[문제] 정수의 소인수분해를 기반으로 한 RSA 암호에서 공개키 (e, n) = (7, 33)을 이용하여 생성된 암호문 C 값이 7일 때, 이를 다시 복호화한다면 원문 메시지 값은? [2017년 국가 7급]

① 11 ② 13 ③ 17 ④ 19

♤ RSA 암호 알고리즘 - 해킹 문제

// 문제 분석

- 먼저, 이 문제는 해킹 문제이다. 해서, 풀이 방법은 여러 가지가 될 수 있다.
- RSA 암호 알고리즘에서 개인키를 모르는데 어떻게 암호문을 해독할 수 있는가?
- c = m^e mod n 이므로
- 7 = m^7 mod 33 → 여기서, 원문 메시지 m을 찾는 문제이다.(m = 13)

// 답을 찾는 방법(풀이 방법)

- m = 13이므로
- 7 = 13^7 mod 33을 증명하면 된다.

// 풀이 1 : 단순한 지수 계산

- 13^7 = 62748517 = 7 mod 33 → 원문 메시지 m이 13이라는 것을 증명
  ↳ 이 방식은 13^7을 구하는데 시간이 많이 소모되므로 짧은 시간에는 불가능

// 풀이 2 : 모듈러 연산에서 지수 연산은 곱셈의 반복으로 간단하게 계산할 수 있다.

- c = 13^7 mod 33 → 계산 결과가 **c = 7이라는 것을 증명**하면 된다.
  ↓**곱셈 반복 원리 이용**
- 13^7 mod 33 = **?**
- 13^2 = (13 × 13) mod 33 = 169 mod 33 = **4**
- 13^4 = (13^2 × 13^2) mod 33 = (4 × 4) mod 33 = 16 mod 33 = **16**
- 13^7 = (13 × 13^2 × 13^4) mod 33 = (13 × 4 × 16) mod 33 = 832 mod 33 = **7**
  → 계산 결과에서 **c = 7**이라는 것은 원문 메시지 **m이 13이라는 것을 증명**

// 풀이 3 : RSA 암호시스템 응용 - 만약, d 값이 크면 풀이 2를 알아야 함

- p=3, q=11이면, n = p × q = 3 × 11 = **33**
- Phi(n) = (p−1)(q−1) = (3−1)(11−1) = 2 × 10 = **20**
- (e × d) mod 20 = (7 × d) mod 20 = 1
  ↓**d=3**이면
- (e × d) mod 20 = (7 × 3) mod 20 = 21 mod 20 = **1**
- **m** = c^d mod n = 7^3 mod 33 = 343 mod 33 = **13** → 메시지 복호화,

---

정답 : ②