科目名 : **정보보호개론**	학부	컴퓨터공학부			학년	
2022學年度 1學期 중간試驗	학번		성명			

1. (25점) 원격에 있는 두 사용자가 동전 던지기를 하기 위해 다음과 같은 프로토콜을 사용할 수 있다.

   - 단계 1. Alice는 매우 큰 양의 정수 X를 임의로 선택하여 그것의 해시값 $H(X)$를 Bob에게 전달한다.
   - 단계 2. Bob은 짝수, 홀수 중 하나를 선택하여 Alice에게 자신의 선택을 알린다.
   - 단계 3. Alice는 X를 Bob에게 전달한다. Bob의 추측이 맞으면 Bob이 이긴 것이 된다.

   이 프로토콜과 관련하여 다음 각각에 대해 답하시오.

   ① (5점) 선택 가능한 X의 범위가 이 프로토콜의 안전성에 어떤 영향을 주는지 설명하시오.

   ② (5점) Bob이 무엇을 할 수 있으면 항상 이길 수 있는지 제시하고, 해시함수의 어떤 특성 때문에 그것이 가능하지 않은지 제시하시오.

   ③ (5점) Alice가 무엇을 할 수 있으면 항상 이길 수 있는지 제시하고, 해시함수의 어떤 특성 때문에 그것이 가능하지 않은지 제시하시오.

   위 프로토콜을 블록방식의 대칭 암호알고리즘을 사용하여 다음과 같이 변경하였다.

   - 단계 1. Alice는 블록 크기의 랜덤한 값 X와 대칭키 K를 임의로 선택하여 X를 K로 채우기 없이 ECB 모드로 암호화한 암호문을 Bob에게 전달한다.
   - 단계 2. Bob은 짝수, 홀수 중 하나를 선택하여 Alice에게 자신의 선택을 알려준다.
   - 단계 3. Alice는 K를 Bob에게 전달한다.

   ④ (10점) 이 프로토콜에서 Alice가 무엇을 할 수 있으면 항상 이길 수 있는지 제시하고, 이 측면에서 이 프로토콜의 안정성을 논하시오.

2. (10점) 비밀성 보장을 위해 사용하는 암호화 함수는 확률적 알고리즘이어야 바람직하다. 암호화 함수가 확률적 알고리즘이라는 것은 같은 평문을 같은 키로 암호화하여도 암호화할 때마다 다른 암호문을 주는 경우를 말한다. 이와 관련하여 다음 각각에 대해 답변하시오.

   ① (5점) 대칭 암호알고리즘에서 암호화 함수가 결정적 알고리즘일 경우 어떤 문제가 있는지 설명하시오.

   ② (5점) 비대칭 암호알고리즘의 암호화 함수는 대칭 방식보다 더욱더 확률적 알고리즘이 되는 것이 필요하다. 그 이유를 설명하시오.

3. (20점) 프로토콜에서 메시지 최근성을 보장하기 위해 8byte 크기의 난스(nonce)를 사용한다. 이 프로토콜은 프로토콜 수행마다 하나의 난스를 사용하며, 이 난스를 암호학적으로 안전한 난수 발생 알고리즘을 이용하여 생성한다. 이와 관련하여 다음 각각에 대해 답변하시오.

   ① (10점) 난스는 예측 불가능성보다는 이전에 사용하지 않은 값을 사용하는 것이 더 중요하다. 문제에서 설명한 것처럼 랜덤하게 난스를 생성하였을 때, 얼마만큼 많은 난스를 생성하여 사용해야 50%의 확률로 이전에 사용한 난스를 다시 사용할 수 있는지 제시하고, 이 수의 제시에 사용한 근거 이론을 설명하시오.

   ② (5점) ①과 같이 우연히 일치하는 것을 방지하기 위해 어떻게 해야 하는지 설명하시오.

   ③ (5점) 이 문제와 유사한 상황으로 ②에 제시된 해결책으로 방지할 수 있는 또 다른 경우를 제시하시오.

4. (20점) 서버는 각 사용자마다 카운터와 대칭키를 공유하고 있다. 예를 들어 서버는 Alice와 대칭키 K_{AS}와 카운터 C_{AS}를 공유하고 있다. 이들을 이용하여 대칭키만 사용하는 키 전송 방식의 키 확립 프로토콜을 제시하시오. 이 프로토콜은 4장 다섯번째 시도 프로토콜에서 메시지 최근성 보장 기법을 난스 대신에 카운터를 이용하도록 수정하면 된다. 제시한 프로토콜에는 키 확인 과정이 포함되어야 한다.

5. (45점) 난스는 8byte, 세션키는 16byte, 사용자 식별자는 16byte, 블록 크기는 16byte이며, $\{N_A||K_{AB}||B\}.K_{AS}$는 ECB 모드로 암호화한 암호문이다. 이 암호문을 수신하기 전에 A는 N_A를 S에게 평문으로 전달하였으며, 채우기는 표준 채우기를 사용한다고 가정한다. 이와 관련하여 다음 각각에 대해 답변하시오.

   ① (5점) 주어진 암호문의 블록 수를 제시하시오.

   ② (5점) 이 암호문에서 여분 정보 역할을 할 수 있는 것을 모두 제시하시오.

   ③ (10점) 과거에 사용한 동일 암호문 $\{N'_A||K'_{AB}||B\}.K_{AS}$가 있을 때, 공격자가 두 암호문을 이용하여 모든 여분 정보는 확인되지만, 키의 무결성은 깨지도록 공격할 수 있는지 설명하시오. 현재 A가 기대하는 난스는 N_A이다.

   ④ (20점) ③의 공격이 CBC와 CTR 모드로 메시지를 암호화하였을 때에도 여전히 가능한 공격인지 설명하시오.

   ⑤ (5점) CTR 모드로 메시지를 암호화할 경우 과거 암호문을 활용하지 않고 아주 간단한 방법으로 키의 무결성은 보장되지 않지만 모든 여분 정보는 확인이 가능하도록 공격할 수 있다. 그 방법을 설명하시오.

6. (20점) 같은 키로 암호화된 두 개의 암호문 $C = C_0||C_1||C_2||C_3$와 $C' = C'_0||C'_1||C'_2||C'_3$이 있을 때, 두 개를 조합하여 $C_0||C_1||C'_1||C'_2$를 만든 경우 그것을 복호화하면 올바르게 복호화되는 블록과 복호화하여 얻은 평문을 통해 복호화한 사용자가 알 수 있는 것을 CBC, CTR 모드로 나누어 비교 설명하시오. 여기서 C_0와 C'_0는 암호화할 때 사용한 IV이며, CBC는 표준 채우기를 사용한다.

7. (10점) 교재에 제시된 Otway-Rees 프로토콜은 메시지 1과 2에 포함된 $\{N_A||N||A||B\}.K_{AS}$와 메시지 3과 4에 포함된 $\{N_A||K_{AB}\}.K_{AS}$에서 K_{AB}와 $N||A||B$의 길이가 같을 경우 타입 공격이 가능하다. 이 프로토콜에서 N_A가 8byte, K_{AB}가 16byte, N는 8byte, 식별자는 20byte, 블록 크기는 16byte일 때, ECB 모드를 이용하여 메시지를 암호화한 경우 타입 공격이 여전히 가능한지 논하시오.

8. (30점) 기본 Diffie-Hellman 키 동의 프로토콜은 중간자 공격에 취약하다. 이 때문에 국제 표준에서는 다음과 같이 하도록 권고하고 있다.

$$\begin{array}{lll} \text{Msg 1.} & A \to B: & A, g^a \\ \text{Msg 2.} & B \to A: & B, g^b, \text{Sig}_B(g^a||g^b||A) \\ \text{Msg 3.} & A \to B: & \text{Sig}_A(g^b||g^a||B) \end{array}$$

   여기서 g는 이산대수 문제가 계산적으로 어려운 순환군 G의 생성자이며, a와 b는 G의 크기 범위 내에서 A와 B가 임의로 선택한 값이다. 이와 관련하여 다음 각각에 대해 답변하시오.

   ① (5점) 이 프로토콜은 왜 중간자 공격에 대해 강건한지 설명하시오.

   ② (5점) 메시지 2를 수신한 A는 주어진 서명의 최근성을 확인 가능한지 설명하시오.

   ③ (5점) 메시지 2를 수신한 A는 주어진 서명을 확인하기 위해서는 B의 인증서(certificate)가 필요하다. 인증서란 무엇인지 설명하시오. 인증서와 관련하여 인증기관의 역할을 설명하시오.

   ④ (5점) 이 프로토콜은 완벽한 전방향 안전성을 제공한다. 완벽한 전방향 안전성이 무엇인지 설명하시오.

   ⑤ (5점) 이 프로토콜은 강한 개체 인증을 제공한다. 강한 개체 인증이 무엇인지 설명하시오.