

정보보호론

2019년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 2017년 대규모 사이버 공격을 발생시킨 워너크라이(WannaCry)에 대한 다음 물음에 답하시오. (총 10점)

- 1) 워너크라이의 공격 대상이 된 윈도우즈 운영체제의 통신 프로토콜을 설명하시오. (4점)
- 2) 워너크라이 감염에 따른 시스템 피해 증상을 설명하시오. (6점)

제 2 문. 국내에서 사용하는 공인인증서는 전자서명 알고리즘(Digital Signature Algorithm)을 포함하고 있으며 이를 통해 인터넷 뱅킹과 같은 전자 거래, 전자 문서 교환 서비스 등을 지원한다. 송신자가 서명 알고리즘(Signing Algorithm)을 통해 메시지에 서명하고, 해당 메시지와 서명이 수신자에게 전달된 후 수신자가 검증 알고리즘(Verifying Algorithm)을 통해 이에 대한 확실성을 점검한다. 이러한 전자서명이 유효하기 위한 조건을 기술하시오. (10점)

제 3 문. IPSec에 대한 다음 물음에 답하시오. (총 15점)

- 1) IPSec의 연결방식에 따른 2가지 모드(Mode)를 비교 설명하시오. (5점)
- 2) AH(Authentication Header)와 ESP(Encapsulation Security Payload)의 특징을 정보보호 요소와 연관하여 각각 설명하시오. (10점)

제 4 문. 무선랜 표준에 대한 다음 물음에 답하시오. (총 15점)

- 1) WEP(Wired Equivalent Privacy)의 취약점 2가지를 기술하시오. (8점)
- 2) WPA(Wi-Fi Protected Access)의 엔터프라이즈(Enterprise) 모드는 중앙 인증 서버가 필요하기 때문에 작은 규모의 회사나 사용자들에게는 적합하지 않다. 이를 보완하기 위해 WPA에서 지원하는 인증 모드는 무엇이며, 이 인증 모드가 해당 문제를 어떻게 해결하는지 설명하시오. (7점)

인사혁신처 시험출제과장