ㄴ, 하나의 열 혼합 변환 결과를 나타냄

128bit 블록(변환 전)

◈ **라운드 키 더하기(add round key)**

• 확장된 키 일부와 현재 블록을 비트별로 **XOR** 연산한다.

```
    0101 ← 확장된 키 일부
xor)1001 ← 현재 블록
    1100
```

기출문제 분석

1. AES 알고리즘의 블록 크기와 키 길이에 대한 설명으로 옳은 것은? [2017년 국가 9급]

① 블록 크기는 64비트이고 키 길이는 56비트이다.
② 블록 크기는 128비트이고 키 길이는 56비트이다.
③ 블록 크기는 64비트이고 키 길이는 128/192/256비트이다.
④ 블록 크기는 128비트이고 키 길이는 128/192/256비트이다.

♤ AES 알고리즘

AES 종류	키 길이	라운드	블록 크기	라운드 키	라운드 키 수
AES-128	128bit	10	128bit	128bit	11
AES-192	192bit	12	128bit	128bit	13
AES-256	256bit	14	128bit	128bit	15

정답 : ④

2. AES(Advanced Encryption Standard) 알고리즘을 구성하는 변환 과정 중, 상태 배열의 열 단위의 행렬 곱셈과 같은 형태로 표현되는 것은? [2016년 국가 7급]

① 바이트 치환(substitute bytes)
② 행 이동(shift row)
③ 열 혼합(mix columns)
④ 라운드 키 더하기(add round key)

♤ AES(Advanced Encryption Standard) 암호 알고리즘 – 열 혼합(mix column)

• 열 혼합 변환 단계에서는 다음처럼 행렬 곱셈 연산에 의해 수행된다.

$$\begin{pmatrix} a1 & a2 & a3 & a4 \\ b1 & b2 & b3 & b4 \\ c1 & c2 & c3 & c4 \\ d1 & d2 & d3 & d4 \end{pmatrix} \times \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} a1\cdot 1 + a2\cdot 2 + a3\cdot 3 + a4\cdot 4 \\ b1\cdot 1 + b2\cdot 2 + b3\cdot 3 + b4\cdot 4 \\ c1\cdot 1 + c2\cdot 2 + c3\cdot 3 + c4\cdot 4 \\ d1\cdot 1 + d2\cdot 2 + d3\cdot 3 + d4\cdot 4 \end{pmatrix}$$

↓ 128비트 블록(변환 전)

↳ 하나의 열 혼합 변환 결과를 나타냄

정답 : ③

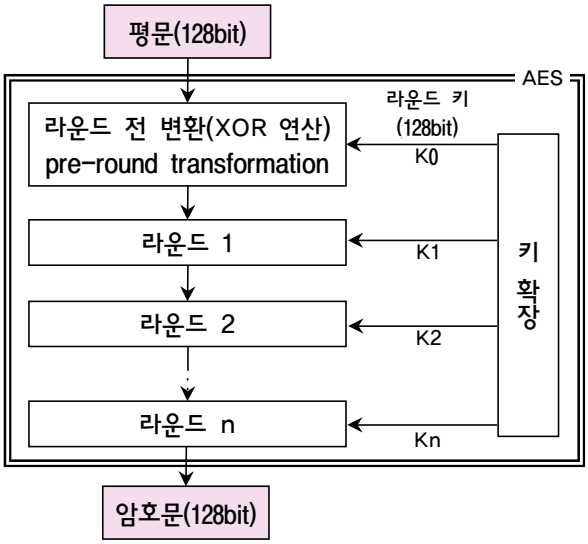
3. AES 알고리즘에 대한 설명으로 옳지 않은 것은? [2022년 지방 9급]

① 블록 암호 체제를 갖추고 있다.
② 128/192/256bit 키 길이를 제공하고 있다.
③ DES 알고리즘을 보완하기 위해 고안된 알고리즘이다.
④ 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드 키의 NOR 연산을 수행한다.

♤ AES 알고리즘

- 첫 번째 라운드를 **수행하기 전**에 먼저 초기 평문과 라운드 키의 NOR 연산을 수행한다.(×)
  → 첫 번째 라운드를 **수행하기 전**에 먼저 초기 평문과 라운드 키의 XOR 연산을 수행한다.

// AES 암호 구조도



종류	암호키	라운드	라운드 키 수
AES-128	128bit	10	11
AES-192	192bit	12	13
AES-256	256bit	14	15

- AES는 각 라운드에서 사용할 **라운드 키**를 생성하기 위해 **키 확장** 과정을 거친다.
- **라운드 키**는 **암호키(128bit)**를 이용하여, **키 확장** 과정을 통해 생성된다.
- **라운드 수**가 n이면, n+1개의 **라운드 키**를 생성한다.
- **처음** 생성한 **라운드 키(k0)**는 첫 번째 라운드를 **수행하기 전**에 **평문**과 XOR 연산한다.
- 나머지 **라운드 키**는 각 라운드의 마지막 단계에서 XOR 연산한다.

① **바이트 치환(substitute byte)**	S-box 표를 이용하여 바이트 단위로 블록 교환(**대치**)
② **행 이동(shift row)**	P-box, 단순히 행과 행을 이동(**전치**)
③ **열 혼합(mix column)**	행렬 곱셈 연산(행렬을 사용하여 열의 각 바이트를 **대치**)
④ **라운드 키 더하기(add round key)**	확장된 키의 일부와 현재 블록을 XOR 연산(**대치**)

- **각 라운드**는 **마지막**을 **제외**하고, 위의 **표**에 있는 **4개의 변환**을 사용한다.
- 암호의 **마지막 라운드**는 MixColumns을 제외한 **3의 변환**을 사용한다.

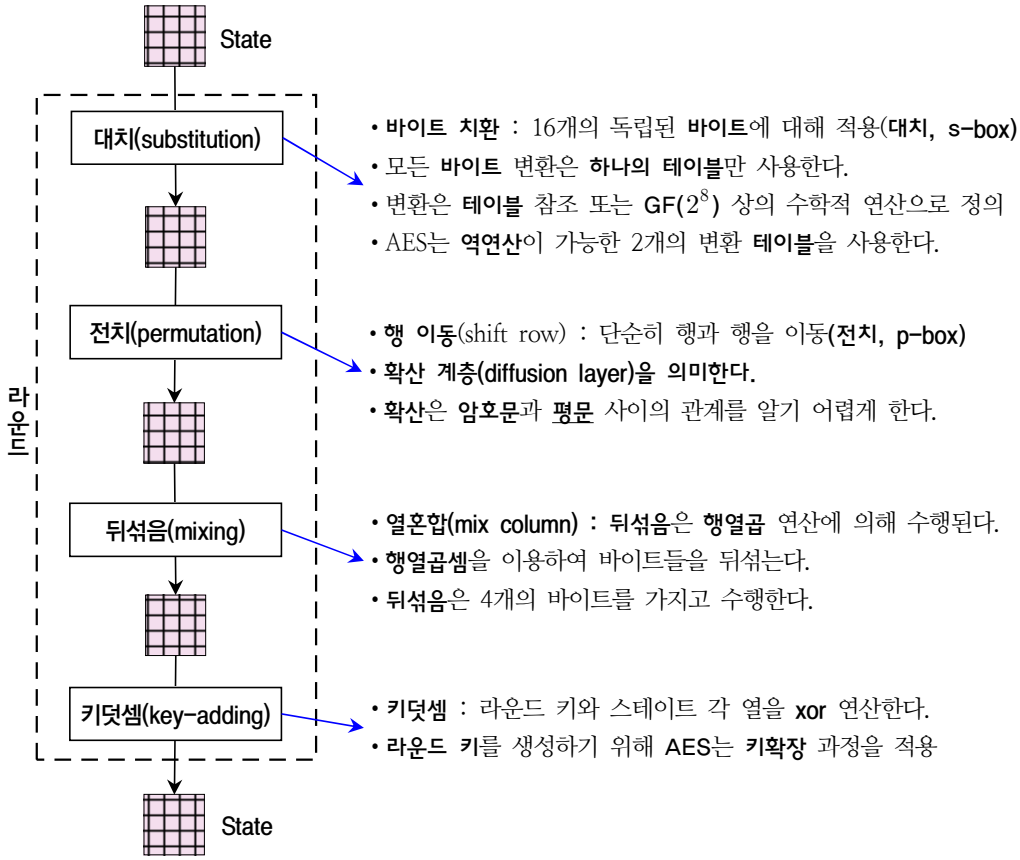
정답 : ④

4. AES 알고리즘에 대한 설명으로 옳지 않은 것은? [2022년 국가 9급]

① 대먼과 리즈먼이 제출한 Rijndael이 AES 알고리즘으로 선정되었다.
② 암호화 과정의 모든 라운드에서 SubBytes, ShiftRows, MixColumns, AddRoundKey 연산을 수행한다.
③ 키의 길이는 128, 192, 256bit의 크기를 사용한다.
④ 입력 블록은 128bit이다.

♤ AES 알고리즘

• 암호 과정의 **모든 라운드**에서 SubBytes, ShiftRows, MixColumns, AddRoundKey 연산을 수행한다.**(×)**
→ **각 라운드**는 **마지막**을 **제외**하고 **4개의 변환**을 사용한다.
→ 암호의 **마지막 라운드**는 MixColumns을 제외한 **3의 변환**을 사용한다.



• **4단계** 모두 역 계산이 가능하므로 **복호** 과정에서는 **역변환**이 사용된다.

정답 : ②

5. 암호화 기법들에 대한 설명으로 옳지 않은 것은? [2019년 지방 9급]

① Feistel 암호는 전치(permutation)와 대치(substitution)를 반복시켜 암호문에 평문의 통계적인 성질이나 암호키와의 관계가 나타나지 않도록 한다.
② Kerckhoff의 원리는 암호 해독자가 현재 사용되고 있는 암호 방식을 알고 있다고 전제한다.
③ AES는 암호키의 길이를 64비트, 128비트, 256비트 중에서 선택한다.
④ 2중 DES(Double DES) 암호 방식은 외형상으로는 DES에 비해 2배의 키 길이를 갖지만, 중간일치공격 시 키의 길이가 1비트 더 늘어난 효과밖에 얻지 못한다.

♤ AES 기본 사양

AES 종류	암호키	라운드	평문/암호문	라운드 키	라운드 키 수
AES-128	128bit	10	128bit	128bit	11
AES-192	192bit	12	128bit	128bit	13
AES-256	256bit	14	128bit	128bit	15

• AES는 암호키 길이를 128비트, 192비트, 256비트 중에서 선택한다.

정답 : ③

6. AES(Advanced Encryption Standard)에 대한 설명으로 옳은 것은? [2020년 지방 9급]

① DES(Data Encryption Standard)를 대신하여 새로운 표준이 된 대칭 암호 알고리즘이다.
② Feistel 구조로 구성된다.
③ 주로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 고안되었다.
④ 2001년에 국제표준화기구인 IEE가 공표하였다.

♤ AES(Advanced Encryption Standard)

② Feistel 구조로 구성된다.(×)
→ AES 알고리즘은 SPN(Substitution Permutation Network) 구조이다.
③ 주로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 고안되었다.(×)
→ AES 알고리즘은 유연성(flexibility)과 단순성(simplicity) 구조이다.
④ 2001년에 국제표준화기구인 IEE가 공표하였다.(×)
→ 미국표준기술연구소(NIST)가 공표하였다.(1997년 9월)

정답 : ①

7. 미국 NIST가 표준으로 제정한 AES(Advanced EncryptionStandard) 암호의 특징으로 가장 옳지 않은 것은? [2022년 군무원 9급]

① 평문과 암호문의 크기가 128비트인 블록암호이다.
② 키는 128비트, 192비트, 256비트 중 선택하여 사용한다.
③ Substitution-and-Permutation Network 형태의 암호체계이다.
④ Weak Key가 존재한다.

♤ **AES 암호**

· Weak Key가 존재한다.(×) → **AES**에는 Weak Key가 없다.(**AES**는 **취약키 공격**에 **안전**)

취약키 (weak key)	· 취약키는 암호에서 특정한 조작을 통해 쉽게 **복호화**가 가능한 키를 의미한다. · DES, RC4, IDEA, 블로피시 등의 암호에는 취약키가 존재한다.

// DES에서 취약키

취약키 (weak key)	· DES는 **4**개의 취약키를 갖고 있다. · **같은키**를 암호문을 다시 암호화하면 복호화 연산한 **결과(평문)**가 된다. · 여기서, **같은키**가 **취약키**가 된다. · **평문** = $E_{\text{취약키}}(E_{\text{취약키}}(\textbf{평문}))$ ← **E는 암호 알고리즘** ↓**4**개의 **취약키** · **0101 0101 0101 0101**이 입력되면 0000 0000 0000 0000이 출력된다. · **1F1E 1F1E 1F1E 1F1E**이 입력되면 0000 0000 FFFF FFFF가 출력된다. · **E0E0 E0E0 F1F1 F1F1**이 입력되면 FFFF FFFF 0000 0000이 출력된다. · **FEFE FEFE FEFE FEFE**이 입력되면 FFFF FFFF FFFF FFFF가 출력된다.
준취약키 (semi-weak key)	· DES는 **6**개의 **쌍**의 **준취약키**를 갖고 있다. · **키쌍** 중 하나의 키로 암호화하고, 다른 키로 또 암호화하면 **평문**이 된다. · **평문** = $E_{\text{준취약키1}}(E_{\text{준취약키2}}(\textbf{평문}))$ ← **E는 암호 알고리즘** ↓**6**개의 **준취약키 쌍 (취약키1, 취약키2)** (011F011F010E010E, 1F011F010E010E01) (01E001E001F101F1, E001E001F101F101) (01FE01FE01FE01FE, FE01FE01FE01FE01) (1FE01FE00EF10EF1, E01FE01FF10EF10E) (1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E) (E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1)

출처 : NIST Special Publication 800-67, McGrawHill Cryptography and Network Security

정답 : ④