

정보보호 기술

2022년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 다음은 공개키 암호(Public Key Cryptosystem) 방식의 RSA 암호 알고리즘이다.
물음에 답하시오. (총 10점)

- ① 두 개의 소수 p 와 q 를 선택한다.($p \neq q$)
- ② 두 수를 곱하여 $n = pq$ 를 계산한다.
- ③ $\phi(n) = (p-1)(q-1)$ 을 계산한다.
- ④ 1보다 크고 $\phi(n)$ 보다 작으며, $\phi(n)$ 과 서로소인 A 를 찾는다.
- ⑤ 확장 유클리드 알고리즘(Extended Euclidean Algorithm)을 이용하여
수식 (가)을 만족하는 B 를 찾는다.
- ⑥ 여기에서 공개키는 (나)이고, 개인키는 (다)이다.

- 1) (가) ~ (다)에 들어갈 내용을 각각 제시하시오. (3점)
- 2) $p = 3$, $q = 11$, $A = 7$ 로 주어진 상태에서 확장 유클리드 알고리즘을 이용하여 B 를 계산하고, 계산과정을 기술하시오. (3점)
- 3) $p = 3$, $q = 11$, $A = 7$ 및 2)에서 구한 B 를 이용하여, 평문이 5로 주어질 때 암호문을 계산하고, 계산과정을 기술하시오. 또한, 계산한 암호문을 복호화하는 계산과정을 기술하시오. (4점)

제 2 문. 사물인터넷(IoT, Internet of Things) 환경에서는 센서나 작은 디바이스에서 암호를 이용한 보안시스템 구현이 많이 사용되고 있다. 이 경우 센서나 디바이스의 입출력 처리 부분을 직접 공격하지 않고, 시스템이 동작하면서 발생하는 전자적 신호를 분석하여 암호시스템을 공격하는 부채널공격(SCA, Side Channel Attack) 방법이 있다. 부채널공격과 관련하여 다음 물음에 답하시오. (총 5점)

- 1) 전력분석을 이용한 부채널공격 방법을 설명하시오. (2점)
- 2) 단순 소모전력분석(SPA, Simple Power Analysis) 공격 방법을 RSA 암호 알고리즘의 암호·복호화 과정의 예를 들어 설명하시오. (3점)

제 3 문. IETF의 RFC 2104에 정의되어 있는 HMAC은 암호학적 해시 함수(Cryptographic Hash Function)에 기반한 메시지 인증 코드(MAC, Message Authentication Code)이다. 송신자와 수신자가 공유하고 있는 비밀키(Secret Key) K 와 인증 대상 텍스트 M 에 대해 다음과 같이 계산할 때, 물음에 답하시오. (총 15점)

$$HMAC(K, M) = H[(K \oplus opad) \parallel H[(K \oplus ipad) \parallel M]]$$

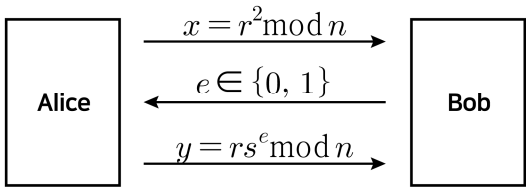
※ $H[\cdot]$ 는 암호학적 해시 함수, $ipad$ 는 0x3636...36, $opad$ 는 0x5C5C...5C, \oplus 는 배타적 논리합(XOR), \parallel 는 연접(Concatenation)

- 1) 송신자가 $(M, HMAC(K, M))$ 을 전송하였을 때, 비밀키 K 를 소유한 수신자는 M 의 무결성(Integrity) 검증 및 데이터 출처 인증(Data Origin Authentication)을 수행할 수 있다. 수신자가 어떤 작업을 하면 되는지, 그리고 이것이 왜 무결성과 데이터 출처 인증을 보장하는지 설명하시오. (5점)
- 2) 만약 충돌 저항성(Collision Resistance)을 만족하지 않는 해시 함수를 사용할 경우, 공격자가 어떻게 메시지 변조 공격을 수행할 수 있는지 설명하시오. (5점)
- 3) 위와 같은 HMAC이 송신자 부인봉쇄(Origin Nonrepudiation) 기능을 제공하는지 여부와 그러한 판단의 근거를 제시하시오. (5점)

제 4 문. 다음은 영지식 증명(Zero-Knowledge Proof) 중 Fiat-Shamir 프로토콜이다. 물음에 답하시오. (총 20점)

아래 그림은 Fiat-Shamir 프로토콜을 나타내고 있다. 신뢰받는 제3자는 두 개의 큰 소수 p 와 q 를 선택하여 $n = p \times q$ 를 계산한다. 이 값 n 을 공개하고 두 소수 p 와 q 는 비밀로 한다. Alice는 비밀 값 s 를 $1 < s < n - 1$ 범위에서 선택하고 $v = s^2 \bmod n$ 을 계산한다. Alice는 s 를 자신의 개인키로 보관하고 v 를 자신의 공개키로 하고 제3자에게 등록을 한다. 주장자(Claimant)인 Alice는 검증자(Verifier)인 Bob에게 s 에 대한 어떤 정보도 노출하지 않고 s 를 알고 있다고 설득해야 한다. Fiat-Shamir 프로토콜의 절차는 다음과 같다.

- ① Alice는 난수 r 을 선택하여 Bob에게 $x = r^2 \bmod n$ 을 전송한다.
- ② Bob은 난수 값 $e \in \{0, 1\}$ 를 선택하여 Alice에게 전송한다.
- ③ Alice는 $y = rs^e \bmod n$ 으로 응답한다.
- ④ Bob은 식 $y^2 \bmod n = xv^e \bmod n$ 이 성립하는지 확인한다.



위의 절차가 하나의 라운드가 된다. 이러한 라운드를 여러 차례 수행한다. 매 라운드마다 e 값을 0과 1중에서 임의로 선택한다. Alice는 자신을 인증하기 위해서 모든 라운드를 통과해야만 한다. 만약에 단 한 라운드라도 실패한다면, 이 과정은 끝나게 되고 Alice는 인증을 통과하지 못한다.

- 1) 진짜 Alice가 자신의 개인 키 s 를 이용하여 프로토콜을 정상적으로 수행했을 때, Bob이 전송하는 e 값이 0일 경우와 1일 경우로 나누어 Alice가 인증을 정상적으로 통과함을 보이시오. (5점)
- 2) 공격자가 Alice로 위장하기 위해서 Bob이 단계 ②에서 메시지 e 를 0으로 전송할 것으로 기대할 경우와 1로 전송할 것으로 기대할 경우, 두 경우에 대해 Bob의 검증과정을 통과하기 위한 방법을 제시하시오. (10점)
- 3) 공격자가 위의 라운드를 n 회 수행하였을 때, Bob을 속일 수 있는 확률이 얼마인지 설명하시오. (5점)

인사혁신처 시험출제과장