

정보보호론

2015년 시행 5급(기술) 공채 제2차시험

응시번호 :

성명 :

제 1 문. 공개키 암호 시스템 중 RSA(Rivest, Shamir, Adleman) 암호 알고리즘에 대하여 다음 물음에 답하시오. (총 13점)

- 1) 공개키 (n, e) 및 개인키 (d)의 생성과정을 제시하시오. (7점)
- 2) 공개키를 이용하여 평문 메시지 M을 암호화하고, 암호문 C를 복원하는 복호화 과정에 대하여 설명하시오. (6점)

제 2 문. 우리나라는 국가·공공기관이 정보보호시스템을 도입할 때 안전성을 검증하는 인증제도를 운영하고 있다. A 국가기관은 웹 침입차단시스템과 파일 암호화 제품을 도입하고자 한다. 이에 대하여 다음 물음에 답하시오. (총 12점)

- 1) A 국가기관이 웹 침입차단시스템을 도입할 때 고려해야 하는 인증제도에 대하여 설명하시오. (6점)
- 2) A 국가기관이 암호 모듈이 내장된 파일 암호화 제품을 도입할 때 고려해야 하는 인증제도에 대하여 설명하시오. (6점)

제 3 문. SSL/TLS(Secure Socket Layer/Transport Layer Security)는 인터넷에서 데이터를 안전하게 전송하기 위해 만들어진 통신 규약 프로토콜이다. SSL/TLS는 응용계층(Application Layer)으로부터 생성된 데이터에 대한 보안과 압축 서비스를 제공하도록 설계되어 있으며, 응용계층으로부터 수신된 데이터는 압축, 서명 및 암호화되어 TCP와 같은 신뢰성 있는 전송계층(Transport Layer)으로 넘겨진다. 이에 대하여 다음 물음에 답하시오. (총 13점)

- 1) SSL/TLS에서 사용되는 핸드셰이크 프로토콜의 기능에 대하여 설명하시오. (5점)
- 2) SSL/TLS 레코드 계층에서의 데이터 처리과정에 대하여 설명하시오. (8점)

제 4 문. 침입탐지시스템(IDS: Intrusion Detection System)은 탐지분석 방법에 따라 오용 탐지(misuse detection)기반과 비정상 행위 탐지(anomaly detection)기반으로 나눌 수 있다. 이에 대하여 다음 물음에 답하시오. (총 12점)

- 1) 오용 탐지 기반 IDS와 비정상 행위 탐지 기반 IDS에 대하여 설명하시오. (6점)
- 2) 1)의 각 IDS의 장단점을 설명하시오. (4점)
- 3) IDS의 false negative와 false positive에 대하여 설명하시오. (2점)

인사혁신처 시험출제과장