

정보보호론<선택>

2023년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 공개된 네트워크상에서 통신하고자 하는 호스트 간 키를 공유하는 방법에 대한 다음 물음에 답하시오. (총 15점)

- 1) Diffie-Hellman 키 교환 메커니즘을 그림으로 도식하여 설명하시오. (5점)
- 2) Diffie-Hellman 키 교환에 대한 중간자 공격(Man-in-the-Middle Attack)을 그림으로 도식하여 설명하시오. (5점)
- 3) Kerberos는 중간자 공격에 대응할 수 있다. Kerberos에서 키 분배 센터(Key Distribution Center)를 운영하기 위한 구성요소 및 요소별 역할에 대하여 설명하시오. (5점)

제 2 문. 위험 관리(Risk Management)란 위험을 평가하고 조직이 수용할 수 있는 수준까지 위험 부담을 줄이려는 조치를 강구하여 그러한 위험을 용인할 수 있는 수준으로 유지하는 것을 말한다. 위험 관리를 위한 분석 방법에 대한 다음 물음에 답하시오. (총 10점)

- 1) 정량적 위험 분석 방법을 두 가지 제시하고 각각에 대하여 설명하시오. (5점)
- 2) 정성적 위험 분석 방법을 두 가지 제시하고 각각에 대하여 설명하시오. (5점)

제 3 문. 접근 제어(Access Control)에 대한 다음 물음에 답하시오. (총 10점)

- 1) 강제적 접근 제어(Mandatory Access Control)와 임의적 접근 제어(Discretionary Access Control)를 권한설정의 주체 측면에서 설명하시오. (5점)
- 2) 강제적 접근 제어인 벨-라파둘라(Bell-LaPadula) 모델과 비바(Biba) 모델의 보안 정책에 대하여 각각 설명하시오. (5점)

제 4 문. 암호학적 해시 함수(Hash Function)에 대한 다음 물음에 답하시오. (총 15점)

- 1) 해시 함수의 안전성 개념인 일-방향성(One-wayness)과 충돌 저항성(Collision Resistance)에 대하여 설명하시오. (5점)
- 2) 1)에서 설명한 두 안전성 개념 사이의 관계를 설명하시오. (5점)
- 3) 생일 역설(Birthday Paradox)을 설명하고 이와 연관지어 해시 함수의 충돌 저항성을 정량적으로 평가하시오. (단, 해시 함수의 출력은 n비트이며 균일하게 분포한다고 가정한다) (5점)

인사혁신처 시험출제과장