블록체인 HW 1: 보안지식 테스트

이름:
학번:

1. 컴퓨터 보안의 3 대 요소를 적어라.

2. Kerckhoff's Principe 이란?
   a. 공격자가 암호화 알고리즘과 암호키를 모른다고 가정한다
   b. 공격자가 암호화 알고리즘은 모르나 암호키는 알고 있다고 가정한다
   c. 공격자가 암호화 알고리즘은 알고 있으나 암호키는 모른다고 가정한다
   d. 공격자가 암호화 알고리즘과 암호키를 알고 있다고 가정한다.

3. 랜덤 넘버를 무작위로 선택할 때 같은 숫자가 나타날 확률이 적지 않은데 이러한 현상을 ( )라고 한다.

4. Block Cipher 의 Mode of Operation 은 ( )의 사이즈 보다 큰 메시지를 암호하 하는 방법을 말한다.

5. Cryptographic Hash 함수가 갖춰야 할 다섯가지 성질 중에서 weak collision resistance 와 strong collision resistance 를 설명하여라.

6. Sender 가 작성한 메시지가 중간에 수정되었는지 혹은 Attacker 가 임의로 작성한 메시지인지를 감지해 내기 위해서 메시지에 추가적으로 덧붙여서 보내는 정보를 ( ) 라고 하는데, 이정보는 보안의 목적 중 ( )를 보장해 준다.

7. -2 mod 5 는 이 숫자를 ( )와 더하면 ( ) mod 5 가 나오는 숫자이다. 따라서 -2 mod 5= ( ) 이다.

8. 3^{-1} mod 5 는 이 숫자를 ( )와 곱하면 ( ) mod 5 가 나오는 숫자이다. 따라서 3^{-1} mod 5 = ( ) 이다.

9. Certificate 는 사용자의 identity, ( ), 그리고 발행인의 signature 를 반드시 포함하고 있다.

10. Public Cryptography 에서 암호화는 ( )키를 사용하여야 하고 전자서명은 ( )키를 사용하여야 한다.

11. 전자서명은 암호화 및 해쉬기술로 해결할 수 없는 중요한 보안목적을 달성해 주는데 이것이 무엇인지 용어를 말하여라.

12. 해시값을 계산할 때 비밀키를 알아야 계산할 수 있는 표준화된 해시방법을 무엇이라고 하나? ( )