

## 정보보호기술

### 2019년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

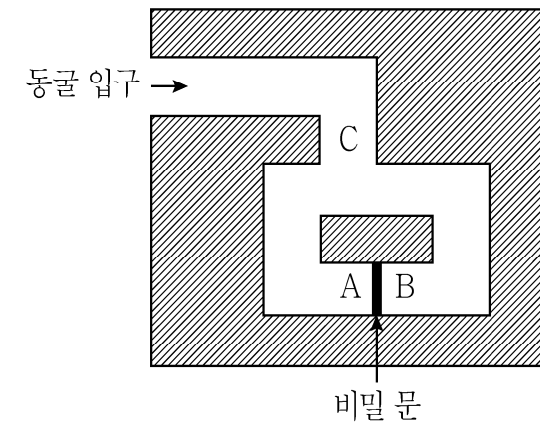
성명 :

제 1 문. Alice는 패딩(padding)을 사용하지 않는 기본 RSA(textbook RSA)를 이용하여 두 소수(prime number)  $p = 17$ ,  $q = 19$ 를 선택하고, 이에 대응하는 공개정보  $(n, e) = (323, 13)$ 을 생성하였다. 다음 물음에 답하시오. (총 15점)

- 1) Alice의 개인키(private key)  $d$ 를 구하고, 그 계산과정을 기술하시오. (5점)
- 2) Bob이 평문  $m = 2$ 를 Alice에게 보내고자 한다. Alice의 공개정보를 활용하여 암호문  $c$ 를 구하고, 그 계산과정을 기술하시오. (5점)
- 3) 두 정수  $a$ ,  $b$ 와 모듈러스(modulus)  $N$ 에 대해 함수  $F$ 를  $F(a, b, N) = ab \pmod{N}$ 라 정의하자. 이진 모듈러 뺄승(binary modular exponentiation 또는 square-and-multiply) 알고리즘을 이용하면, 함수  $F$ 를 5회만 호출하여 2)의 암호문  $c$ 를 구할 수 있다. 그 과정을 설명하시오. (5점)

제 2 문. 영지식 증명(zero knowledge proof)은 자신(증명자)이 가지고 있는 비밀정보를 노출하지 않고 자신이 그 비밀정보를 알고 있음을 상대방(검증자)에게 증명하는 방법이다. 따라서 영지식 증명은 증명자와 검증자 사이에 프로토콜로 주어진다. 다음 물음에 답하시오. (총 15점)

- 1) 영지식 증명 프로토콜이 만족해야하는 세 가지 성질인 완전성(completeness), 정당성(soundness), 영지식성(zero-knowledgeness)을 각각 설명하시오. (6점)
- 2) 그림과 같이 동굴 내부에 비밀 문이 있고, 증명자 P는 비밀 문을 여는 비밀번호를 알고 있다. 증명자 P가 검증자 V에게 비밀번호를 알려주지 않고도 증명자 P가 비밀번호를 알고 있음을 증명할 수 있는 영지식 증명 프로토콜을 설명하시오. (단, A, B, C는 동굴 내부의 특정 위치를 나타내고, 비밀 문은 A나 B 어느 쪽에서든 비밀번호를 알아야만 열 수 있다) (6점)



- 3) 2)에서 설명한 프로토콜이 1)의 세 가지 성질을 만족함을 설명하시오. (3점)

제 3 문. 암호 공격 또는 암호 분석에 대한 다음 물음에 답하시오. (총 10점)

- 1) 암호 공격 기법 중 가장 대표적인 방법인 암호문 단독 공격(Ciphertext only Attack), 알려진 평문 공격(Known Plaintext Attack), 선택 평문 공격(Chosen Plaintext Attack)에 대해 설명하시오. (6점)
- 2) 암호 분석에서 절대 안전성(Unconditionally Secure)과 계산상 안전성(Computationally Secure)에 대하여 정의하시오. 그리고 절대 안전성을 제공할 수 있는 암호화 방법의 명칭을 적고, 이에 대해 설명하시오. (4점)

제 4 문. 전자 서명(Digital Signature)은 전자문서에 서명을 하였음을 나타내기 위해 전자문서에 첨부되는 전자적 형태의 정보를 말한다. 전자 서명에서는 서명자가 ‘서명 작성’ 행위를 하면 검증자가 ‘서명 검증’ 행위로 첨부된 전자 서명을 검증한다. 다음 물음에 답하시오. (총 10점)

- 1) 공개키 기반 구조(PKI)와 해시 함수를 이용한 전자 서명의 ‘서명 작성’과 ‘서명 검증’ 과정을 제시하시오. (4점)
- 2) 전자 서명은 전자문서의 무결성 검증, 서명자 인증과 부인 방지의 기능을 제공한다. 그 이유를 각각 기술하시오. (6점)

## 인사혁신처 시험출제과장