1. 정보보안 3요소에 대한 <보기>의 설명에서 (가), (나), (다)에 들어갈 말을 옳게 짝지은 것은?

<보기>

(가)은 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것을 말하며 변경, 가장, 재전송 등과 같은 공격에 의해 위협받을 수 있다.
(나)은 인가된 사용자만 정보 자산에 접근할 수 있다는 것으로 일반적인 보안의 의미와 가장 가깝다. 방화벽, 암호 패스워드 등이 대표적인 예이다.
(다)은 필요한 시점에 정보 자산에 대한 접근이 가능하도록 하는 것을 말하며 DDoS와 같은 공격에 의해 위협 받을 수 있다.

	(가)	(나)	(다)
①	무결성	가용성	기밀성
②	무결성	기밀성	가용성
③	기밀성	가용성	무결성
④	기밀성	무결성	가용성

2. 블록암호 알고리즘 운영모드에 대한 설명으로 가장 옳지 않은 것은?

① CBC 모드는 현재의 평문 블록을 암호키로 암호화한 후 바로 직전의 암호블록과 XOR 연산을 수행한다.
② CFB 모드 동작에서는 평문 블록 내에 한 비트의 오류가 발생하면 모든 암호문에 영향을 미치게 된다.
③ OFB 모드는 전송 중에 비트 오류가 전파되지 않는 동기식 스트림 암호이다.
④ CTR 모드는 패딩이 필요 없고 암호화 및 복호화의 사전 준비를 할 수 있어 병렬처리가 가능하다.

3. 「개인정보 보호법」에서 규정하는 개인정보보호책임자의 업무로 가장 옳지 않은 것은?

① 개인정보 보호 계획의 수립 및 시행
② 개인정보 처리와 관련한 불만의 처리 및 피해 구제
③ 정보보호 취약점 분석·평가 및 개선
④ 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

4. <보기>에서 SSL(Secure Sockets Layer)프로토콜이 수신된 데이터에 제공하는 서비스를 모두 고른 것은?

<보기>

ㄱ. 압축 ㄴ. 메시지 무결성
ㄷ. 기밀성 ㄹ. 단편화

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄱ, ㄴ, ㄹ ④ ㄱ, ㄴ, ㄷ, ㄹ

5. <보기>에서 설명하는 접근 제어 모델로 가장 옳은 것은?

<보기>

시스템 자원이 얼마나 민감하고 중요한지를 나타내는 보안 레이블과 어떤 시스템 개체가 특정 자원에 접근할 수 있는지를 나타내는 보안 허가에 기반하는 접근제어 방식이다.

① 강제 접근 제어(Mandatory Access Control)
② 임의 접근 제어(Discretionary Access Control)
③ 역할 기반 접근 제어(Role-based Access Control)
④ 속성 기반 접근 제어(Attribute-based Access Control)

6. 가상사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은?

① PPTP는 OSI 3계층에서 동작하는 터널링 기술이다.
② 이미 구축되어 있는 공용망을 이용하므로 추가적인 구축비용 부담이 적다.
③ 가상사설망은 응용프로그램 하단 계층에서 작동하므로 응용프로그램을 수정할 필요가 없다.
④ 정보의 기밀성을 제공하기 위해 데이터를 암호화한다.

7. 악성 소프트웨어에 대한 설명으로 가장 옳지 않은 것은?

① 트로이목마는 악성 루틴이 숨어 있는 프로그램으로, 겉보기에는 정상적인 프로그램으로 보이지만 프로그램을 실행하면 악성 코드가 실행된다.
② 스파이웨어는 특정 컴퓨터를 감염시켜 장악한 뒤 원격 조정할 수 있는 스파이 네트워크로, 해커는 파일을 검색하거나 내려 받을 수 있고 촬영이나 녹음을 지시할 수도 있다.
③ 랜섬웨어는 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성 코드이다.
④ PC의 부팅영역인 MBR을 조작하는 프로그램을 부트킷이라고 한다.

8. 리버스 엔지니어링을 어렵게 만드는 안티 리버싱 기술에 대한 설명으로 가장 옳지 않은 것은?

① 원본 프로그램을 새로운 파일에 패킹된 형태로 압축하고 암호화하여 저장한다.
② 공격에 이용될 수 있는 코드를 최소화하기 위해 쓰레기(Garbage)코드를 모두 삭제한다.
③ 리버스 엔지니어링 수행을 위한 디버거 활동을 탐지하여 프로그램을 강제 종료한다.
④ 다단계 점프문을 섞어 코드를 치환하여 배치한다.

9. 암호 시스템에 대한 설명으로 가장 옳지 않은 것은?
① 대칭키 암호 알고리즘은 공개키 암호 알고리즘보다 수행속도가 매우 빠르다.
② 하이브리드 암호 시스템에서 세션키는 공개키 암호화 방식을 사용해서 복호화한다.
③ 대칭키 암호 시스템에서 MAC(메시지 인증 코드)을 이용하여 기밀성과 무결성을 제공한다.
④ 타원 곡선 암호는 RSA보다 키의 비트수를 적게 하면서도 동일한 성능을 제공하는 것이 가장 큰 특징이다.

10. <보기>에서 2-요소 인증(Two-factor authentication) 방식에 해당하는 것을 모두 고른 것은?

<보기>
ㄱ. 정부24 사이트 사용을 위해, 보안 토큰에 저장되어 있는 공인인증서를 로딩하고 공인인증서 패스워드를 입력하여 로그인하였다.
ㄴ. OTP(one-time-password)를 인터넷 쇼핑몰 사이트에 입력하고 사용자 인증을 수행하였다.
ㄷ. ATM에서 현금을 인출하기 위해 현금카드를 ATM 기기에 꽂고 계좌 비밀번호를 입력하였다.
ㄹ. 서버실 출입문을 열기 위해서 얼굴인식과 홍채인증을 하였다.

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄴ, ㄹ

11. 「개인정보의 안전성 확보조치 기준」에 대한 설명으로 가장 옳지 않은 것은?
① 개인정보취급자란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
② 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.
③ 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
④ 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 연1회 이상 점검하여야 한다.

12. 키 교환 알고리즘인 Diffie-Hellman 알고리즘에 대한 설명으로 가장 옳지 않은 것은?
① 이 알고리즘의 안전성은 이산대수를 계산하는 어려움에 기초한다.
② 대칭키를 공유하기 위해 사용한다.
③ 중간자 공격에 대해 강한 안정성을 가진다.
④ 실제로 키를 교환하는 것이 아니고, 공유할 키를 각자 계산하여 만들어내는 것이다.

13. 웹 보안 취약점에 관한 <보기>의 설명에서 (가), (나)에 들어갈 말을 옳게 짝지은 것은?

<보기>
__(가)__ 공격은 브라우저로 전달되는 데이터에 악성 스크립트가 포함되어 개인의 브라우저에서 실행되면서 해킹을 하는 것이며, 이 공격용 악성 스크립트는 공격자가 웹 서버에 구현된 웹 어플리케이션의 취약점을 이용하여 서버 측 또는 URL에 미리 삽입을 해 놓은 것이다. 이에 대한 대응 조치로 게시물의 본문뿐만 아니라 댓글 및 검색어 입력 창 등 사용자 측에서 전달되는 모든 값에 대해서 __(나)__ 을/를 수행한다.

	(가)	(나)
①	Cross Site Scripting	암호화
②	Cross Site Request Forgery	암호화
③	Cross Site Request Forgery	필터링
④	Cross Site Scripting	필터링

14. <보기>에서 설명하는 네트워크 공격으로 가장 옳은 것은?

<보기>
ICMP 패킷을 일반보다 훨씬 큰 65,500바이트의 크기로 전송하여, 하나의 패킷이 네트워크를 통해 공격 대상에게 전달되는 동안 여러 개의 ICMP 패킷으로 나누어져 시스템에 과부하를 일으키게 한다.

① Ping of Death 공격 ② TearDrop 공격
③ Land 공격 ④ Smurf 공격

15. S/MIME에 대한 설명으로 가장 옳지 않은 것은?
① 보안 기능을 제공하는 전자 우편 시스템이며 X.509 인증서를 지원한다.
② 메시지 기밀성, 메시지 무결성, 부인 방지 서비스 등을 제공한다.
③ DSA 알고리즘을 사용하여 봉인된 데이터(Enveloped Data)를 생성한다.
④ 순수한 서명 데이터(Clear-Signed Data)에는 내용에 대한 전자서명이 들어있다.

16. <보기>에서 설명하는 블루투스 보안 위협으로 가장 옳은 것은?

<보기>

블루투스 장치는 장치 간 종류(전화통화, 키보드 입력, 마우스 입력 등) 식별을 위해 서비스 발견 프로토콜(SDP)을 보내고 받는다. 이 서비스 발견 프로토콜을 이용해 공격자는 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다.

① 블루프린팅 ② 블루스나프
③ 블루버그 ④ 블루재킹

17. X.509는 공개키 암호의 사용과 디지털 서명을 기반으로 한다. X.509 디지털 인증서의 구조에 포함된 것이 아닌 것은?

① 발행자 유일 식별자(Issuer Unique Identifier)
② 발행자 공개키 정보(Issuer Public Key Information)
③ 유효기간(Period of Validity)
④ 서명 알고리즘 식별자(Signature Algorithm Identifier)

18. <보기>의 ㈎~㈑에 들어갈 용어를 바르게 연결한 것은?

<보기>

IEEE 802.11i 표준은 무선랜 사용자 보호를 위해서 사용자 인증 방식, 키 교환 방식 및 향상된 무선구간 암호 알고리즘을 정의하고 있다. 무선구간에서 전송되는 데이터를 보호하기 위한 방법으로 __㈎__의 취약성을 해결한 __㈏__ 방식과 AES 암호 알고리즘을 사용하는 __㈐__ 방식을 지원한다. __㈏__ 방식은 암호키가 각 데이터프레임마다 변경되도록 만들고 메시지 무결성을 보장하기 위해 __㈑__을 프레임에 포함시킴으로써 __㈎__의 보안 취약성을 해결하였다.

	㈎	㈏	㈐	㈑
①	WEP	TKIP	CCMP	MIC
②	WAP	TKIP	CCMP	MAC
③	WEP	CCMP	TKIP	MAC
④	WAP	CCMP	TKIP	MIC

19. 보안 등급 평가 기준인 TCSEC에 대한 설명으로 가장 옳지 않은 것은?

① 보안 요구조건을 명세화하고 평가 기준을 정의하기 위한 ISO 표준이다.
② B3 보안단계에서는 운영체제에서 보안에 불필요한 부분을 모두 제거하고 모듈에 따른 분석 및 테스트가 가능하다.
③ C2 보안단계에서는 보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있다.
④ B1 보안단계에서는 시스템 내에 보안 정책을 적용할 수 있고, 각 데이터에 대해 보안 레벨 설정이 가능하다.

20. <보기>에서 디지털 포렌식 절차를 순서대로 바르게 나열한 것은?

<보기>

ㄱ. 보고서 작성
ㄴ. 사전준비
ㄷ. 보관 및 이송
ㄹ. 증거수집
ㅁ. 분석 및 조사

① ㄴ → ㄹ → ㅁ → ㄷ → ㄱ
② ㄴ → ㅁ → ㄹ → ㄷ → ㄱ
③ ㄴ → ㄹ → ㄷ → ㅁ → ㄱ
④ ㄴ → ㅁ → ㄷ → ㄹ → ㄱ

이 면은 여백입니다.