전자서명

1. 전자서명이 제공하는 보안 4가지를 말하고 설명하세요
2. MAC과 전자서명의 공통점과 차이점 서술
3. 이론적(Textbook) RSA 전자서명의 단점 두가지를 말하고 해결방안을 예시와 함께 서술하세요
   (각 단점을 어떻게 해결했는지..)
4. 공개키 기반 구조 (PKI)에서 Alice가 Bob을 인증하는 과정을 최대한 자세하게 서술하세요
   (Bob의 인증서 발급 절차, Alice가 Bob에게 요청했을 때 과정...)
5. Alice가 은행에 거래를 요청하려 할 때, 인증서를 사용하는 과정

개체인증

1. Message Authentication과 Entity Authentication의 특징 및 예시를 들어 설명
2. 패스워드 기반 인증에서, 패스워드를 해시할 때 salt를 사용하는 이유와 이로 인해 얻을 수 있는 효과
3. Challenge-Response 방식에서 Challenge에 Freshness가 필요한 이유와 Freshness의 종류

키관리 시스템

1. KDC 기반 공유 방법에 대해 서술하고, 해당 방법의 장/단점
   (단점 - 구조상 발생할 수 있는 공격.. 등)
2. 디피-헬만 동의 프로토콜의 방법에 대해 말하고 안전한 이유 서술
3. 디피-헬만 동의 프로토콜의 한계 및 해결방안

네트워크 보안 기초 1

1. Link Encryption, End-to-End Encryption을 예시를 들어 설명
2. SSL/TLS 프로토콜은 무슨 목적으로 사용되며, 어떠한 방식으로 사용하는지
   (방식 - Layer사이에서.. HTTP 위에... 이런느낌)
3. TLS HandShake 과정에 대해 설명
   (어떤 정보를 주고받는지, 그 정보를 어떻게/어떤 곳에 사용하는지.. 등)
4. 최종적으로 TLS는 Application data의 무엇을 보장해주는지 과정과 함께 설명

네트워크 보안 기초 2

1. WEP가 취약한 이유
2. WPA1 (TKIP), WPA2 (CCMP)의 차이점과 각 특징 한가지씩
3. Enterprise / Personal Mode의 차이점과 각 특징 한가지씩

네트워크 보안 3

1. IPSec를 사용하는 이유를 데이터 보호 / 헤더 보호 측면에서 서술
2. Transport / Tunnel 지원 모드의 작동 방식과 각 모드의 특징 서술
3. AH / ESP 보안 프로토콜의 차이점 두가지
4. IPSec의 4가지 방법 중 가장 효과적이라고 생각한 것을 고르고 그렇게 생각한 이유를 서술
5. TLS와 IPSec를 비교했을 때, 차이점 두가지 서술