【정보보호론】

1. 정보보호의 속성에 대하여 <보기 1>의 설명과 <보기 2>의 용어를 가장 적절하게 연결한 것은?

<보기 1>

(가) 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다.
(나) 허락된 사용자 또는 객체가 정보에 접근하고자 할 때 방해받지 않도록 하는 것이다.
(다) 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다.
(라) 어떤 주체나 객체가 틀림없음을 보장하는 것이다.

<보기 2>

㉠ 무결성(Integrity) ㉡ 가용성(Availability)
㉢ 기밀성(Confidentiality) ㉣ 인증성(Authentication)

	(가)	(나)	(다)	(라)
①	㉣	㉡	㉢	㉠
②	㉡	㉠	㉣	㉢
③	㉠	㉡	㉢	㉣
④	㉢	㉣	㉠	㉡

2. 보안 공격(Security Attack)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 적극적 공격(Active Attack)은 무결성과 가용성을 위협하며 변경, 재전송, 서비스 거부 공격 등이 있다.
② 대부분의 적극적 공격은 상당 기간 동안의 수동적 공격 수행을 통해 수집된 정보를 바탕으로 수행된다.
③ 소극적 공격(Passive Attack)은 기밀성을 위협하며 스누핑(Snooping), 트래픽 분석 공격 등이 있다.
④ 소극적 공격은 시스템 작동에 치명적인 피해를 입히며 예방보다는 탐지가 중요하다.

3. 스테가노그래피(Steganography)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 비밀정보를 매체에 은닉하여 그 정보의 존재 자체를 숨기는 보안 기술이다.
② 메시지 정보를 은닉하며 트래킹이 불가능하다.
③ 비밀키를 이용하여 제3자가 메시지 내용을 알 수 없도록 변경하는 기술이다.
④ 정보가 제3자로부터 불법적으로 사용 및 변조되는 것을 방어하는 기술이다.

4. 종단 간 암호화(End-to-End Encryption)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 헤더를 포함한 모든 데이터를 암호화한다.
② 알고리즘에 대한 통제는 사용자가 한다.
③ 사용자 인증 등 보안 서비스 제공이 가능하다.
④ 중간 노드에서도 데이터가 암호문으로 존재한다.

5. 보안모델에 대한 설명으로 가장 적절하지 **않은** 것은?

① 만리장성(Chinese Wall) 모델은 주체와 객체 사이에서 이해충돌을 야기하는 방식으로 정보가 전달되지 않도록 한다.
② 벨-라파듈라(Bell-LaPadula) 모델은 보안단계가 높은 정보가 보안단계가 낮은 사용자에게 전달되는 것을 방지하는 기밀성 유지의 특성을 가진다.
③ 비바(Biba) 모델은 벨-라파듈라 모델의 단점을 보완한 모델로 무결성을 보장할 수 있다.
④ 클락-윌슨(Clark-Wilson) 모델은 무결성 보장을 못하지만 모든 보안모델에 기본적으로 사용된다.

6. 다음에서 설명하는 대칭키 암호 알고리즘의 유형으로 가장 적절한 것은?

·선정 기준은 안전성, 비용, 구현 효율성이며 Rijndael이 최종 선정되었다.
·암호화 과정의 각 라운드는 [바이트치환(Substitute Bytes)] → [행이동(Shift Rows)] → [열혼합(Mix Columns)] → [라운드키더하기(Add Round Key)] 단계의 변환을 적용한다.
·마지막 라운드는 [열혼합(Mix Columns)] 단계를 제외한 3개의 변환을 적용한다.

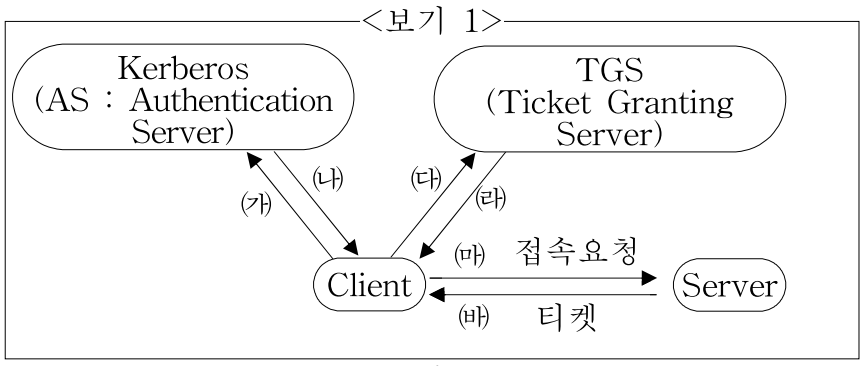
① AES(Advanced Encryption Standard)
② Blowfish
③ ARIA(Academy Research Institute Agency)
④ DES(Data Encryption Standard)

7. 블록 암호의 운영 모드인 CBC(Cipher Block Chaining)에 대한 설명으로 가장 적절한 것은?

① 각각의 평문 블록은 암호화되기 전에 이전 암호문 블록과 AND 연산한다.
② 전송 도중 암호문 블록 C_j에서 한 비트 오류가 발생하면 평문 블록 P_j에서 한 비트에서만 오류가 발생된다.
③ 초기벡터가 필요하며 암호화에서는 병렬처리를 할 수 없다.
④ 내부적으로 1씩 증가하는 카운터(Counter)가 필요하다.

8. 다음은 커버로스(Kerberos)에 대한 인증 절차를 나타낸 것이다. <보기 1>의 (가)~(라)와 <보기 2>의 용어를 가장 적절하게 연결한 것은?

<보기 1>



<보기 2>

㉠ 패스워드 ㉡ 인증값 ㉢ 티켓

	(가)	(나)	(다)	(라)
①	㉠	㉡	㉡	㉢
②	㉡	㉠	㉢	㉡
③	㉠	㉢	㉢	㉡
④	㉡	㉠	㉠	㉢

9. 인증기관(Certification Authority)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 공개키 인증서를 발행하고 필요에 따라 취소한다.
② 사용자의 개인키를 포함한 인증정보를 인증기관의 개인키로 서명한다.
③ 인증서 위조를 방지하기 위해서 인증기관의 공개키는 반드시 신뢰할 수 있어야 한다.
④ 인증서 폐지목록(Certificate Revocation List) 등을 관리한다.

10. 메시지 인증코드(Message Authentication Code)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 메시지 인증 방식에는 메시지 암호화 방식, 해시함수를 이용하는 방식 등이 있다.
② 임의 길이의 메시지와 송·수신자가 공유하는 비밀키를 입력하여 가변비트 길이의 출력을 계산하는 함수이다.
③ IPSec과 SSL/TLS는 통신 내용의 인증과 무결성을 확인하기 위해 메시지 인증코드로 사용한다.
④ 송·수신자가 같은 키를 갖고 있으므로 제3자에 대한 증명을 할 수 없으며 부인방지(non-repudiation)를 할 수 없다.

11. 임의적 접근제어(Discretionary Access Control)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 중앙 집중화된 환경에서 제어되는 것이 아니며 강제적 접근제어(Mandatory Access Control)의 정적인 역할에 비해 사용자에게 동적으로 정보에 접근할 수 있도록 해준다.

② 접근 권한 관리가 매우 편리하여 DBMS 및 운영체제의 파일 시스템 등에 널리 사용된다.

③ 접근 권한 부여를 오직 식별자에게만 의존하므로 데이터의 의미(Semantics)에 대해 아무런 지식도 갖고 있지 않아 데이터에 의한 통제를 할 수 있는 방법이 전혀 없다.

④ 모든 접근 데이터에 대해 보안 레이블을 정의하고 보안정책을 확인해야 하므로 성능이 좋지 않고 개발 및 구현이 쉽지 않다.

12. 다음에서 설명하는 내용으로 가장 적절한 것은?

·암호 알고리즘은 모든 내용이 공개되어도 키가 노출되지 않으면 안전해야 한다. ·암호시스템의 안전성은 암호 알고리즘의 비밀을 지키는데 의존되어서는 안되며 키의 비밀을 지키는데 기반을 두어야 한다.

① 비둘기집(Pigeon Hole)의 원리

② 오일러(Euler)의 정리

③ 페르마(Fermat)의 정리

④ 케르히호프(Kerckhoff)의 원리

13. IPSec Protocol에 대한 설명으로 가장 적절하지 **않은** 것은?

① ESP(Encapsulating Security Payload)는 IP 데이터그램에서 제공하는 선택적 인증과 무결성, 기밀성, 재전송 공격 방지 기능이 있다.

② AH(Authentication Header)는 인증서비스, 재전송 공격 방지 서비스를 제공하며 기밀성을 보장한다.

③ Tunnel Mode는 IP 헤더를 포함한 전체에 대해서 보호 서비스를 제공하며 여러 호스트에 대해서 같은 터널을 사용할 수 있다.

④ Transport Mode는 종단 간 서비스를 제공하며 트래픽 분석에 취약할 수 있다.

14. 사이버 공격유형에 대한 <보기 1>의 설명과 <보기 2>의 용어를 가장 적절하게 연결한 것은?

<보기 1>

(가) 사용자에게 실제 사이트와 동일한 경험을 제공하면서 ID나 비밀번호 등 중요 정보를 중간에 탈취하는 공격

(나) 특정인(조직)을 표적으로 신뢰할만한 발신인이 보낸 것처럼 위장한 메일을 이용하여 악성 웹 사이트 유도, 악성 첨부파일로 악성코드를 감염시키는 방식

(다) 해당 사이트가 공식적으로 운영하고 있는 도메인 자체를 탈취하는 공격

(라) 스마트폰에 첨부된 URL을 실행하면 악성 앱이 설치되어 개인정보나 금융정보를 탈취하는 방식

<보기 2>

㉠ 액티브 피싱(Active Phishing) ㉡ 파밍(Pharming)
㉢ 스피어 피싱(Spear Phishing) ㉣ 스미싱(Smishing)

	(가)	(나)	(다)	(라)
①	㉠	㉢	㉡	㉣
②	㉣	㉠	㉢	㉡
③	㉢	㉡	㉠	㉣
④	㉠	㉢	㉣	㉡

15. 영지식 인증(Zero Knowledge Authentication)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 증명하려는 자는 자신의 비밀정보를 노출하지 않으면서 자신이 비밀정보를 알고 있음을 증명할 수 있다.

② Fiat-Shamir 프로토콜, Feige-Fiat-Shamir 프로토콜 등이 있다.

③ 정당성(Soundness), 완전성(Completeness), 영지식성(Zero Knowledgeness)을 만족해야 한다.

④ 모든 프로토콜에 대해 반복 수행 없이 정당성을 높일 수 있다.

16. SSL(Secure Socket Layer)에 대한 설명으로 가장 적절하지 **않은** 것은?

① SSL 보안 서비스는 클라이언트와 서버 상호 인증, 메시지 무결성 등이 있다.

② Handshake 프로토콜은 [보안설정] → [클라이언트 인증과 키교환] → [서버 인증과 키교환] → [종료] 단계로 진행된다.

③ Alert 프로토콜은 통신 과정에서 발생하는 오류를 통보하기 위해 사용한다.

④ Record 프로토콜은 단편/결합, 암호화/복호화, 압축/압축풀기 등의 기능을 제공한다.

17. 모바일 운영체제에 대한 설명으로 가장 적절하지 **않은** 것은?

① iOS는 프로그램 실행 권한이 관리자(root)에게 있고 안드로이드는 일반 사용자에게 있다.

② iOS는 보안통제권이 애플에 있고 안드로이드는 개발자 또는 사용자에게 있다.

③ iOS와 안드로이드의 각 응용프로그램은 개발자가 서명하여 배포한다.

④ iOS의 샌드박스(Sandbox)는 엄격하게 프로그램 간 데이터 통신을 통제하고 안드로이드는 iOS에 비해 자유로운 형태의 어플리케이션 실행이 가능하다.

18. 블록체인(Block Chain)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 앞 블록의 내용을 변경하면 뒤에 이어지는 블록은 변경할 필요가 없다.

② 키를 분실할 경우 자산 이전이 불가능해질 수 있으며 공격자가 키를 획득하여 악용한 경우에도 확인이 불가능하다.

③ 퍼블릭 블록체인은 모든 참여자가 권한을 보유하지만 프라이빗 블록체인은 구성원에 따라 사용 가능한 권한 지정이 가능하다.

④ 특정기관이나 제3자의 거래를 보증하지 않고 거래 당사자끼리 가치를 교환할 수 있다.

19. OTP(One Time Password)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 시간 동기화(Time-Synchronous) 방식은 해시 체인에 기반하고 있으며 해시함수의 일방향성(one-way)을 이용한다.

② 시도-응답(Challenge-Response) 방식은 서버에서 난수 발생 등을 통해 임의의 수를 생성하여 클라이언트에 보낸다.

③ 시간-이벤트 동기화(Time-Event Synchronous) 방식은 OTP 생성 입력값으로 시간값과 카운트값을 모두 사용한다.

④ 이벤트 동기화(Event-Synchronous) 방식은 서버와 클라이언트가 카운트(Count) 값을 동일하게 증가시켜 OTP를 생성한다.

20. 「개인정보 보호법」 상 개인정보가 유출되었음을 알게 되었을 때에 개인정보처리자가 해당 정보주체에게 알려야 하는 사항으로 가장 적절하지 **않은** 것은?

① 유출된 개인정보의 항목 및 유출된 시점과 그 경위

② 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법

③ 개인정보처리자가 운영하는 시스템 정보

④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처