

정보보호 기술

2023년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. Diffie-Hellman 키 교환 알고리즘의 안전성은 이산대수를 계산하는 어려움에 기반을 둔다. 사용자 A와 B가 키 교환을 할 때, 다음 물음에 답하시오.

(총 14점)

- 1) 소수 p 가 7일 때 원시근을 구하는 과정과 원시근을 제시하시오. (4점)
- 2) 1)에서 구해진 원시근들 중에서 가장 작은 수를 선택하여, Diffie-Hellman 키 교환 과정을 통해 사용자 A와 B가 키를 교환하는 과정을 보이시오. 이때 사용자 A는 5, 사용자 B는 3을 난수로 선택한다. (6점)
- 3) Diffie-Hellman 키 교환은 중간자 공격에 대해 취약하다. 이 문제를 해결하기 위한 방법을 2가지 이상 제시하시오. (4점)

제 2 문. 접근제어에 대한 다음 물음에 답하시오.

(총 12점)

- 1) 접근제어의 실행 3단계를 제시하고 각각 설명하시오. (9점)
- 2) 접근제어의 유형 중 역할기반접근제어(Role-Based Access Control)에 대해 설명하시오. (3점)

제 3 문. 공개키 인증서의 표준인 X.509에 대한 다음 물음에 답하시오. (총 12점)

- 1) 인증서의 역할을 설명하시오. (4점)
- 2) 인증서 형식에 포함된 정보 5가지 이상을 제시하시오. (5점)
- 3) 메시지 송수신 과정에서 인증서가 기밀성, 인증, 무결성을 어떻게 제공하는지 각각 설명하시오. (3점)

제 4 문. 보안취약점 분석과 점검에 대한 다음 물음에 답하시오.

(총 12점)

- 1) 블랙박스 테스트(Black Box Test)와 화이트박스 테스트(White Box Test) 방식에 대하여 설명하고 각각의 장점과 단점을 기술하시오. (8점)
- 2) 보안취약점 점검 방법 중 포트 스캐닝(Port Scanning)을 통해 알아낼 수 있는 정보에 대하여 설명하시오. (4점)

인사혁신처 시험출제과장