科目名 : **정보보호개론**	학부	컴퓨터공학부			학년	
2021學年度 1學期 중간試驗	학번		성명			

1. (15점) 프라이버시를 논할 때, 프라이버시를 크게 강한 프라이버시와 약한 프라이버시를 나눌 수 있는데, 그것을 나누는 기준을 구체적으로 설명하고, 조건부 프라이버시라는 것은 무엇인지 설명하시오.

2. (15점) 인증서를 사용한다는 표현은 정확한 표현이 아니다. 예를들어 어떤 기사에 "인터넷 뱅킹을 할 때 인증서를 사용하기 위해 사용자는 먼저 패스워드를 입력해야 한다"고 서술되어 있다면 이것은 정확한 표현이 아니다. 은행에 최초 접속할 때 인증서를 이용하여 계좌의 소유주를 인증한다면 어떤 절차가 인증서와 관련하여 진행되는지 구체적으로 기술하시오.

3. (10점) 탈중앙 PKI인 DPKI에서는 신뢰하는 인증기관이 발급하는 인증서를 통해 공개키를 인증하는 것이 아니라 각 개인이 스스로 만든 인증서와 같은 문서를 블록체인에 저장하는 방식을 사용한다. 이 방식에서는 블록체인에 문서 저장을 제한할 수 있어야 공개키 인증 역할을 할 수 있다. 그 이유를 설명하시오. 참고로 블록체인은 첨삭 전용이기 때문에 블록체인에 저장되어 있는 데이터를 수정하거나 삭제할 수 없다.

4. (10점) 보통 전자서명 알고리즘은 공개키 암호알고리즘에서 개인키를 이용하여 메시지를 암호화하는 방식으로 구성된다. 하지만 메시지 자체를 암호화하기보다는 메시지의 해시값을 암호화하는 방식을 사용한다. 메시지 자체보다는 메시지 해시값을 암호화하는 이유를 설명하고, 이때 사용하는 해시함수는 반드시 충돌회피 해시함수이어야 하는 이유를 설명하시오.

5. (40점) 128bit 블록 방식의 대칭 암호알고리즘 사용한다고 가정하고, 사용하는 프로토콜의 일부가 다음과 같다고 가정하자.

   1. $A \rightarrow S: \quad A, B, N_A$
   2. $S \rightarrow A: \quad \{N_A||B||K_{AB}\}.K_{AS}, \ldots$

   여기서 K_{AS}는 S와 A 간 공유하고 있는 128bit 크기의 장기간 대칭키이고, 난스, 식별자, K_{AB}의 길이는 각각 64bit, 128bit, 128bit라 하자. 이와 관련하여 다음에 대해 답하시오.

   ① (10점) $\{N_A||B||K_{AB}\}.K_{AS}$를 표준 채우기를 이용하여 CBC 모드로 암호화하였을 때, 암호문은 블록 수와 블록 수가 그렇게 된 이유를 구체적으로 설명하시오.

   ② (10점) N_A와 B는 모두 명백한 여분 정보이다. Alice는 이 암호문을 복호화하여 둘 다 기대하는 값임을 확인하였고, 채우기도 문제가 없음을 확인하였다. 이 경우 K_{AB}의 무결성을 확인할 수 있는지 여부를 설명하시오.

   ③ (10점) 만약 식별자의 길이가 128bit가 아니라 192bit라 가정하고. K_{AB}의 무결성을 확인할 수 있는지 여부를 설명하시오.

   ④ (5점) 식별자의 길이가 128bit가 아니라 192bit일 때, CBC가 아니라 CTR 모드로 암호화하였을 경우 K_{AB}의 무결성을 확인할 수 있는지 여부를 설명하시오.

   ⑤ (5점) 식별자의 길이가 128bit가 아니라 192bit일 때, CTR 모드와 MAC 함수를 이용하여 encrypt-then-mac 방법으로 인증 암호화하였을 경우 K_{AB}의 무결성을 확인할 수 있는지 여부를 설명하시오.

6. (25점) Otway-Rees 프로토콜에 대한 타입 공격은 1, 2번 메시지에 포함된 $\{N_A||N||A||B\}.K_{AS}$와 3, 4번 메시지에 포함된 $\{N_A||K_{AB}\}.K_{AS}$의 길이가 같을 경우 Bob이 Alice에게 4번 메시지를 보낼 때 공격자가 1번에 있는 암호문으로 교체하여 $N||A||B$를 K_{AB}로 사용하도록 하는 공격이다. 난스는 64bit, N은 32bit, 식별자는 128bit, 키는 128bit라 하고, 128bit 블록 암호화를 이용하여 암호화한다고 가정하고, 다음에 대해 각각 답하시오.

   ① (5점) 표준 채우기 ECB 모드로 암호화할 경우 $\{N_A||N||A||B\}.K_{AS}$와 $\{N_A||K_{AB}\}.K_{AS}$의 암호 블록 수와 블록 수가 그렇게 된 이유를 구체적으로 설명하시오.

   ② (10점) 공격자가 $\{N_A||K_{AB}\}.K_{AS}$와 동일한 길이가 되도록 $\{N_A||N||A||B\}.K_{AS}$의 일부를 $\{N_A||K_{AB}\}.K_{AS}$와 교체하면 타입 공격에 성공할 수 있는지 설명하시오.

   ③ (10점) CTR 모드로 암호화할 경우 이전 문제처럼 동일한 크기가 되도록 $\{N_A||N||A||B\}.K_{AS}$의 일부를 $\{N_A||K_{AB}\}.K_{AS}$와 교체하면 타입 공격에 성공할 수 있는지 설명하시오.

7. (40점) 기본 Diffie-Hellman 키 동의 프로토콜은 이산대수 문제가 계산적으로 해결하기 어려운 순환군 G에서 생성자 g가 주어졌을 때, 다음과 같이 진행된다. 여기서 A와 B는 각각 a와 b를 G의 크기 범위 내에서 임의로 선택하여 프로토콜을 진행한다.

$$\begin{array}{ll} \text{Msg 1.} & A \to B: \quad g^a \\ \text{Msg 2.} & B \to A: \quad g^b \end{array}$$

이와 관련하여 다음 각각에 대해 답변하시오.

① (10점) 기본 DH 키 동의 프로토콜은 중간자 공격에 취약하다. 이 프로토콜에 대한 중간자 공격을 자세히 설명하시오.

② (10점) 중간자 공격을 방어하기 위한 MTI 프로토콜은 매 번 새롭게 생성하는 g^a, g^b만 사용하여 세션키를 계산하지 않고, 장기간 키를 사용한다. x_A, x_B가 A와 B의 장기간 개인키이고, $y_A = g^{x_A}$, $y_B = g^{x_B}$가 대응되는 공개키일 때, A는 $S_{AB} = (y_B)^a (g^b)^{x_A}$를 이용하여 계산한다. 하지만 이 방법은 완벽한 전방향 안전성을 보장하지 못하는 문제점이 있다. 완벽한 전방향 안전성이 무엇인지 설명하고, 왜 보장되지 않는지 설명하시오.

③ (20점) 주어진 기본 DH 키 동의 프로토콜이 중간자 공격에 강건하도록 전자서명을 이용하여 개선한 프로토콜을 제시하시오. 이때 최근성을 포함한 강한 개체 인증을 제공해야 하며, 키 확인 요소가 포함되어야 한다.