

정보보호론

2016년 시행 5급 공채(기술) 제2차시험

응시번호 :

성명 :

제 1 문. 임의 길이의 메시지 m 을 전자 서명하기 위하여 암호학적으로 안전한 해쉬 함수 h 의 해쉬 값 $h(m)$ 을 구한 후, 이 값의 서명값을 계산하여 메시지에 첨부한다. 다음 물음에 답하시오. (총 13점)

- 1) 전자 서명의 생성 및 검증 과정을 설명하시오. (3점)
- 2) 암호학적으로 해쉬 함수가 가져야 하는 안전성 요구 조건 중 제2역상 저항성(Second Primage Resistance)의 개념을 설명하고, 제2역상 저항성을 갖추지 못한 해쉬 함수가 전자 서명에 결합되어 사용되었을 때 어떤 취약성을 갖는지 설명하시오. (5점)
- 3) 해쉬 함수에 대한 충돌 저항성(Collision Resistance)의 개념을 설명하고, 충돌 저항성을 갖고 있는 해쉬 함수는 제2역상 저항성을 갖고 있음을 증명하시오. (5점)

제 2 문. A 국가기관은 차년도 정보보호 대책의 우선순위 및 투자 금액을 분석 중이다. 아래 표는 A 국가기관 민원처리시스템의 위험도 자료로 위험 요인별 발생확률, 손실 규모, 연간 손실액을 나타내고 있다. 표를 참고하여 다음 물음에 답하시오. (총 12점)

위험 요인	발생확률	손실 규모 (단위 : 천원)	연간 손실액 (단위 : 천원)
전력 중단	30 %	5,000 ~ 2,000,000	
횡령	5 %	1,000 ~ 50,000	
사용자 오류	98 %	200 ~ 40,000	

- 1) A 국가기관이 분석 중인 위험도 평가의 목적 및 효과에 대하여 서술하시오. (5점)
- 2) A 국가기관의 위험 요인별 연간 손실액을 구하고, 위험 요인에 대한 정보 보호 대책 우선순위를 도출하시오. (7점)

제 3 문. SSH(Secure Shell)는 클라이언트가 네트워크 상의 다른 컴퓨터에 접속하거나 원격 시스템에서 명령을 실행하기 위해 사용되는 네트워크 암호 프로토콜이다. 다음 물음에 답하시오. (총 13점)

- 1) 서버가 SSH를 이용하여 클라이언트를 인증할 수 있는 방법을 두 가지 이상 기술하시오. (4점)
- 2) SSH 다운그레이드 중간자 공격(SSH Downgrade Man-In-The-Middle Attack)을 수행하는 과정을 설명하시오. (4점)
- 3) 2)에서 SSH 다운그레이드 중간자 공격이 가능한 이유를 설명하시오. (5점)

제 4 문. B 기업은 서류철로 관리하고 있던 고객 자료를 데이터베이스로 구축하고자 한다. 고객 자료 중 개인정보를 비롯한 중요 데이터의 비중이 크지는 않지만 민감한 정보이기 때문에 보안대책이 필요하다고 판단하였다. B 기업은 데이터 베이스 보안 솔루션이 필요하다는 결론을 내리고 DB접근제어·감사 솔루션과 DB암호화 솔루션 중 하나를 도입하고자 한다. 다음 물음에 답하시오. (총 12점)

- 1) DB접근제어·감사 솔루션 및 DB암호화 솔루션의 기능을 각각 설명하시오. (4점)
- 2) 각 솔루션 도입에 따른 장단점을 비교 설명하시오. (4점)
- 3) B 기업의 상황을 고려하여 두 솔루션 중 하나를 선택하고, 그 이유를 설명하시오. (4점)

인사혁신처 시험출제과장