

정보보호 기술

2020년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 공개키 암호화는 다양한 응용 분야에서 보안성을 제공하기 위하여 사용된다.
다음 물음에 답하시오. (총 8점)

- 1) 평문에서 암호문으로, 암호문에서 평문으로 변환하는 공개키 암호복호화 과정을 도식화하고 설명하시오. (4점)
- 2) 비밀키 암호화 방식과 비교하여 공개키 암호화 방식의 장점과 단점을 설명하시오. (4점)

제 2 문. 싱글사인온(SSO) 구현에 사용 가능한 Kerberos 시스템의 프로토콜은 아래와 같다.
다음 물음에 답하시오. (총 15점)

- | | |
|------------------------|---|
| ① $C \rightarrow AS:$ | $ID_C \parallel ID_{tgs} \parallel TS_1$ |
| ② $AS \rightarrow C:$ | $E_{K_c}[K_{c,tgs} \parallel ID_{tgs} \parallel TS_2 \parallel L_2 \parallel Ticket_{tgs}]$ |
| ③ $C \rightarrow TGS:$ | $ID_V \parallel Ticket_{tgs} \parallel Authenticator_c$ |
| ④ $TGS \rightarrow C:$ | $E_{K_{c,tgs}}[K_{c,v} \parallel ID_V \parallel TS_4 \parallel Ticket_v]$ |
| ⑤ $C \rightarrow V:$ | $Ticket_v \parallel Authenticator_c$ |
| ⑥ $V \rightarrow C:$ | $E_{K_{c,v}}[TS_5 + 1]$ |

※ C는 클라이언트, AS는 인증 서버, TGS는 티켓발급 서버, V는 서비스제공 서버

- 1) $Ticket_{tgs}$ 의 구성요소와 역할을 설명하시오. (5점)
- 2) $Ticket_v$ 의 구성요소와 역할을 설명하시오. (5점)
- 3) ⑤에서 나타난 $Authenticator_c$ 의 구성요소와 역할을 설명하시오. (5점)

제 3 문. 블록 암호화 방식은 ECB(Electronic Code Book)와 같은 운영모드로 동작시킬 수 있다. 다음 물음에 답하시오. (총 15점)

- 1) 블록 암호화 방식의 운영모드 중에서 ① 암호화 및 복호화를 동일한 알고리즘으로 구현할 수 있고, ② 패딩을 사용할 필요가 없으며, ③ 하드웨어 및 소프트웨어 구현의 효율성이 높은 운영모드를 제시하고, 그 운영모드의 암호화 및 복호화 과정을 도식화하고 설명하시오. (7점)
- 2) 운영모드를 활용하면 MAC(Message Authentication Code)을 생성시킬 수 있는데, 예를 들어, 데이터 인증 알고리즘(DAA: Data Authentication Algorithm)은 DES 암호화 방식을 기반으로 하여 CBC 운영모드를 적용한다. DAA에서의 MAC(DAC: Data Authentication Code)이 생성되는 과정을 도식화하고 설명하시오. (8점)

제 4 문. 하이브리드 암호화 방식은 대칭키 암호화 방식과 공개키 암호화 방식의 장점을 조합한 방식을 의미하며, SSL(Secure Socket Layer), PGP(Pretty Good Privacy) 등과 같은 암호화 응용 분야에서 사용되고 있다. 다음 물음에 답하시오. (총 12점)

- 1) 응용 분야의 사용자가 대폭 증가한다고 가정할 경우, 대칭키 암호화 방식의 단점을 공개키 암호화 방식에서 어떻게 해결하는지 키 관리적인 관점에서 설명하시오. (6점)
- 2) Alice가 Bob에게 대용량 메시지 M을 하이브리드 암호화 방식을 이용하여 전송하는 과정을 설명하시오. (단, Bob의 공개키는 K_{pub} , Bob의 개인키는 K_{pri} , 대칭키 암호화 방식은 128비트 AES, 공개키 암호화 방식은 RSA를 사용한다) (6점)

인사혁신처 시험출제과장