1. 암호 알고리즘에 관한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 공개키 암호는 대칭키 암호보다 키 관리가 용이하다.
나. 대칭키 암호는 공개키 암호보다 암호화 속도가 빠르다.
다. AES는 암호화와 복호화를 위해 서로 다른 키를 사용한다.
라. 3DES는 128, 192, 256비트 길이를 갖는 3개의 키를 사용한다.

① 가, 나
② 다, 라
③ 가, 나, 다
④ 가, 나, 라

2. 해시 함수(Hash Function)에 관한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 어느 메시지의 해시값이 주어졌을 때 그 해시값을 갖는 다른 메시지를 발견하는 것이 매우 곤란한 성질을 강한 충돌 내성이라고 한다.
나. 해시값으로부터 입력 메시지를 역으로 계산하는 것은 불가능해야 한다.
다. 입력 메시지가 다르면 생성되는 해시값도 달라야 하는 특성을 가져야 한다.

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

3. AES에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 라운드 키는 128비트를 사용한다.
나. 암호화 알고리즘과 복호화 알고리즘이 동일하지 않다.
다. 128비트 크기의 평문 블록을 사용하여 암호문을 생성한다.
라. 암호화에 사용되는 키 길이에 따라 라운드 수가 결정된다.

① 가, 나
② 가, 다, 라
③ 나, 다, 라
④ 가, 나, 다, 라

4. 블록 암호에 대한 설명으로 가장 적절한 것은?

① SEED는 SPN 구조로 이루어져 있다.
② ARIA는 256비트 크기의 블록을 사용한다.
③ CBC 모드는 오류 전파가 발생하지 않는다.
④ 암호 알고리즘에 따라 블록의 크기는 다를 수 있다.

5. 다음 블록 암호 공격 기법에 관한 설명으로 가장 적절한 것은?

두 개의 평문 블록들의 비트 차이에 대하여 대응되는 암호문 블록들의 비트 차이를 이용하여 사용된 암호키를 찾아내는 방법이다.

① 통계적 분석(Statistical Analysis)
② 선형 해독법(Linear Cryptanalysis)
③ 전수 공격법(Exhaustive Key Search)
④ 차분 해독법(Differential Cryptanalysis)

6. 전자서명에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 개인키로 서명을 검증한다.
나. 키 배송 문제가 발생할 수 있다.
다. 부가형 전자서명은 원래의 메시지가 필요하다.
라. 메시지 복원형 전자서명은 RSA로 구현할 수 있다.

① 가, 나
② 나, 다
③ 가, 다, 라
④ 나, 다, 라

7. PKI에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 등록기관은 인증서 발급과 취소를 담당한다.
나. 인증기관, 등록기관, 저장소, 키배포 센터는 PKI의 구성요소에 해당한다.
다. 인증서와 사용자 관련 정보, 인증서 취소 목록 등을 저장 및 검색하는 장소를 저장소라고 한다.
라. 계층구조에서는 최상위 인증기관 간의 상호인증은 허용되지만 하위 인증기관 간의 상호인증은 허용되지 않는다.

① 가, 나
② 나, 다
③ 다, 라
④ 나, 다, 라

8. 다음 RSA 암호화와 복호화 과정에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

○ 암호문 = $(\text{평문})^{E} \bmod N$ ○ 평문 = $(\text{암호문})^{D} \bmod N$

① {D, N}을 개인키라고 한다.
② 암호문의 크기는 평문의 크기와 같다.
③ N이 소인수 분해되면 D를 찾을 수 있다.
④ N을 생성하기 위해 2개의 소수가 필요하다.

9. 무결성을 위협하는 공격으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 부인(Repudiation) 나. 스누핑(Snooping) 다. 재전송(Replaying) 라. 트래픽분석(Traffic Analysis)

① 가, 다
② 가, 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

10. 메시지 인증 코드(MAC)로 해결할 수 있는 것으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 인증 나. 기밀성 다. 무결성 검증 라. 제3자에 대한 증명

① 가, 다
② 가, 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

11. 다음은 암호에 대한 설명이다. 빈칸 가, 나에 해당하는 것으로 가장 적절한 것은?

(가)는 하나의 문자를 다른 문자로 변경할 수 있으나 문자의 순서는 변하지 않는다. (나)는 평문 내의 문자들이 다른 위치로 변경될 수 있으나 문자 자체는 변하지 않는다.

	가	나
①	전치 암호	치환 암호
②	치환 암호	전치 암호
③	치환 암호	공개키 암호
④	공개키 암호	치환 암호

12. 스트림 암호에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. RC4는 동기식 스트림 암호이다. 나. AES를 CFB 모드로 운용하면 스트림 암호로 사용할 수 있다. 다. 동기식 스트림 암호에서는 암호문에 비트 오류가 발생할 경우 오류 전이가 발생한다. 라. 동기식 스트림 암호에서는 키스트림 수열이 평문과 관계없이 생성되어 동기식으로 사용한다.

① 가, 다
② 가, 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

13. 해시 함수(Hash Function)의 강한 충돌 내성을 위협하는 공격 방법으로 가장 적절한 것은?

① 중간자(Man In The Middle) 공격
② 무차별(Brute Force) 공격
③ 생일(Birthday) 공격
④ 사전(Dictionary) 공격

14. 대칭키 암호의 키 배송 문제를 해결하기 위한 방법으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 키 사전 공유 나. RSA 암호 이용 다. 전자서명 이용

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

15. 클라우드 보안 서비스(SECaaS : Security as a Service)에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 보안 솔루션 도입 비용 절감과 유연성을 확보할 수 있다.
② 주요 기능으로 네트워크 보안, 웹 보안, 취약점 스캐닝 등의 서비스를 제공한다.
③ 보안 위협에 대응하기 위해서는 사용 기관에서 보안 업데이트를 직접 수행해야 한다.
④ 클라우드 환경과 솔루션을 투자하기 어려운 환경에서 서비스 형태로 이용할 수 있다.

16. 인증 수단의 사례로 가장 적절하지 않은 것은?

① 자신의 모습(Something you are) : 신분증
② 알고 있는 것(Something you know) : ID/PW
③ 위치하는 곳(Somewhere you are) : 사용자 IP
④ 가지고 있는 것(Something you have) : 스마트키

17. 퍼블릭 클라우드의 특징에 대한 설명으로 가장 적절하지 않은 것은?

① 사용자는 필요한 서비스를 언제나 이용할 수 있다.
② 대표적인 사례로 AWS, MS Azure 등의 서비스가 있다.
③ 클라우드 제공자가 하드웨어와 소프트웨어 및 기타 IT 자원을 소유한 형태이다.
④ 공공기관이 자체 데이터 센터 내에서 클라우드 환경을 구축하는 방식이다.

18. 다음에서 설명하는 내용으로 가장 적절한 것은?

가. 시스템을 사용할 수 없을 경우를 대비한 계획이다. 나. 사이버 테러 등의 피해가 발생되어 기관의 활동이 중지될 가능성에 대비한다. 다. 지진이나 화재 등의 재해로 인해 시스템을 사용할 수 없을 때를 대비하여 가용성을 확보하기 위한 방안이다.

① 데이터 품질 관리
② 업무 연속성 계획
③ 소프트웨어 결함 분석
④ 취약점 분석 계획 수립

19. 보안 솔루션의 특징에 대한 설명으로 가장 적절하지 않은 것은?

① 백신은 PC 또는 서버에 설치되어 시스템의 바이러스를 탐지한다.
② DRM(Digital Right Management)은 문서의 열람, 편집, 인쇄에 접근 권한을 설정하여 통제한다.
③ DLP(Data Loss Prevention)는 인터넷 회선을 임대 회선처럼 사용할 수 있도록 해주는 솔루션이다.
④ NAC(Network Access Control)는 MAC(Media Access Control) 주소를 기반으로 접근제어 및 인증을 수행하여 임의의 사용자가 접속할 수 없도록 한다.

20. ISMS-P(정보보호 및 개인정보보호 관리체계)에 대한 설명으로 가장 적절하지 않은 것은?

① ISMS-P 제도에는 갱신 심사를 운영하지 않는다.
② 심사기관은 심사팀장과 심사원을 구성해 인증을 수행하는 기관이다.
③ ISMS의 인증범위는 정보 시스템의 운영 및 보호에 필요한 조직, 물리적 위치, 정보 자산을 포함한다.
④ 사후 심사는 인증을 취득한 이후 정보보호 관리체계가 지속적으로 유지되고 있는지 확인하는 것으로 인증 유효기간 중 매년 1회 이상 시행하는 심사이다.

21. 다음 블록체인 설명 중 옳은 것의 총 개수는?

가. 비트코인 블록체인은 트랜잭션들을 기록한 데이터베이스이다. 나. 블록체인 헤더에는 이전 블록 해시값이 포함되어 있다. 다. 반감기가 지날 때마다 비트코인 지급은 반으로 줄어들게 된다. 라. 난이도를 통해 비트코인 공급이 예측 가능하고 특정 일정을 따르도록 할 수 있다.

① 1개 ② 2 개 ③ 3개 ④ 4개

22. TLS(Transport Layer Security) 프로토콜에 대한 설명으로 가장 적절하지 않은 것은?

① TLS는 SSL(Secure Socket Layer)을 기반으로 구성한 프로토콜이다.
② Record 프로토콜은 프로토콜 개체의 가용성을 모니터링 할 때 사용하는 프로토콜이다.
③ TLS 1.2에는 안전하지 않은 프로토콜이 포함되어 있으므로 사용 시 주의할 필요가 있다.
④ Handshake 프로토콜을 사용하여 서버와 클라이언트가 서로 인증하고, TLS 레코드 안에 송신 데이터를 보호하는데 사용할 암호화키를 협상할 수 있다.

23. SQL Injection 공격의 종류와 설명으로 가장 적절한 것은?

① Blind SQL Injection 공격은 오류 메시지가 아닌 쿼리 결과의 참과 거짓을 통해 의도하지 않은 SQL 문을 실행하여 DB를 비정상적으로 공격하는 방법이다.
② Form SQL Injection 공격은 DB 쿼리에 대한 에러값을 기반으로 한 단계씩 점진적으로 DB 정보를 획득하는 방법이다.
③ Union SQL Injection 공격은 게시판이나 자료실과 같은 사용자 글을 저장할 수 있는 부분에 정상적인 평문이 아닌 스크립트 코드를 입력하는 방법이다.
④ Error-based SQL Injection 공격은 피해자가 공격을 인지하지 못하는 상태에서 피해자의 브라우저가 특정 사이트에 강제적으로 request를 보내도록 하는 방법이다.

24. 다음에서 설명하는 내용으로 가장 적절한 것은?

가. 구축 시 새로운 프로토콜이나 라이브러리를 도입할 필요는 없다.
나. 네트워크 상의 모든 호스트를 인터넷에 연결된 호스트처럼 취급한다.
다. 호스트가 어디에 있든 상관 없이 네트워크에 해커가 존재하며 언제든 공격할 준비가 되어 있다고 가정한다.
라. 네트워크 상의 설정을 담당하는 시스템을 컨트롤 플레인이라고 부르며, 컨트롤 플레인이 설정하고 관리하는 다른 모든 부분은 데이터 플레인이라고 한다.

① 아마존 웹 서비스(Amazon Web Service)
② 제로 트러스트 네트워크(Zero Trust Networks)
③ 구글 클라우드 플랫폼(Google Cloud Platform)
④ 서비스 수준 계약(Service Level Agreement)

25. WAF(Web Application Firewall)에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 웹 애플리케이션을 겨냥한 전형적인 공격으로부터 시스템을 보호한다.
② 통신 식별 방식으로 블랙리스트 방식과 화이트리스트 방식 모두 사용한다.
③ 발견된 공격 패턴을 WAF에 등록하고 등록된 패턴과 매치되면 부정 접속으로 간주한다.
④ SQL 인젝션 공격, XSS 공격을 방어하기 어렵다.

26. CVSS(Common Vulnerability Scoring System)에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 기업이나 담당자의 경험에 의존한다.
② 정량적으로 취약점의 심각도를 비교할 수 있다.
③ 취약점에 대한 개방적이고 범용적인 평가 방법으로 국제적으로 사용되고 있다.
④ 취약점에 대해 동일한 기준으로 비교할 수 있기 때문에 우선적으로 대응해야 할 내용을 판단할 수 있다.

27. 다음의 동작 과정에 해당하는 공격으로 가장 적절한 것은?

가. 웹 브라우저에서 실행 가능한 웹 프로그램을 파일 업로드를 통해 웹 서버에 업로드하여 공격자가 명령을 입력할 수 있는 명령 창을 획득한다.
나. 서버 게시판의 파일 업로드 기능을 이용하여 공격에 활용할 도구를 업로드한다.
다. 서버의 공격용 도구를 활용하여 공격자에게 신호를 보내면 공격자는 이를 통해 명령을 입력할 수 있도록 한다.

① 포트 스캔
② 리버스 텔넷
③ 중간자 공격
④ 세션 하이재킹

28. 개인정보보호법 제4조(정보주체의 권리)는 정보주체의 개인정보 처리와 관련된 권리를 규정하고 있다. 이 조항과 관련된 정보주체의 권리로 가장 적절하지 <u>않은</u> 것은?

① 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
③ 완전히 자동화된 개인정보 처리에 따른 결정을 거부하거나 그에 대한 설명 등을 요구할 권리
④ 개인정보의 처리에 관한 실태조사 및 개인정보 보호 수준을 평가할 권리

29. 개인정보보호위원회에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 둔다. 나. 위원회는 상임위원 2명을 포함한 11명의 위원으로 구성한다. 다. 위원장과 부위원장은 정무직 공무원으로 임명한다.

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

30. 개인정보보호법 제17조(개인정보의 제공)에서 개인정보처리자는 정보의 주체의 동의를 받고 정보주체의 개인정보를 제3자에게 제공할 수 있다. 이 경우에 제3자에게 개인정보를 제공하는 개인정보처리자가 정보주체에게 알려할 항목에 해당하지 <u>않은</u> 것은?

① 개인정보를 제공받는 자
② 개인정보의 수집 출처
③ 개인정보를 제공받는 자의 개인정보 이용 목적
④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간

31. 개인정보보호법 시행령 제19조(고유식별정보의 범위)에서 정하는 고유식별정보로 가장 적절하지 <u>않은</u> 것은?

① 유전자검사 등의 결과로 얻어진 유전정보
② 주민등록번호
③ 운전면허의 면허번호
④ 외국인등록번호

32. 정보통신기반 보호법 시행령 제20조(보호지침의 제정)에서 보호지침에 포함되어야 할 사항으로 가장 적절하지 <u>않은</u> 것은?

① 정보보호체계의 관리 및 운영
② 유사한 침해사고의 방지를 위한 예방대책
③ 취약점 분석·평가 및 침해사고 예방
④ 침해사고에 대한 대응 및 복구

33. 다음은 개인정보보호법 및 동법 시행령에서 개인정보의 열람에 대한 내용과 개인정보 유출 등의 통지에 대한 내용이다. 빈 칸 ㉠, ㉡에 해당하는 것으로 가장 적절한 것은?

가. 정보주체가 개인정보처리자에게 자신의 개인정보에 대한 열람을 요청할 경우, 개인정보처리자는 (㉠) 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 나. 개인정보처리자는 개인정보가 분실·도난·유출되었음을 알게 되었을 때에는 (㉡) 이내에 정보주체에게 알려야 한다.

	㉠	㉡
①	5일	24시간
②	7일	24시간
③	10일	72시간
④	14일	72시간

34. 약칭 정보통신망법 시행령 제55조의2(정보보호 관리등급 부여의 심사기준)에서 정보보호 관리등급 부여의 심사기준으로 가장 적절하지 <u>않은</u> 것은?

① 정보보호 관리체계의 구축 범위 및 운영기간
② 정보보호를 위한 전담조직 및 예산
③ 정보보호 관리체계를 수립·운영하는 방법과 절차
④ 정보보호 관리 활동 및 보호조치 수준

35. 위치정보의 보호 및 이용에 관한 법률 시행령 제20조(위치정보의 관리적·기술적 보호조치)에서 관리적 보호조치에 해당하는 것으로 가장 적절한 것은?

① 위치정보 제공사실 등을 기록한 취급대장의 운영·관리
② 위치정보 및 위치정보시스템의 접근권한을 확인할 수 있는 식별 및 인증 실시
③ 위치정보시스템에 대한 접근사실의 전자적 자동 기록·보존장치의 운영
④ 위치정보시스템의 침해사고 방지를 위한 보안프로그램 설치 및 운영

36. ISMS-P(정보보호 및 개인정보보호 관리체계) 보호대책 요구사항 영역에 있는 인증 및 권한관리 분야의 항목으로 가장 적절하지 <u>않은</u> 것은?

① 사용자 계정 관리
② 사용자 식별
③ 비밀번호 관리
④ 직무 분리

37. CC(공통 평가 기준)의 보안 기능 요구사항으로 가장 적절하지 <u>않은</u> 것은?

① 취약성 평가
② 식별 및 인증
③ 암호 지원
④ 보안 감사

38. 동일한 데이터가 2개 이상의 디스크에 동시에 저장되는 RAID 유형으로 가장 적절한 것은?

① RAID 0
② RAID 1
③ RAID 2
④ RAID 5

39. 다음 보기에서 설명하는 재해복구시스템의 복구 수준별 유형으로 가장 적절한 것은?

가. 주 센터와 재해복구센터 모두 액티브 상태이며 실시간으로 동시 서비스하는 방식이다. 나. 재해 발생 시 복구까지의 소요시간은 이론적으로 0이다.

① hot site
② warm site
③ mirror site
④ cold site

40. 소프트웨어 개발 보안 가이드에서 설계단계 보안항목으로 가장 적절하지 <u>않은</u> 것은?

① DBMS 조회 및 결과 검증
② 허용된 범위내 메모리 접근
③ 암호키 관리
④ 종료되지 않은 반복문 재귀함수