6. Rabin 암호

① Rabin 암호에서 (공개키, 개인키) 생성

- 서로소인 두 소수 p, q를 선택하고, 곱 n = p × q를 계산한다.
- n을 공개키로 하고, {p, q}를 개인키로 한다.(단순)

---

② Rabin 암호에서 메시지 암호화 및 복호화

암호화	C = M^2 (mod n)
복호화	M = $C^{\frac{1}{2}}$ (mod n)

- C는 암호문, M은 메시지(평문)
- Rabin 암호 알고리즘은 **2차 잉여문제**를 이용한 암호화 방식이다.

③ Rabin 암호는 암호화 과정에서 평문에 대한 제곱 연산을 실시한다.(이차합동)

- Rabin 암호는 RSA 암호의 변형이다.
- Rabin 암호는 RSA 암호보다 계산이 훨씬 빠르다.(단순)
- Rabin 암호는 제한된 메모리를 갖고 있는 플랫폼에서도 잘 작동될 수 있다.(스마트카드)

④ Rabin의 암호는 비결정적 알고리즘이다.

- 즉, 결정적 알고리즘이 아니다.(의미 있는 해를 고르면 그것이 평문이 된다)
- Rabin의 암호시스템은 복호화를 하면 동등 확률의 **평문 후보 4개**가 나타난다.
- **중국인의 나머지 정리**를 이용해서 4개의 가능한 평문을 구할 수 있다.
- 평문 후보 4개 중에서 하나의 최종 답을 선택하는 것은 수신자가 결정한다.
- 대부분의 경우, 수신자는 답을 쉽게 선택할 수 있다.

⑤ Rabin 암호 안전성은 소인수분해 문제 해결의 어려움에 기반을 한다.

- Rabin 암호 해독은 큰 수 N을 소인수분해하는 정도의 어려움으로 증명되어 있다.
- Rabin는 RSA 암호만큼 안전하다고 할 수 있다.
- 공격자가 암호 해독을 위해서 반드시 소인수분해를 하는 것은 아니다.

예제

평문 M=10을 서로 다른 두 소수 p=7, q=11을 이용한 암호화 및 복호화
[p≡q≡3 (mod 4)인 경우의 Rabin 암호 알고리즘 예제]

(1) 준비 과정(키 생성)

• p≡q≡3 (mod 4)와 합동인 서로 다른 두 소수 p=7, q=11을 선택하고,

• n = p • q = 7 • 11 = 77을 구한다.

→ 공개키 : 77. 개인키 : {7, 11}

(2) 암호화 과정(송신자)

• 평문 M = 10을 암호화 한다.(n보다 작은 평문 M을 법 n에 관해 제곱하여 C 생성)

• 암호화 : C = M^2 mod n이므로

C = 10^2 mod 77 = 100 = **23** mod 77 → **23**을 수신자에게 전송

(3) 복호화 과정(수신자)

① 수신자는 23을 수신하고

먼저, 복호화는 다음 두 이차합동식의 해를 구해야 한다.

$$\begin{cases} x^2 \equiv 23 \equiv 2 \equiv 3^2 \pmod 7 \\ x^2 \equiv 23 \equiv 1 \equiv 1^2 \pmod{11} \end{cases}$$

② p≡q≡3 (mod 4)이다. (만약, p≠3 또는 q≠3 (mod 4)이면 일반적인 풀이 사용)

$$r \equiv 23^{\frac{(7+1)}{4}} \equiv 2^2 \equiv 4 \pmod 7$$

$$s \equiv 23^{\frac{(11+1)}{4}} \equiv 1^3 \equiv 1 \pmod{11}$$

③ Euclid 알고리즘을 이용하여 (7, 11) = 1 = 7 • (−3) + 11 • (2)을 구한다.

$$\begin{cases} m_1 \equiv 7 \cdot (-3) \cdot 1 + 11 \cdot 2 \cdot 4 \equiv 21 + 88 \equiv 32 \pmod{77} \\ m_2 \equiv 7 \cdot (-3) \cdot 1 - 11 \cdot 2 \cdot 4 \equiv 21 - 88 \equiv -67 \equiv 10 \pmod{77} \end{cases}$$

④ 이차합동식 x^2 ≡ 23 (mod 77)의 해는 다음과 같다.

$$\begin{cases} x \equiv \pm m_1 \equiv \pm 32 \pmod{77} \\ x \equiv \pm m_2 \equiv \pm 10 \pmod{77} \end{cases}$$ → 이 중에 평문 m=10이 있다.

◈ Rabin 암호 알고리즘 - 일반적인 구조

단 계	행위자	내 용
준 비	수신자	• 서로소인 두 소수 p, q를 선택하고, 곱 n = p×q를 계산한다. • n을 공개키로 하고, {p, q}를 개인키(비밀키)로 한다.
암호화	송신자	• n보다 작은 수인 평문 M을 법 n에 관해 제곱하여 암호문 C를 생성하여 수신자에게 보낸다. • 암호문 : C = $M^2 \pmod{n}$
복호화	수신자	① 수신된 암호문 C를 개인키 {p, q}를 이용하여 법 n에 관한 이차잉여 제곱근을 계산하면 평문 M을 얻을 수 있다. ② C는 법 n에 이차잉여이므로, 법 p와 q에도 이차잉여가 된다. $\begin{cases} x^2 \equiv C \pmod{p} \\ x^2 \equiv C \pmod{q} \end{cases}$ → 2차합동식 성질 ③ 2차 연립합동식의 각 해를 다음처럼 나타내면 $\begin{cases} x \equiv \pm m_1 \pmod{p} \\ x \equiv \pm m_2 \pmod{q} \end{cases}$ ④ 중국인의 나머지 정리에 의해 연립합동식 해를 구할 수 있다. $\begin{cases} x \equiv m_1 \pmod{p}, & x \equiv m_2 \pmod{q} \\ x \equiv m_1 \pmod{p}, & x \equiv -m_2 \pmod{q} \\ x \equiv -m_1 \pmod{p}, & x \equiv m_2 \pmod{q} \\ x \equiv -m_1 \pmod{p}, & x \equiv -m_2 \pmod{q} \end{cases}$ → 4쌍의 해 중에 의미 있는 평문 M이 존재한다.

◈ Rabin 암호에서 두 소수 p, q가 "p≡q≡3 (mod 4)"인 경우

• Rabin 알고리즘에서 복호화 할 때 개인키 p, q를 이용하여 "2차잉여"를 구해야 한다.
→ 해를 구하는데 시간이 많이 소요될 수 있다.

• 그런데, "p≡q≡3 (mod 4)"인 두 소수 p, q를 이용하면 좀 더 쉽게 계산할 수 있다.

// 중국인의 나머지 정리

문제

상자에 들어 있는 사과를 다음처럼

- 사과를 3개씩 묶었더니 1개가 남았고,
- 사과를 5개씩 묶었더니 2개가 남았고,
- 사과를 7개씩 묶었더니 3개가 남았다.

상자에 있는 사과는 최소 모두 몇 개인가? – 최소의 자연수 구하기

(풀이) 풀이 과정은 다음과 같다.

사과 묶음	나머지	나머지가 1이 되는 공배수 찾기	나머지 * 공배수
① 3개씩 묶음	1개	5와 7의 공배수이면서 3으로 나누면 나머지가 1이 되는 공배수 = 70	1 * 70 = 70
② 5개씩 묶음	2개	7과 3의 공배수이면서 5로 나누면 나머지가 1이 되는 공배수 = 21	2 * 21 = 42
③ 7개씩 묶음	3개	3과 5의 공배수이면서 7로 나누면 나머지가 1이 되는 공배수 = 15	3 * 15 = 45

④ 그리고, ①②③에서 구한 각 수를 더한다. a = 70 + 42 + 45 = 157

⑤ 사과를 묶은 수를 곱한 결과를 구한다. m = 3 * 5 * 7 = 105

⑥ a = 157이 m = 105 값보다 크면, 105를 뺀다. 157 – 105 = 52

→ 만약, 뺀 값이 105보다 크면 105보다 작은 수가 될 때까지 뺀다.

⑦ 이처럼, 105보다 작은 수가 될 때까지 빼서 얻은 수, 52가 구하려는 사과 개수이다.

[확인] 구한 값 52를 이용하여 나머지를 구해 보면 된다. (사과 수는 52개)

52 mod 3 = 1 → 사과를 3개씩 묶었더니 1개가 남았고,

52 mod 5 = 2 → 사과를 5개씩 묶었더니 2개가 남았고,

52 mod 7 = 3 → 사과를 7개씩 묶었더니 3개가 남았고,

// 중국인의 나머지 정리

- 중국인의 나머지 정리는 중국 대대로 전해오는 유명한 수학책에 나오는 내용이다.
- 중국인의 나머지 정리는 연립합동식을 하나의 합동식으로 만드는 것이다.
- 연립합동식은 말 그대로 합동식이 여러 개 있는 것이다.
- 합동식 : $ax \equiv b \pmod{m}$

기출문제 분석

1. 공개키 암호시스템에 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.
  → 공개키 e를 이용하여 개인키 d를 계산하는 것은 어렵다.
- ElGamal 암호는 암호문 길이가 **평문의 2배**가 되는 결점이 있다.(통신량 증가)
- ElGamal 암호는 타원곡선 이산대수 기반으로 전환할 수 있다.

// 타원곡선 암호(elliptic curve cryptosystem; ECC)

- ECC는 타원곡선 이산대수 문제에 기초한 공개키 암호 알고리즘이다.
- ECC의 안전성은 무작위 타원곡선의 이산대수를 찾는 어려움에 의존한다.
- 타원곡선을 정하고, 그 곡선 상에 있는 점에 대하여 특수 연산을 정의한다.
- ECC는 무선 환경과 같이 전송량과 계산량이 상대적으로 열악한 환경에 적합하다.
- 현재, 타원곡선 암호는 전자서명과 키 교환에 많이 적용되고 있다.

// Rabin 암호시스템

- Rabin 암호 해독은 큰 수 N을 **소인수분해**하는 정도의 어려움으로 증명되어 있다.
- Rabin 암호 안전성은 소인수분해 문제 해결의 어려움에 기반을 한다.
- Rabin의 암호시스템은 복호화를 하면 동등 확률의 평문 후보 4개가 나타난다.
- Rabin의 암호는 **비결정적** 알고리즘이다.

정답 : ④