8. ElGamal 암호

// ElGamal(엘가말) 암호 알고리즘

단 계	행위자	내 용
준 비	수신자	① 큰 소수 p와 Z_p^*의 원소 중에서 **원시근 g**를 선택한다. ② 개인키 d를 선택하고, $e \equiv g^d \pmod p$를 계산한다. ③ {p, g, e}를 공개키로 한다. → 공개키가 3개
암호화	송신자	① 평문 m에 대해, 임의의 **난수 r**을 선택한다. • 난수 r은 **비밀**로 유지한다. ② 암호문 생성 : $\begin{cases} c_1 \equiv g^r \pmod p \\ c_2 \equiv m \times e^r \pmod p \end{cases}$ 을 계산한다. ③ 암호문 **(c_1, c_2)**를 수신자에게 보낸다. → **암호문이 2개**
복호화	수신자	• 수신된 암호문 (c_1, c_2)와 • 수신자 개인키 d를 이용하여 평문 m을 구한다. • $m = [c_2 \times (c_1^d)^{-1}] \bmod p$ → 복호화 • $m = [c_2 \times c_1^{p-1-d}] \bmod p$와 같음**(페르마 리틀 정리)**

① ElGamal 암호는 같은 메시지, 같은 키에 대해 암호화마다 다른 암호문을 얻는다.
- 이유는 암호에 임의의 **난수 r을 사용**하기 때문이다.(난수 생성기 필요)
- 송신자가 암호문을 보낼 때마다 r을 바꾸지 않으면 암호공격에 취약하다.

② ElGamal 암호는 암호문 길이가 평문의 2배가 되는 결점이 있다.(통신량 증가)

③ ElGamal 암호는 "Diffie-Hellman의 키교환"에 암호 알고리즘을 접목한 형태이다.
- ElGamal 암호는 RSA 암호가 활용될 수 있는 곳에 어디에나 사용될 수 있다.

④ ElGamal 암호는 타원곡선 이산대수 기반으로 전환할 수 있다.
- 타원곡선을 이용한 암호는 최근 주목받고 있는 공개키 암호 알고리즘이다.

⑤ ElGamal 암호 안전성은 유한체상에서 이산대수 문제 계산 어려움에 기반을 한다.
- 공개키 e를 이용하여 개인키 d를 계산하는 것은 어렵다.

기출문제 분석

1. ElGamal 공개키 암호 방식의 기본 원리인 이산대수 문제를 바르게 설명한 것은? (단, p, q는 소수, α는 p의 원시원소이고, Φ( )는 Euler's totient 함수이다) [2016년 국가 7급]

① a, p, q가 주어졌을 때, y = a^x mod p를 만족하는 x를 구하는 문제

② a, p, x, Y가 주어졌을 때, Y = a^x mod p를 만족하는 a^{xy} mod p를 구하는 문제

③ n이 주어졌을 때, n = p • q를 만족하는 Φ(n)을 구하는 문제

④ n과 Φ(n)과 서로소인 e가 주어졌을 때, n = p • q이면서 e • d mod Φ(n) = 1을 만족하는 d를 구하는 문제

♤ **ElGamal(엘가말) 암호**

- a, p, q가 주어졌을 때,
- y = a^x mod p를 만족하는 x를 구하는 문제
  ↓다음 내용과 같은 것이다.
- 큰 소수 p, **원시근 g**, 개인키 d를 선택하고
- e≡ g^d (mod p)를 계산한다.

- 개인키 : d
- 공개키 : {p, g, e} → 공개키가 3개

◈ **오일러 파이 함수(Euler's totient 함수)**

- Φ(n)은 오일러 파이 함수이다.
- Φ(n)은 1부터 n까지 양의 정수 중에 n과 서로소인 것의 개수를 나타내는 함수이다.
- Φ(n)은 양의 정수 n에 대하여 정의된다.

정답 : ①