1. 공개키 암호 개요

① 공개키 암호는 이중키, 비대칭키 암호 방식이라고도 한다.
② 공개키 암호는 암호화와 복호화에 서로 **다른 키**를 사용한다.(비대칭키)
③ 공개키 암호는 암복호화를 위해서 반드시 한 쌍의 키가 필요하다.(공개키, 개인키)

공개키(public key)	누구나 알고 있어도 상관이 없다.(공개된 저장소에 보관)
개인키(private key)	개인키 소유자 자신만 알고 있어야 한다.

④ 송수신자는 서로 다른 키를 사용하므로 제3자에게 비밀이 누설될 가능성이 없다.
⑤ 공개키 암호 알고리즘에 사용되는 키는 길이가 길다.(10진수 300자리 이상)
→ 길이가 긴 키를 이용하므로 평문을 암호문으로 만드는데 많은 시간을 필요로 한다.
⑥ 공개키 암호 알고리즘은 일반적으로 복잡하고, 속도가 느리다.
→ 따라서, 공개키 암호는 적은 양의 메시지 비밀통신에 적합하다.

◈ **대칭키 / 공개키 암호 비교**

대칭키 암호	• 송수신자 사이에 키 교환을 어떻게 할 것인가? → 문제점 • 대칭키는 반드시 비밀유지가 되어야 한다. • 알고리즘과 암호문의 샘플을 이용하여 대칭키를 찾을 수 없어야 한다. • 공개키 암호에 비해 암호화, 복호화 속도가 빠르다.
공개키 암호	• 공개키를 어떻게 공개할 것인가? → 문제점 • 개인키는 반드시 비밀유지가 되어야 한다. • 하나의 키를 이용하여 대응하는 키를 찾을 수 없어야 한다. • 키 사용 기간은 비교적 길다.(빈번한 키 교체는 불필요)

• 공개키를 인터넷 등에 무작정 공개하면,
• 특정인의 공개키를 찾기 어렵고, 누군가에 의해 공개키가 위조될 수 있다.

◈ **소인수분해와 이산대수**

공개키 암호 안전성은 **"소인수분해와 이산대수(이산로그)"** 계산 문제의 어려움에 기반한다.
실제, 이들 문제를 푸는데 얼마나 어려운지 직접 경험하기로 한다.

문제 1

다음 두 문제의 값을 구하여라.(소인수분해 계산 어려움)

① $x = 13 \times 17 = ?$

② 수 221을 소인수분해 하시오.

[풀이]----------

① $x = 13 \times 17 =$ **221** → 매우 쉽다. 수가 커져도 특별하게 더 어려운 것은 없다.

② 수 **221**을 소인수분해 → 조금 어렵다. 수가 커질수록 더 어려울 수 있다.

$13 \overline{)\ 221}$

17 $\quad\therefore\ 221 = 13 \times 17$

문제 2

지수와 로그이다. 각 식의 값을 구하여라.(이산대수 계산 어려움)

① $x = 3^5 = ?$

② $x = \log_3 243 = ?$

[풀이]----------

① $x = 3^5 = 3\times3\times3\times3\times3 =$ **243** → 3을 5번 곱하면 된다. 어려울 것이 없다.

② $x = \log_3 243 = \log_3 3^5 =$ **5** → 수가 커지면 더 어려울 수 있다.

☞ **이산대수(이산로그)**

• 수식 $x = \log_3 243$에서 x를 **이산대수**라 한다.

◈ **공개키 암호 탄생**

- 1976년, 디피(Diffie)와 헬만(Hellman)이 공개키 암호의 아이디어를 발표
  → 공개키가 가져야 할 특성을 제시
- 1977년, 배낭 암호(knapsack cryptosystem) 알고리즘이 발표되었다.
  → 배낭 암호는 랠프 메르클레(Ralph Merkle)와 마틴 헬만(Martin Hellman)이 발표
  → 배낭 암호는 최초의 기발한 공개키 암호시스템이다.
  → 배낭 암호는 오늘날 기준으로 안전하지는 않지만 공개키 암호를 만드는 토대가 되었다.
- 1978년, RSA 암호 알고리즘이 발표되었다.
- 1985년, ElGamal 암호 알고리즘이 발표되었다.
- 최근, 타원곡선 이론에 근거한 타원곡선암호 알고리즘이 개발되었다.

// 공개키 암호 안전성

공개키 암호 안전성은 **"소인수분해와 이산대수(이산로그)"** 계산 문제의 어려움에 기반한다.

소인수분해 문제	RSA : RSA는 지수 합동을 이용한 암호 방식
	Rabin : 2차 잉여문제를 이용한 암호 방식(RSA **변형**)
이산대수 문제	ElGamal : Diffie-Hellman 키 교환 알고리즘 응용
	ECC : 타원곡선 이론 응용(160bit 정도의 짧은 키 사용 가능)
	DSA : 디지털 서명 규격용

// 공개키 암호 원리

RSA 암호	• RSA 암호는 **지수 합동**에 근거한다. • RSA 암호에서는 소인수분해를 하지 않는다. • 암호화 : C = M^e mod n → 모듈로 지수 계산 형식이다. • 복호화 : M = C^d mod n
Rabin 암호	• Rabin 암호는 **이차 합동**에 근거한다. • 이차 합동은 2차 잉여문제이다. • 암호화 : C = M^2 mod n → 이차 합동(2차 잉여문제) 형식이다. • 복호화 : M = $C^{\frac{1}{2}}$ mod n

기출문제 분석

1. 공개키 암호 알고리즘에 대한 설명으로 옳은 것은? [2016년 국가 9급]

① Diffie-Hellman 키 교환 방식은 중간자(man-in-the-middle) 공격에 강하고 실용적이다.
② RSA 암호 알고리즘은 적절한 시간 내에 인수가 큰 정수의 소인수분해가 어렵다는 점을 이용한 것이다.
③ 타원곡선암호 알고리즘은 타원곡선 대수 문제에 기초를 두고 있으며, RSA 알고리즘과 동일한 안전성을 제공하기 위해서 더 긴 길이의 키를 필요로 한다.
④ ElGamal 암호 알고리즘은 많은 큰 수들의 집합에서 선택된 수들의 합을 구하는 것은 쉽지만, 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용한 것이다.

♤ **공개키 암호 알고리즘**

- 디피-헬만 키 교환은 다음 2가지 공격에 대해 취약점을 가진다.
  → 이산대수 공격 / 중간자 공격(man in the middle attack, MITM)
- 타원곡선암호 알고리즘은 이산대수 문제에 기초한 공개키 암호 알고리즘이다.
  → RSA에 비하여 짧은 키를 사용하면서 비슷한 수준의 안전성을 제공한다.
- ElGamal 암호 안전성은 유한체상에서 이산대수 문제 해결 어려움에 기반을 한다.

정답 : ②

2. 공개키 암호시스템에 대한 설명으로 옳은 것만을 모두 고르면? [2021년 국가 9급]

ㄱ. 한 쌍의 공개키와 개인키 중에서 개인키만 비밀로 보관하면 된다.
ㄴ. 동일한 안전성을 가정할 때 ECC는 RSA보다 더 짧은 길이의 키를 필요로 한다.
ㄷ. 키의 분배와 관리가 대칭키 암호시스템에 비하여 어렵다.
ㄹ. 일반적으로 암호화 및 복호화 처리속도가 대칭키 암호시스템에 비하여 빠르다.

① ㄱ, ㄴ ② ㄱ, ㄹ ③ ㄴ, ㄷ ④ ㄷ, ㄹ

♤ **공개키 암호시스템**

ㄷ. 키의 분배와 관리가 대칭키 암호시스템에 비하여 **어렵다.(×)**
→ 키의 분배와 관리가 대칭키 암호시스템에 비하여 **쉽다.**
ㄹ. 일반적으로 암호화 및 복호화 처리속도가 대칭키 암호시스템에 비하여 **빠르다.(×)**
→ 일반적으로 암호화 및 복호화 처리속도가 대칭키 암호시스템에 비하여 **느리다.**

정답 : ①

3. 공개키 암호에 대한 설명 중 ㉠~㉢에 들어갈 말로 옳게 짝지어진 것은? [2017년 국가 9급]

○ (㉠)의 안전성은 유한체의 이산대수 계산의 어려움에 기반을 둔다.
○ (㉡)의 안전성은 타원곡선군의 이산대수 계산의 어려움에 기반을 둔다.
○ (㉢)의 안전성은 소인수분해의 어려움에 기반을 둔다.

	㉠	㉡	㉢
①	ElGamal 암호시스템	DSS	RSA 암호시스템
②	Knapsack 암호시스템	ECC	RSA 암호시스템
③	Knapsack 암호시스템	DSS	Rabin 암호시스템
④	ElGamal 암호시스템	ECC	Rabin 암호시스템

♤ **공개키 암호시스템**

◉ **ElGamal 암호시스템**

- ElGamal 암호 안전성은 **유한체상에서 이산대수** 문제 해결 어려움에 기반을 한다.
- ElGamal 암호는 암호문 길이가 **평문의 2배**가 되는 결점이 있다.(통신량 증가)

◉ **타원곡선암호(elliptic curve cryptosystem; ECC)**

- ECC는 타원곡선 이산대수 계산 어려움에 기반한 공개키 암호 알고리즘이다.
- ECC는 무선 환경과 같이 전송량과 계산량이 상대적으로 열악한 환경에 적합하다.

◉ **Rabin 암호시스템**

- Rabin 암호 해독은 큰 수 N을 소인수분해하는 정도의 어려움으로 증명되어 있다.
- Rabin의 암호 시스템은 복호화를 하면 동등 확률의 평문 후보 4개가 나타난다.

정답 : ④

4. 다음 중 소인수분해 문제 어려움에 기초한 암호 알고리즘은 무엇인가? [2014년 국회 9급]

① Diffie-Hellman ② SHA-1
③ AES ④ DES ⑤ RSA

♤ **공개키 암호 알고리즘**

- RSA 암호 안전성은 소인수분해 문제 해결의 어려움에 기반을 한다.

정답 : ⑤

5. 공개키 암호(public key cryptosystem)에 대한 설명으로 옳은 것은? [2014년 서울 9급]

① 대표적인 암호로 AES, DES 등이 있다.
② 대표적인 암호로 RSA가 있다.
③ 일반적으로 같은 양의 데이터를 암호화하기 위한 연산이 대칭키 암호(symmetric key cryptosystem)보다 현저히 빠르다.
④ 대칭키 암호(symmetric key cryptosystem)보다 수백 년 앞서 고안된 개념이다.
⑤ 일반적으로 같은 양의 데이터를 암호화한 암호문(ciphertext)이 대칭키 암호(symmetric key cryptosystem) 보다 현저히 짧다.

♤ **공개키 암호(public key cryptosystem) – 비대칭키**

• 공개키 암호의 대표적인 암호로 RSA가 있다.

정답 : ②