

정보보호기술

2016년 시행 5급 공채(기술) 제2차시험

응시번호 :

성명 :

제 1 문. 블록 암호 알고리즘은 긴 평문을 암호화하기 위하여 일반적으로 블록 암호 운영모드를 이용하며, 대표적인 블록 암호 운영모드로는 ECB, CBC, OFB, CFB, CTR 등이 있다. 다음 물음에 답하시오. (총 15점)

- 1) ECB 모드는 안전성에 문제가 있다고 알려져 있다. 그 이유를 설명하시오. (3점)
- 2) CBC 모드를 사용하면 ECB 모드의 안전성 문제를 해결할 수 있다. CBC 모드의 암호·복호화 방식을 설명하고, ECB 모드의 안전성 문제를 해결하기 위해 사용된 CBC 모드의 2가지 특성을 설명하시오. (6점)
- 3) CTR 모드의 암호·복호화 방식을 설명하고, CBC 모드와 비교한 CTR 모드의 장점을 2가지 이상 기술하시오. (6점)

제 2 문. RSA 공개키 암호와 해쉬함수 $H()$ 를 이용하여 전자서명을 설계한다고 하자. RSA에서는 두 소수 p, q 로부터 $n = pq$ 를 계산한 후 서명검증용 공개정보 (n, e) 와 서명용 비밀정보 d 를 생성한다. 다음 물음에 답하시오. (총 20점)

- 1) 해쉬함수를 이용한 메시지 M 의 서명 생성과정과 검증과정을 각각 기술하시오. (4점)
- 2) 위의 전자서명 방식에서 $p = 53, q = 59, e = 7$ 일 때 d 를 구하고 그 계산 과정을 기술하시오. (7점)
- 3) 암호학적 해쉬함수가 만족해야 하는 안전성 조건 3가지를 기술하고, 각각의 조건이 만족되지 않을 때 전자서명에서 발생하는 문제점을 설명하시오. (9점)

제 3 문. Alice의 공개키는 PK_A 이고 Bob의 공개키는 PK_B 이다. 다음은 공개키 암호를 이용하여 Alice와 Bob이 세션키 K_S 를 공유하는 프로토콜이다.

Alice	Bob
----- PK_A, ID_A ----->	
<----- $E(PK_A, K_S)$ -----	

위 프로토콜에서 ID_A 는 Alice의 식별자이고 $E()$ 는 공개키 암호 알고리즘이다. $E(PK_A, K_S)$ 는 세션키 K_S 를 Alice의 공개키 PK_A 로 암호화(encryption)한 암호문을 나타낸다. 다음 물음에 답하시오. (총 15점)

- 1) 상기 프로토콜은 공개키 소유자를 확인할 수 있는 방법이 없기 때문에 중간자 공격(Man-In-The-Middle Attack)이 가능하다. 상기 프로토콜에 대한 중간자 공격을 보이시오. (5점)
- 2) 상기 프로토콜에서 공개키 소유자를 확인할 수 있는 방법이 제공되었다고 가정하자. 즉, Alice와 Bob은 서로의 공개키를 안전하게 공유하였다고 가정하자. 이러한 환경에서 재전송 공격(Replay Attack)으로부터 안전하도록 공개키 암호를 이용한 세션키 분배 프로토콜을 설계하시오. (단, 암호 알고리즘으로는 주어진 공개키 암호 알고리즘 $E()$ 만 사용할 수 있으며, nonce를 이용한 도전-응답(Challenge-Response) 방식의 상호인증을 제공해야 한다) (10점)

인사혁신처 시험출제과장