

## 정보보호기술

### 2018년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. Diffie-Hellman 키 합의 프로토콜을 사용하여 Alice와 Bob이 세션키를 공유하려고 한다. 사용되는 소수를  $p$ , 생성자(generator)를  $g$ , Alice의 비밀 값을  $x$ , Bob의 비밀 값을  $y$ , 생성한 공유 세션키를  $K$ 라고 할 때, 다음 물음에 답하시오. (총 10점)

- 1) Alice와 Bob이 공유 세션키를 생성하는 과정을 수식을 이용하여 설명하시오. (5점)
- 2) 기본적인 Diffie-Hellman 키 합의 프로토콜은 중간자 공격(man-in-the-middle attack)에 취약하다. 중간자 공격 과정을 설명하시오. (5점)

제 2 문. 정보보호서비스 중에서 기밀성, 무결성, 인증, 부인방지에 대한 다음 물음에 답하시오. (총 15점)

- 1) 각 서비스에 대하여 설명하시오. (5점)
- 2) 메시지인증코드(MAC, Message Authentication Code)가 인증 서비스를 지원하는 방식을 설명하시오. (5점)
- 3) 메시지인증코드가 부인방지 서비스를 제공하지 않는 이유를 기술하시오. (5점)

제 3 문. 100개의 블록(block)으로 구성된 평문을 블록암호 운영모드인 CBC(Cipher Block Chaining), CFB(Cipher Feedback)를 사용하여 암호화하려고 한다. 다음 물음에 답하시오. (총 10점)

- 1) CBC 모드로 암호화하여 전송하는 도중에 20번째 암호문 블록에 한 비트 오류가 발생하였다. 이 경우 원래대로 복호화되지 않는 평문 블록을 구하고, 오류가 파급되는 과정을 설명하시오. (5점)
- 2) CFB 모드를 사용하여 암호화하는 과정 중에 20번째 평문 블록에 입력 오류가 발생하였다. 이 경우 영향을 받는 암호문 블록을 구하고, 오류가 파급되는 과정을 설명하시오. (단, CFB의 블록 크기는 암호알고리즘의 블록 크기와 같다고 가정한다) (5점)

제 4 문. 다음은 ECDSA(Elliptic Curve Digital Signature Algorithm)의 키 생성, 서명 생성 및 검증 과정이다. 물음에 답하시오. (총 15점)

<p><b>&lt;시스템 파라미터&gt;</b>  <math>E</math>: 타원곡선  <math>P</math>: <math>E</math>상의 기저 점(base point)  <math>n</math>: <math>P</math>의 위수(order)  <math>H</math>: 암호학적 해시함수</p>	
<p><b>&lt;키생성&gt;</b>  1) <math>1 &lt; d &lt; n</math>를 만족시키는 정수 <math>d</math>를 랜덤하게 선택한다.  2) <math>Q = dP</math>를 계산한다.  3) 개인키 = <math>d</math>, 공개키 = <math>Q</math></p>	
<p><b>&lt;서명 생성 알고리즘&gt;</b>  입력: 메시지 <math>m</math>  출력: <math>m</math>에 대한 서명 <math>(r, s)</math>  1) <math>1 &lt; k &lt; n</math>을 만족시키는 정수 <math>k</math>를 랜덤하게 선택한다.  2) <math>kP = (x, y)</math>, <math>r = x \bmod n</math>을 계산한 후 만약 <math>r = 0</math>이면 단계 1)에서 다시 시작한다.  3) <math>h = H(m)</math>을 계산한다.  4) <math>s = k^{-1}(h + dr) \bmod n</math>을 계산한 후 만약 <math>s = 0</math>이면 단계 1)에서 다시 시작한다.  5) <math>(r, s)</math>를 출력한다.</p>	<p><b>&lt;서명 검증 알고리즘&gt;</b>  입력: 메시지 <math>m</math>과 서명 <math>(r, s)</math>  출력: '검증 성공' 또는 '검증 실패'  1) <math>r, s</math>가  <math>0 &lt; r &lt; n, 0 &lt; s &lt; n</math>을 만족하지 못하면 '검증 실패'를 출력한다.  2) <math>h = H(m)</math>을 계산한다.  3) <math>u_1 = s^{-1}h \bmod n</math>,  <math>u_2 = s^{-1}r \bmod n</math>을 계산한다.  4) <math>X = u_1P + u_2Q</math>를 계산한 후 <math>X = O(\text{point at infinity})</math>이면 '검증 실패'를 출력한다.  5) <math>X = (x, y)</math>에 대하여  <math>v = x \bmod n</math>을 계산한다.  6) 만약 <math>v = r</math>이면 '검증 성공'을, 그렇지 않으면 '검증 실패'를 출력한다.</p>

- 1) 서명 생성 알고리즘에서  $k$ 가 알려지면 개인키  $d$ 가 노출될 수 있음을 설명하시오. (5점)
- 2) 서명 생성 알고리즘을 통해 생성된 메시지  $m$ 의 서명  $(r, s)$ 가 서명 검증 알고리즘의 단계 6)에서 '검증 성공'을 출력함을 보이시오. (단,  $(r, s)$ 가 서명 검증 알고리즘의 단계 1)에서 단계 4)까지는 모두 통과했다고 가정한다) (10점)

## 인사혁신처 시험출제과장