

정보보호 기술

2021년도 국가공무원 5급[기술] 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 메시지 인증 코드(Message Authentication Code)와 전자 서명(Digital Signature)에 대한 다음 물음에 답하시오. (총 10점)

- 1) 메시지 인증 코드에 대한 재전송 공격을 방지하기 위한 방법 중 두 가지를 설명하시오. (4점)
- 2) 메시지 인증 코드로 해결할 수 없는 부인 방지 문제는 전자 서명으로 해결할 수 있다. 그 이유를 설명하시오. (2점)
- 3) 전자 서명 방법 중 메시지에 서명하는 방법은 이해하기 쉽지만 실제로는 사용되지 않는다. 반면에 메시지의 해시 값에 서명하는 방법은 실제로 사용되고 있다. 메시지에 서명하는 방법의 단점과 메시지의 해시 값에 서명하는 방법의 장점을 설명하시오. (4점)

제 2 문. 타원 곡선 암호시스템(Elliptic Curve Cryptosystem)에 대한 다음 물음에 답하시오. (총 13점)

- 1) RSA 알고리즘에 비하여, 타원 곡선 암호시스템이 갖는 장점을 설명하시오. (3점)
- 2) Z_7 에서의 타원 곡선 $E_7(1,6)$ 의 방정식은 $y^2 = x^3 + x + 6$ 이고 모듈러 7을 방정식 계산에 이용한다. 무한점 O 를 제외한 타원 곡선 $E_7(1,6)$ 의 모든 점들을 보이시오. (7점)
- 3) $P = (3,1)$ 에 대하여, $-P$ 를 구하시오. (3점)

제 3 문. AES 암호 알고리즘의 라운드에서 “바이트 치환(Substitute Bytes)”, “행 이동(Shift Rows)”, “열 혼합(Mix Columns)”, “더하기 라운드 키(Add Round Key)” 변환이 사용된다. 16바이트(bytes)의 키 길이를 사용하는 AES-128의 암호화 과정에 대한 다음 물음에 답하시오. (단, $(k)_{16}$ 에서 k 는 16진수를 의미한다) (총 15점)

- 1) 암호화 과정의 마지막 10번째 라운드에서 수행되는 변환을 순서대로 나열하시오. (3점)
- 2) “열 혼합(Mix Columns)” 변환에서 사용되는 $GF(2^8)$ 의 덧셈 방법을 설명하고, $GF(2^8)$ 의 원소 $(2A)_{16}$ 와 $(74)_{16}$ 의 덧셈 과정을 보이시오. (4점)
- 3) “열 혼합(Mix Columns)” 변환에서 사용되는 $GF(2^8)$ 의 곱셈 방법을 설명하고, $GF(2^8)$ 의 원소 $(0C)_{16}$ 와 $(82)_{16}$ 의 곱셈 과정을 보이시오. (단, $GF(2^8)$ 의 곱셈에 사용되는 기약 다항식은 $x^8 + x^4 + x^3 + x + 1$ 이다) (8점)

제 4 문. 사용자 인증 방법에 대한 다음 물음에 답하시오. (총 12점)

- 1) Two Factor 인증에 대하여 설명하시오. (2점)
- 2) 생체인증 기술의 정확도를 측정할 수 있는 항목을 기술하시오. (4점)
- 3) 신체적 특징을 이용한 생체인증 기술 세 가지를 제시하고 각각의 장점과 단점을 기술하시오. (6점)

인사혁신처 시험출제과장