13. 암호 해독(cryptanalysis)

암호 해독은 비밀키를 모르는 상태에서 암호문을 복호화 시키는 것이다.
암호 해독의 목적은 사용되는 **비밀키**나 **평문**을 찾는 것이다.

1. 커크호프 원리(Kerckhoff's principle)

① **커크호프**는 암호시스템에 대해 다음처럼 **주장**하였다.(1883년)

"암호시스템에서 키를 제외한 나머지는 모든 것이 공개되어도 안전해야 한다"

- 이를 **Kerckhoff's principle**이라 한다.

② 암호 안전성은 "암호 알고리즘의 비밀을 유지하는데 의존되어서는 안 되고, 비밀키의 비밀을 지키는데 의존되어야 한다"는 원리이다.
- 커크호프 원리는 "**암복호 알고리즘**은 **공개**하지만
- **비밀키**는 절대로 **누출**해서는 안 된다"는 원리이다

③ 현대 암호에서 **암호시스템의 안전성**은 Kerckhoff's principle에 기반한다.
- 현대 암호에서는 암호 알고리즘을 공개하도록 권장하고 있다.
- 암호 알고리즘을 감춘다고 해서 무조건 암호의 보안성이 높아지는 것도 아니다.
- **암호 알고리즘을 공개**하면 많은 암호 학자들에 의해 **안전성을 검증**받을 수 있다.

2. 선형공격(linear cryptanalysis) / 차분공격(differential cryptanalysis)

선형공격과 차분공격은 블록 암호의 안전성 분석 또는 공격하는 도구이다.

◈ **선형공격**

- 선형공격은 알고리즘 내부의 **비선형 구조**를 적당히 **선형화시켜 비밀키를 찾는 공격**이다.
- 선형공격은 암호화에서 사용된 근사적인 선형 관계를 찾아 평문을 공격하는 것이다.
- 선형공격은 S-box의 연산을 선형 과정으로 근사화할 방법을 찾는 것이 목표이다.
  → S-box의 대치 과정에서는 비선형적인 변환이 일어난다.
  → S-box는 완전한 선형함수는 아니다.
- 근사적인 선형 관계를 발견하면, 이를 이용하여 평문을 공격할 수 있다.

◈ **차분공격**

- 차분공격은 **두 평문**의 XOR 값과 대응되는 **두 암호문**의 XOR 값을 비교 분석하는 공격이다.
- 예 : P1 ⊕ P2 = C1 ⊕ C2
- 평문 차분은 △P=P1⊕P2로 정의하고, 암호문 차분은 △C=C1⊕C2로 정의한다.
- 평문 차분과 암호문 차분 사이의 관계를 파악하여, 공격할 수 있다.
- 현재, 차분공격은 **블록 암호**에 대한 가장 **강력한 공격**법 중 하나이다.

[예제] C1 ⊕ C2 = P1 ⊕ P2를 증명하시오.

(단, 암호 알고리즘은 단순하게 XOR 연산으로만 구성된다고 가정한다)

증명	C1 = P1 ⊕ K C2 = P2 ⊕ K	이다. (k는 암호화에 사용된 **비밀키**이다)

↓증명

C1 ⊕ C2 = P1 ⊕ K ⊕ P2 ⊕ K
= P1 ⊕ P2 ⊕ K ⊕ K → K ⊕ K는 XOR 연산하면 0은 된다.
= P1 ⊕ P2 ⊕ 0 → 임의의 비트열을 0(영)과 XOR 연산하면 0은 없어진다.
= P1 ⊕ P2

자신과 XOR 연산	0과 XOR 연산
0 1 0 1 XOR) 0 1 0 1 0 0 0 0 → 연산 결과는 0이 된다.	1 0 0 1 XOR) 0 0 0 0 1 0 0 1 → 연산 결과 비트열은 그대로이다.

선형(linear)과 비선형(nonlinear)의 차이점

대칭키 암호에서 적용되는 선형변환과 비선형변환은 무엇을 의미하는가?
→ 예 : Feistel 구조에서 분리된 반은 선형, 다른 반쪽은 비선형변환이 적용된다.
→ Feistel 구조는 대칭키 암호에서 구체적으로 다룬다.

먼저, 선형과 비선형의 차이점이 무엇인지 개념을 정확하게 이해하는 것이 중요하다.

1. 선형

- 일차함수의 그래프는 직선 형태이다. 즉, 일차함수는 선형이다.
- 선형은 **단순**하다.
- 선형은 하나의 원인에 하나의 결과가 도출되는 구조이다.
- 따라서, 결과를 보고, 원인이 무엇인지 짐작할 수 있다.

2. 비선형

- 비선형은 우리가 **예상할 수 없는 보다 높은 차원의 현상**을 일으킨다.
- 비선형은 하나의 원인에 다수의 결과가 있는 구조이다.
- 재귀호출에 사용되는 수식은 비선형이다.
- 하나의 수식으로부터 나오는 결과가 항상 다르므로 예측이 어렵다.
- 의미적으로, 비선형, 카오스(chaos), 복잡성 등의 용어는 유사한 뜻을 가진다.
- 카오스(chaos)는 혼돈, 무질서, 무한이라는 뜻을 가진다.
- 자연계는 대부분이 비선형 구조이다.
- 자연계 : 사람의 폐, 혈관, 해안선, 눈송이, 구름, 산, 꽃, 나무 등
- 자연계에서 선형적인 현상은 극히 특수한 경우이다.
- 비선형계는 몇 개의 간단한 구성요소로는 **분석이 불가능**하다.
- 만약, 비선형은 분석되어도 전체 행동을 예측하기 어렵다.
- 이유 : 각 요소들이 종합될 때, 서로 영향을 끼치므로 전체 행동을 예측하기 어렵다.

비선형	• 밥 먹는 양에 비례해서 키가 크거나 힘이 세지지 않는다. • 식물은 물을 준만큼 자라지 않는다.

3. 암호 해독 종류

다음은 암호 해독 공격 대상의 형태이다. 공격 강도가 큰 순서부터 나열하였다.

암호 해독 공격 구분	설 명
암호문 단독 공격 (ciphertext-only attack)	• 공격자는 단지 **임의의 암호문만**을 필요로 한다.**(암호문)** • 공격자가 가장 쉽게 적용할 수 있는 공격이다. • 공격자가 암호 알고리즘을 알고 있는 것으로 가정한다. • 공격자는 단지 암호문을 획득하여 대응되는 **키** 또는 **평문**을 찾아 내는 것이 목적이다.
알려진(기지) 평문 공격 (known-plaintext attack) // 선형공격	• 공격자에게 **약간의 (평문, 암호문) 쌍**을 미리 주어진다. → 공개된 (평문, 암호문) 쌍을 이용하여 다음 암호문을 해독 → 송수신자가 메시지를 주고받은 후에 이를 공개하는 경우 • 평문에 대응하는 암호문을 알고 있는 상태에서 암호문과 평문의 관계로부터 **키**를 추정하는 해독하는 방법이다. • 공격자는 많은 정보를 이용함으로 암호문 해독이 쉽다. • 암호문 단독 공격보다 적용할 상황이 드물다.
선택 평문 공격 (chosen-plaintext attack) // 차분공격	• 핵심은 공격자가 직접 **평문을 선택**한다.**(선택한 평문, 암호문)** • 공격자가 선택한 **평문**에 대응하는 **암호문**을 공격자에게 제공한다. • 단지, 공격자는 **비밀키**를 알 수 없다. • 공격자가 **송신자 컴퓨터(암호기)**에 접근할 수 있어야 가능하다. • 암호문 해독이 쉽지만 적용 가능한 상황은 매우 드물다. • 이 유형의 공격에 안전한 암호시스템은 이상적일 수 있다.
선택 암호문 공격 (chosen-ciphertext attack)	• 핵심은 공격자가 직접 **암호문을 선택**한다.**(평문, 선택한 암호문)** • 공격자가 선택한 **암호문**에 대응하는 **평문**을 공격자에게 제공한다. • 그리고, 공격자는 암호문에 대응하는 평문에 사용된 **키**를 찾는다. • 공격자가 **수신자 컴퓨터(복호기)**에 접근할 수 있어야 가능하다.

• 암호 해독은 암호시스템의 안전성을 평가하기 위해서 필요한 **과학**이다.

• 암호 해독은 **타인의 비밀을 해독**하기 위한 것은 아니다.

4. 암호 해독 공격

◈ **전수조사 공격(brute-force attack, 무차별 공격)**

① 암호문이 이해할 수 있는 평문으로 전환될 때까지 **가능한 모든 키를 대입**한다.

• 조합 가능한 모든 경우의 수를 처음부터 끝까지 대입하는 방식이다.

② 전수조사 공격은 단순하지만 컴퓨터 성능이 향상되면서 무시할 수 없는 기법이다.

• 암호 알고리즘인 DES가 DES cracker라는 특수 기계에 의해 해독되었다.

• 크랙(crack)은 타인의 시스템, 통신망 등에 불법적으로 침입하는 행위이다.

• 정품 프로그램의 암호설정이나 복사방지 장치를 무력화하는 불법적인 프로그램이다.

• 특정 보호 장치를 해제하거나 우회하는 일련의 소프트웨어 기술이다.

③ 전수조사 공격에 안전하기 위해서는 조합 가능한 키의 수가 매우 커야 한다.

◈ **사전 공격(dictionary attack)**

① 통상적으로 자주 사용하는 비밀번호를 **사전식으로 모아서 대입**하는 방식이다.

• 1111, 1234, 4321, 9999, east, love 등으로 구성된 비밀번호 목록을 이용한다.

② 비밀번호 구성은 "문자, 숫자, 특수기호"를 조합하여야 높은 강도를 가지게 된다.

• "p#5w8*$s97"은 강도가 높은 비밀번호이다.

◈ **패턴 공격(pattern attack)**

① 암호문에는 어떤 패턴이 존재할 수 있다. **패턴**을 이용한 암호 해독이다.

• tet는 get, set, bet, … 일 가능성이 있다.

• thkee는 three일 가능성이 있다.

② 공격 방어 : 암호문 구조가 랜덤(random)하도록 암호화되어야 한다.

◈ **통계적 공격(statistical attack)**

① 공격자는 평문에 사용된 언어의 고유한 특징으로부터 정보를 얻어서 해독한다.

• 영어에서 가장 많이 등장하는 문자는 "e"이다.**(빈도수)**

• 영어에서 가장 흔히 등장하는 단어는 "the"이다.

② 공격 방어 : 암호문은 평문 언어가 가지는 특징이 나타나지 않도록 해야 한다.

◈ **수학적 분석(mathematical analysis)**

① 수학적 분석은 **수학적 이론**을 이용하여 암호문을 해독하는 방법이다.

• 수학적 이론은 대수 방정식, 역수 함수, 기약 다항식 등이다.

② 참고로, **수학과 통계학의 차이**는 뭘까?

• 그냥, 단순하게 생각하면 통계학은 수학에 포함되는 것으로 생각할 수 있다.

• 그런데, 세부적으로 보면 수학과 통계학은 서로 다른 학문으로 본다.

• 해서, 암호 해독 방법에 수학적 분석을 별도로 분류하기도 한다.

기출문제 분석

1. 정보보안의 기본 개념에 대한 설명으로 옳지 않은 것은? [2015년 국가 9급]

① Kerckhoff의 원리에 따라 암호 알고리즘은 비공개로 할 필요가 없다.
② 보안의 세 가지 주요 목표에는 기밀성, 무결성, 가용성이 있다.
③ 대칭키 암호 알고리즘은 송수신자 간의 비밀키를 공유하지 않아도 된다.
④ 가용성은 인가된 사용자에게 서비스가 잘 제공되도록 보장하는 것이다.

♤ **대칭키 암호 알고리즘**

• 대칭키 암호 알고리즘은 송수신자 간의 비밀키를 공유하지 않아도 된다.**(×)**
→ 대칭키 암호 알고리즘은 송수신자 간의 비밀키를 공유해야 한다.

정답 : ③

2. 다음의 정보보호와 관련된 원칙을 제시한 사람은? [2022년 국가 7급]

이 원칙은 공격자가 암호 알고리즘을 완전히 알고 있더라도 키가 없이는 복호화해 평문을 얻을 수 없어야 함을 의미하는 것으로, 암호 알고리즘의 안전성이 암호 알고리즘 설계 자체의 비밀성에 의존해서는 안 되고 키의 비밀성에 의존해야 함을 강조한다. 따라서 암호 알고리즘은 널리 공개해서 많은 암호학자의 검증을 거치는 과정을 통해 안전성을 인정받아야 한다.

---

① Rabin ② Hellman
③ Kerckhoffs ④ Koblitz

♤ **커크호프 원리(Kerckhoff's principle)**

• **"암호시스템에서 키를 제외한 나머지는 모든 것이 공개되어도 안전해야 한다"**
• 현대 암호에서 **암호시스템의 안전성**은 Kerckhoff's principle에 기반한다.

정답 : ③

3. 대칭키 암호시스템에 대한 암호 분석 방법과 암호 분석가에게 필수적으로 제공되는 모든 정보를 연결한 것으로 옳지 않은 것은? [2021년 국가 9급]

① 암호문 단독(ciphertext only) 공격 – 암호 알고리즘, 해독할 암호문
② 기지 평문(known plaintext) 공격 – 암호 알고리즘, 해독할 암호문, 임의의 평문
③ 선택 평문(chosen plaintext) 공격 – 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문
④ 선택 암호문(chosen ciphertext) 공격 – 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 암호문과 해독할 암호문에 사용된 키로 복호화한 해당 평문

♤ **암호 해독**

암호 해독 공격 구분	암호 분석가에게 필수적으로 제공되는 모든 정보
암호문 단독 공격 **(ciphertext-only attack)**	• 암호 알고리즘 • 해독할 **암호문** ↓**핵심 내용** • 암호문에 대응하는 **평문** 또는 **비밀키**를 찾는 공격
알려진(기지) 평문 공격 **(known-plaintext attack)**	• 암호 알고리즘 • 해독할 **암호문**과 이에 대응하는 **평문 – (평문, 암호문) 쌍** ↓**핵심 내용** • 알고 있는 평문과 암호문을 바탕으로 **비밀키**를 찾는 공격
선택 평문 공격 **(chosen-plaintext attack)**	• 암호 알고리즘 • 해독할 암호문 • 암호 분석가에 의해 **선택된 평문**과 해독할 암호문에 사용된 키로 생성한 **해당 암호문 – (선택된 평문, 암호문) 쌍** ↓**핵심 내용** • 공격자가 직접 **평문을 선택**한다.
선택 암호문 공격 **(chosen-ciphertext attack)**	• 암호 알고리즘 • 해독할 암호문 • 암호 분석가에 의해 **선택된 암호문**과 해독할 암호문에 사용된 키로 복호화한 **해당 평문 – (평문, 선택된 암호문) 쌍** ↓**핵심 내용** • 공격자가 직접 임의의 **암호문을 선택**한다.

• 기지 평문 공격 – 암호 알고리즘, 해독할 암호문, 임의의 평문(×)
→ 기지 평문 공격 – 해독할 **암호문**과 이에 대응하는 **평문 – (평문, 암호문) 쌍**

정답 : ②

4. 공격자가 일정 부분의 평문과 이에 대응하는 암호문을 모두 알고 있을 때 비밀키를 알아내기 위한 공격은? [2022년 국회 9급]

① 기지 평문 공격
② 선택 암호문 공격
③ 선택 평문 공격
④ 암호문 단독 공격
⑤ 전수조사 공격

♤ **암호 해독**

암호 해독 공격 구분	암호 분석가에게 필수적으로 제공되는 모든 정보
암호문 단독 공격 (ciphertext-only attack)	• 암호 알고리즘 • 해독할 **암호문** ↓**핵심 내용** • 암호문에 대응하는 **평문** 또는 **비밀키**를 찾는 공격
알려진(기지) 평문 공격 (known-plaintext attack)	• 암호 알고리즘 • 해독할 **암호문**과 이에 대응하는 **평문 – (평문, 암호문) 쌍** ↓**핵심 내용** • 알고 있는 평문과 암호문을 바탕으로 **비밀키**를 찾는 공격
선택 평문 공격 (chosen-plaintext attack)	• 암호 알고리즘 • 해독할 암호문 • 암호 분석가에 의해 **선택된 평문**과 해독할 암호문에 사용된 키로 생성한 **해당 암호문 – (선택된 평문, 암호문) 쌍** ↓**핵심 내용** • 공격자가 직접 **평문을 선택**한다.
선택 암호문 공격 (chosen-ciphertext attack)	• 암호 알고리즘 • 해독할 암호문 • 암호 분석가에 의해 **선택된 암호문**과 해독할 암호문에 사용된 키로 복호화한 **해당 평문 – (평문, 선택된 암호문) 쌍** ↓**핵심 내용** • 공격자가 직접 임의의 **암호문을 선택**한다.

• 암호 해독은 암호시스템의 안전성을 평가하기 위해서 필요한 **과학**이다.
• 암호 해독은 **타인의 비밀을 해독**하기 위한 것은 아니다.

정답 : ①

5. <보기 1>의 ㄱ~ㄹ의 암호 공격 방식과 <보기 2>의 ⓐ~ⓓ에 대한 설명으로 옳지 않은 것은? [2015년 국가 7급]

-----<보기 1>----------
ㄱ. 암호문 단독 공격(ciphertext only attack)
ㄴ. 기지 평문 공격(known plaintext attack)
ㄷ. 선택 평문 공격(chosen plaintext attack)
ㄹ. 선택 암호문 공격(chosen ciphertext attack)
-----<보기 2>----------
ⓐ 암호문만을 가지고 평문이나 키를 찾아내는 방법으로 평문의 특성 등을 추정하여 해독하는 방법
ⓑ 약간의 평문에 대응하는 암호문을 알고 있는 상태에서 암호문과 평문의 관계로부터 키나 평문을 추정하여 암호를 해독하는 방법
ⓒ 해독자가 암호기에 접근할 수 있어, 평문을 선택하여 그 평문에 해당하는 암호문을 얻어 키나 평문을 추정하여 암호를 해독하는 방법
ⓓ 해독자가 암호 복호기에 접근할 수 있어, 일부 평문에 대한 암호문을 얻어 암호를 해독하는 방법
---

① ㄱ－ⓐ　② ㄴ－ⓑ　③ ㄷ－ⓒ　④ ㄹ－ⓓ

♤ **암호 공격 방식**

선택 암호문 공격 (chosen-ciphertext attack)	• 핵심은 공격자가 직접 임의의 **암호문을 선택**한다. • 공격자가 선택한 **암호문**에 대응하는 **평문**을 공격자에게 제공한다. • 그리고, 공격자는 암호문에 대응하는 평문에 사용된 **키**를 찾는다. • 공격자가 **수신자 컴퓨터(복호기)**에 접근할 수 있어야 가능하다.

정답 : ④

6. 패스워드(password)에 사용될 수 있는 문자열의 범위를 정하고, 그 범위 내에서 생성 가능한 패스워드를 활용하는 공격은? [2014년 국가 7급]

① 레인보 테이블(rainbow table)을 이용한 공격
② 사전 공격(dictionary attack)
③ 무작위 대입 공격(brute-force attack)
④ 차분공격(differential attack)

♤ **무작위 대입 공격(brute-force attack) – 전수조사 공격**

• 암호문이 이해할 수 있는 평문으로 전환될 때까지 가능한 모든 키를 대입한다.
→ 조합 가능한 모든 경우의 수를 처음부터 끝까지 대입하는 방식이다.

정답 : ③

7. 블록암호는 평문을 일정한 단위(블록)로 나누어서 각 단위마다 암호화 과정을 수행하여 암호문을 얻는 방법이다. 블록암호 공격에 대한 설명으로 옳지 않은 것은? [2015년 서울 9급]

① 선형공격 : 알고리즘 내부의 비선형 구조를 적당히 선형화시켜 키를 찾아내는 방법이다.
② 전수공격 : 암호화할 때 일어날 수 있는 모든 가능한 경우에 대해 조사하는 방법으로 경우의 수가 적을 때는 가장 정확한 방법이지만 일반적으로 경우의 수가 많은 경우에는 실현 불가능한 방법이다.
③ 차분공격 : 두 개의 평문 블록들의 비트 차이에 대응되는 암호문 블록들의 비트 차이를 이용하여 사용된 키를 찾아내는 방법이다.
④ 수학적 분석 : 암호문에 대한 평문이 각 단어의 빈도에 관한 자료를 포함하는 지금까지 모든 통계적인 자료를 이용하여 해독하는 방법이다.

♤ **블록암호 공격**

• 수학적 분석 : 암호문에 대한 평문이 각 단어의 빈도에 관한 자료를 포함하는 지금까지 모든 통계적인 자료를 이용하여 해독하는 방법이다.**(×)**
→ **통계적** 분석

정답 : ④

8. 다음에서 설명하는 패스워드 크래킹(cracking) 공격 방법은? [2017년 지방 9급]

○ 사용자가 설정하는 대부분의 패스워드에 특정 패턴이 있음을 착안한 방법으로 패스워드로 사용할 만한 것을 사전으로 만들어놓고 이를 하나씩 대입하여 일치 여부를 확인하는 방법이다.
○ 패스워드에 부가적인 정보(salt)를 덧붙인 후 암호화하여 저장함으로써 이 공격에 대한 내성을 향상시킬 수 있다.

---

① Brute Force 공격
② Rainbow Table을 이용한 공격
③ Flooding 공격
④ Dictionary 공격

♤ **사전 공격**

• 통상적으로 자주 사용하는 비밀번호를 사전식으로 모아서 직접 대입하는 방식이다.

정답 : ④

9. 정보보안 관련 용어에 대한 설명으로 옳지 않은 것은? [2019년 국가 9급]

① 부인방지(non-repudiation) - 사용자가 행한 행위 또는 작업을 부인하지 못하는 것이다.
② 최소권한(least privilege) - 계정이 수행해야 하는 작업에 필요한 최소한의 권한만 부여한다.
③ 키 위탁(key escrow) - 암호화 키가 분실된 경우를 대비하여 키를 보관하는 형태를 의미한다.
④ 차분공격(differential attack) - 대용량 해시테이블을 이용하여 충분히 작은 크기로 줄여 크랙킹 하는 방법이다.

♤ **정보보안 관련 용어**

• 차분공격(differential attack) - 대용량 해시테이블을 이용하여 충분히 작은 크기로 줄여 크랙킹 하는 방법이다. → **레인보우 테이블**을 이용 비밀번호 크래킹

◈ **레인보우 테이블을 이용한 공격**

· 레인보우 테이블은 **해시함수**를 사용하여 생성된 값들을 대량으로 저장한 표이다.
  → 해시함수 MD5, SHA-1, SHA-2 등을 이용
  → 레인보우 테이블 크기는 작은 것도 기본적으로 100GB이상이 된다.(보통 TB 단위)
· 레인보우 테이블을 이용한 공격도 일종의 **사전공격**이다.
  → 미리 만들어진 테이블에서 해시값을 뽑아서 대입하므로
  → Rainbow Table을 이용하면 해시값 계산 시간이 절약되어 신속한 공격 가능
  → Rainbow Table을 이용하면 12자리 숫자로 된 비밀번호를 순식간에 뚫을 수 있다.
· 레인보우 테이블은 R(reduction) 함수를 이용하여 충분히 작은 크기로 줄일 수 있다.
· 레인보우 테이블은 크기를 줄여도 기본적으로 수십GB이상이 된다.
· R 함수는 비밀번호로 사용되는 문자열을 해시값으로 만드는 함수이다.

◈ **차분공격**

• 차분공격은 두 평문의 XOR 값과 대응되는 두 암호문의 XOR 값을 비교 분석하여 공격하는 방법이다. → 현재, 블록 암호에 대한 가장 강력한 공격법 중 하나이다.
• 평문 차분은 △P=P1⊕P2로 정의하고, 암호문 차분은 △C=C1⊕C2로 정의한다.
• 평문 차분과 암호문 차분 사이의 관계를 파악하여, 공격할 수 있다.

정답 : ④

10. 패스워드 공격에 해당하지 않는 것은? [2020년 국가 7급]

① 사전 대입 공격
② 이블 트윈 공격
③ 무작위 대입 공격
④ 레인보우 테이블을 이용한 공격

♤ **패스워드 공격에 해당하지 않는 것**

◈ **Evil Twin(이블 트윈) - 악의적 쌍둥이**

- 이블 트윈은 합법적인 네트워크처럼 가장한 무선 네트워크를 가리킨다.
- 이블 트윈은 로그온한 사람들을 **속이고,** 비밀번호나 신용카드번호를 훔치기 위한 공격이다.
- 이블 트윈은 **피싱 사기의 무선 버전**이다.
- 공격자는 합법적인 제공자로 가장하여, 노트북이나 휴대폰으로 AP에 연결한 사용자들을 공격한다.

◈ **전수조사 공격(brute-force attack, 무차별 공격)**

- 암호문이 이해할 수 있는 평문으로 전환될 때까지 가능한 모든 **비밀번호**를 대입한다.
- 조합 가능한 모든 경우의 수를 처음부터 끝까지 대입하는 방식이다.
- 전수조사 공격은 단순하지만 컴퓨터 성능이 향상되면서 무시할 수 없는 기법이다.
- 전수조사 공격에 안전하기 위해서는 조합 가능한 키의 수가 매우 커야 한다.

◈ **사전 공격(dictionary attack)**

- 통상적으로 자주 사용하는 **비밀번호**를 사전식으로 모아서 직접 대입하는 방식이다.
- 1111, 1234, 4321, 9999, east, love 등으로 구성된 비밀번호 목록을 이용한다.
- 비밀번호 구성은 "문자, 숫자, 특수기호"를 조합하여야 높은 강도를 가지게 된다.
- "p#5w8*$s97"은 강도가 높은 비밀번호이다.

◈ **레인보우 테이블을 이용한 공격**

- 레인보우 테이블은 **해시함수**를 사용하여 생성된 값들을 대량으로 저장한 표이다.
- 해시함수 MD5, SHA-1, SHA-2 등을 이용
- 레인보우 테이블 크기는 작은 것도 기본적으로 100GB이상이 된다.(보통 TB 단위)
- 레인보우 테이블을 이용한 공격도 일종의 **사전 공격**이다.
  → 미리 만들어진 테이블에서 해시값을 뽑아서 대입하므로
  → Rainbow Table을 이용하면 해시값 계산 시간이 절약되어 신속한 공격 가능
  → Rainbow Table을 이용하면 12자리 숫자로 된 **비밀번호**를 순식간에 뚫을 수 있다.
- 레인보우 테이블은 R(reduction) 함수를 이용하여 충분히 작은 크기로 줄일 수 있다.
- 레인보우 테이블은 크기를 줄여도 기본적으로 수십 GB이상이 된다.
- R 함수는 비밀번호로 사용되는 문자열을 해시값으로 만드는 함수이다.

정답 : ②