

네트워크 보안

2020년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. Diffie-Hellman 키 교환 프로토콜에 대한 다음 물음에 답하시오. (총 20점)

- 1) 소수 p 와 p 의 원시근 g 가 주어져 있을 때, 사용자 A와 B가 공유 비밀키를 합의하는 과정을 설명하시오. (10점)
- 2) 1)에서 $p = 11$, $g = 2$ 이고, A가 5를, B가 7을 각각의 개인키로 선택한 경우에 공유 비밀키의 산출과정을 보이시오. (5점)
- 3) Diffie-Hellman 키 교환에서 중간자 공격(man-in-the-middle attack)이 발생하는 과정을 설명하고 이를 방지하기 위한 대응방안을 제시하시오. (5점)

제 2 문. IPsec ESP(Encapsulating Security Payload)를 이용하여 IPv4 패킷을 전송하는 경우의 IP 보안에 대한 다음 물음에 답하시오. (총 35점)

- 1) IPsec ESP에 의해 제공될 수 있는 보안 서비스를 나열하시오. (5점)
- 2) ESP 패킷의 기본 포맷을 도시하고, 각 필드의 역할을 설명하시오. (10점)
- 3) IP 헤더와 페이로드로 구성된 원래의 IPv4 패킷을 ESP 전송 모드와 ESP 터널 모드로 보낼 경우, 각 패킷의 구성과 암호화 및 인증의 범위를 설명하시오. (10점)
- 4) IPsec을 사용하는 두 호스트 간의 논리적 관계인 보안 연관(security association)과 이를 관리하는 방법을 설명하시오. (5점)
- 5) IPsec ESP 터널 모드를 이용하여 VPN 서비스를 제공하는 경우, 네트워크 구성 사례를 도시하고, 동작 과정을 설명하시오. (5점)

제 3 문. TLS(Transport Layer Security) 표준 프로토콜에 대한 다음 물음에 답하시오. (총 25점)

- 1) TLS에 포함되는 프로토콜의 구조와 목적을 설명하시오. (5점)
- 2) Handshake 프로토콜에서 단계별로 교환되는 메시지를 순서대로 나열하고 각 단계의 기능을 설명하시오. (10점)
- 3) Record 프로토콜의 송신측 처리 과정을 단계별로 설명하시오. (10점)

제 4 문. 네트워크 관리를 위한 SNMP(Simple Network Management Protocol)에 대한 다음 물음에 답하시오. (총 20점)

- 1) 네트워크 관리의 다섯 가지 영역을 나열하시오. (5점)
- 2) SNMP 동작 구조와 교환되는 메시지(PDU)의 유형 및 사용 목적을 설명하시오. (10점)
- 3) 네트워크 관리를 위한 SMI(Structure of Management Information)와 MIB(Management Information Base)에 대해 설명하시오. (5점)

인사혁신처 시험출제과장