1. 정보보안 용어에 대한 설명으로 가장 적절한 것은?
① 위협은 자산에 대한 위협원의 공격 행동이다.
② 취약점은 위협이 약점을 이용하여 해를 끼치는 순간이나 시점이다.
③ 위험은 자산이 가지고 있는 속성이거나 보안 대책의 미비점이다.
④ 노출은 자산에 악영향을 미치는 결과를 가져올 가능성이다.

2. 보안 위협과 보안 위협이 영향을 주는 보안 목표와의 연결 관계로 가장 적절한 것은?
① 가로채기 - 가용성 ② 가로막음 - 무결성
③ 변조 - 기밀성 ④ 위조 - 인증

3. RSA에서 두 소수 p, q를 사용하여 n=p*q를 구성하고, 암호화키가 e일 때 복호화키 d는 법(modulus) ϕ(n)에서 e의 승산 역원이다. p=5, q=11이고 e=7일 때 d의 값으로 가장 적절한 것은?
① 7 ② 13 ③ 23 ④ 33

4. Diffie-Hellman 키 분배 알고리즘에서 원시원소 g=2이고 p=13이며 x=125일 때 가입자 A가 가입자 B에게 전송하는 메시지는 2^{125} mod 13이다. 이 값으로 가장 적절한 것은?
① 2 ② 3 ③ 6 ④ 8

5. 암호화 모드에 대한 설명으로 가장 적절한 것은?
① ECB 모드는 동일한 키에 의한 동일한 평문 블록은 항상 동일한 암호문이 출력된다.
② CBC 모드의 암호문 블록은 이전 암호문 블록과 독립적이다.
③ OFB 모드는 암호화할 때 피드백이 없다.
④ CTR 모드는 출력 암호문이 다음 평문 블록에 영향을 미친다.

6. 공개키 암호 방식을 이용하여 전자서명을 생성하고 검증할 때에는 공개키와 개인키가 사용된다. 송신자가 전자서명을 생성하고 수신자에게 전자서명을 전송하는 경우, 수신자가 전자서명을 검증할 때 사용하는 키로 가장 적절한 것은?
① 송신자의 개인키 ② 송신자의 공개키
③ 수신자의 개인키 ④ 수신자의 공개키

7. SHA(Secure Hash Algorithm)에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?
① SHA-1은 160비트의 해시값을 출력한다.
② SHA-224는 라운드 수가 80이다.
③ SHA-256의 블록 크기는 512비트이다.
④ SHA-384는 입력되는 데이터의 크기가 2^{128}-1비트로 제한된다.

8. 다음 ElGamal 암호 방식에 대한 설명으로 옳은 것의 개수로 가장 적절한 것은?

가. ElGamal 기법은 공개키 암호 방식이다.
나. ElGamal 기법은 소인수 분해 어려움을 이용한다.
다. ElGamal 기법은 전자서명, 암호화, 키교환에 사용될 수 있다.
라. ElGamal 기법은 일반적으로 암호문의 길이가 평문의 길이보다 짧다.

① 1 ② 2 ③ 3 ④ 4

9. 타원 곡선 암호시스템(Elliptic Curve Cryptosystem)에 대한 설명으로 가장 적절한 것은?
① 타원 곡선 방정식은 $y^2=x^3+ax^2+b$ 형태를 갖는다.
② 타원 곡선상의 두 점 P, Q의 덧셈은 P와 Q를 연결하는 직선과 교차하는 곡선상의 점이다.
③ 타원 곡선상의 모든 점은 덧셈 역원을 갖는다.
④ 타원 곡선상의 한 점 $P=(x_1, x_2)$에 상수 k를 곱한 Q=kP인 경우 Q의 점은 $Q=(kx_1, kx_2)$가 된다.

10. MDC(Modification Detection Code)와 MAC(Message Authentication Code) 기법에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① MDC는 일반적으로 키와 메시지를 이어붙인 K|M에 해시함수를 적용하여 h(K|M)을 생성한다.
② 축소(nested) MAC 기법은 두 단계로 해싱이 이루어진다.
③ HMAC 기법은 일방향 해시 함수를 이용하여 메시지 인증 코드를 구성한다.
④ CMAC(Cipher-based MAC) 기법은 암호시스템의 CBC (Cipher Block Chaining) 모드와 유사한 방법이다.

11. X.509 인증서에 들어있는 필드에 대한 설명으로 가장 적절한 것은?

① 서명 알고리즘 ID 필드는 인증서를 서명한 알고리즘을 식별하기 위해 사용된다.
② 발행자(issuer) 이름 필드는 공개키의 소유자인 개체를 나타낸다.
③ 주체(subject) 개인키 필드는 발행자의 개인키를 나타낸다.
④ 서명(signature) 필드는 두 부분으로 이루어진다.

12. WPA2(Wi-Fi Protected Access 2) 설명으로 가장 적절하지 <u>않은</u> 것은?

① 128비트인 통신용 암호화키를 생성하고, 암호화키는 10,000개 패킷마다 바꾼다.
② AES 암호화 알고리즘을 사용하는 것이 가능하다.
③ AES-CCMP를 통한 암호화 기능을 향상 시킨다.
④ AP에 접속하는 사용자마다 같은 암호화키는 상위의 보안성을 보장받는다.

13. 다음 설명에 해당하는 기술로 가장 적절한 것은?

> 암호문 상태에서도 연산이 가능한 차세대 암호기술이다. 데이터를 기존 암호알고리즘을 통해 비식별화하는 경우 클라우드에서 암호화된 데이터에 대한 연산이 불가능하지만, 이 암호기술을 활용하면 민감정보를 안전하게 보호하면서도 유용하게 데이터를 활용할 수 있다.

① 동형암호(Homomorphic Encryption)
② 양자내성암호(Post-Quantum Cryptography)
③ 배낭암호(Knapsack Cryptography)
④ TPM(Trusted Platform Module)

14. 지적 재산권 보호에 사용되는 스테가노그래피(steganography), 워터마킹(watermarking), 핑거프린팅(fingerprinting)에 대한 설명으로 가장 적절한 것은?

① 스테가노그래피는 핑커프린팅보다 저작권 증명이 우수하다.
② 워터마크는 핑거프린팅보다 상대적으로 불법 예방 효과가 좋다.
③ 스테가노그래피의 은닉정보는 주로 판매자 정보이다.
④ 핑거프린팅의 특징에는 비가시성, 견고성, 복잡성 등이 있다.

15. 접근제어(Access Control) 시스템의 일반적인 구분과 특성으로 가장 적절하지 <u>않은</u> 것은?

① 파일 리스트 접근제어(File List Access Control)-접근리스트 기반
② 임의적 접근제어(Discretionary Access Control)-신분 기반
③ 비임의적 접근제어(Non-Discretionary Access Control)-역할 기반
④ 강제적 접근제어(Mandatory Access Control)-규칙 기반

16. Bell-LaPadula 모델에 대한 설명으로 가장 적절한 것은?

① 높은 등급의 정보가 낮은 레벨로 유출되는 것을 통제하는 모델이다.
② 정보는 Top Secret, Secret, Unclassified로 분류하고 정보의 무결성 보장에 초점을 두고 있다.
③ No Write-Down 정책은 주체는 자신보다 낮은 등급의 객체에 정보를 쓸(write) 수 있다.
④ No Read-Up 정책은 주체는 자신보다 높은 등급의 객체를 읽고 쓸(read/write) 수 없다.

17. 스트림 암호 방식과 블록 암호 방식에 대한 설명으로 가장 적절한 것은?

① 스트림 암호는 실시간 처리에 부적합하다.
② RC4는 바이트 단위 스트림 암호이다.
③ ARIA는 키 크기와 라운드 수가 AES와 동일한 규격이다.
④ 블록 암호 방식에는 RC5, 3DES, AES, SEED, HIGHT, LSH 등이 있다.

18. 다음 지문에 대한 설명으로 가장 적절한 것은?

> JavaScript와 HTML5의 Blob, download, anchor, click 등의 특성을 이용하여 인터넷 사용자가 특정 HTML 페이지 방문 시 자동으로 파일을 다운받도록 하는 기법이다.

① HTML Smuggling
② HTML Injection
③ Dangling Markup Injection
④ JavaScript Injection

19. 스마트폰에 메시지가 뜨면, 근처의 다른 블루투스를 인식한 스마트폰에 같은 메시지를 퍼트릴 수 있는 보안 위협으로 가장 적절한 것은?

① 블루프린팅(Blueprinting)
② 블루재킹(Blue-jacking)
③ 블루스나프(BlueSnarf)
④ 블루버그버그(Blue-bugbug)

20. 웹셸(Web shell) 공격의 설명으로 가장 적절하지 <u>않은</u> 것은?

① 예방책으로 시큐어 코딩과 취약점 패치, 키워드와 명령어 필터링이 있다.
② 웹셸공격은 서버로부터 명령을 클라이언트에서 실행시켜주는 프로그램을 말한다.
③ 웹셸공격은 제어권 탈취, 정보탈취, 변조의 악성행위를 한다.
④ 웹셸공격 프로그램은 ASP, PHP, JSP 언어를 사용한다.

21. 웹방화벽(Web firewall) 설명으로 가장 적절하지 <u>않은</u> 것은?

① Cross-site scripting, SQL injection 공격을 탐지하고, 차단한다.
② 웹서버를 통과하는 PPTP 메시지는 공개키로 복호화한다.
③ 애플리케이션 계층의 분석과 정규화 기술을 사용한다.
④ URL에 따른 접근제어 기능과 SSL 트래픽을 복호화하여 검사한다.

22. 블록체인(Block Chain) 거래의 설명 중 가장 적절한 것은?

① 이중지불(Double spending)은 사용자가 자산에 대한 거래를 확정 후에 거래를 취소하거나 자산을 재사용하는 것이다.
② 합의 가로채기(Consensus hijacking)는 사용자 자산의 거래 대금 중, 합의된 수수료를 가로채는 것을 말한다.
③ Dapp(Decentralized application)은 블록체인의 중앙시스템에서 실행되므로, Dapp이 처리하는 정보의 공유를 쉽게 하여 거래를 활성화한다.
④ 거래 수수료(Transaction fee)는 거래를 블록에 추가하는 작업에 대한 수수료를 의미한다.

23. 블록체인(Block Chain) 기술 설명 중 가장 적절하지 <u>않은</u> 것은?

① 앵커링(Anchoring)은 합의된 거래 및 블록의 무결성 보장을 강화하기 위한 타 블록체인을 활용하는 기술이다.
② 작업 증명(Proof of work)은 블록을 생성하는 경량 노드(Light node)가 거래량과 권한을 부여하는 작업 증명 방식이다.
③ 비잔틴 장애 허용(Byzantine Fault Tolerance)은 일부 노드가 결함이 있어도, 이를 허용할 수 있는 합의 방식이다.
④ 메인 체인(Main chain)은 합의 알고리즘에 따라 선정된 블록체인으로 가장 긴 블록체인을 말한다.

24. 전자지불시스템의 정보보호 요구사항으로 가장 적절하지 <u>않은</u> 것은?

① 거래하는 전자화폐는 위조불가능(unforgeability) 해야 한다.
② 송신자와 수신자가 전자지불시스템의 합법적인 사용자임이 인증되어야 한다.
③ 개인들의 신상관련 정보들이 통신망 상에서는 익명성(anonymity)으로 보호되어야 한다.
④ 암호화폐와 가상화폐는 개인별로 법정통화와 교환이 보장되어야 한다.

25. 버퍼 오버플로우(buffer overflow) 공격의 대응책으로 가장 적절하지 <u>않은</u> 것은?

① 스택에서 실행(execute) 권한을 제거하여, 프로그램을 실행할 수 없도록 한다.
② 컴파일러가 프로그램 함수 호출 시 RET 앞에 Canary 값을 주입하고, 종료 시, Canary 값이 변조되었는지 확인한다.
③ 함수 호출 시 RET를 Global RET 스택에 저장하고, 종료 시 RET 값이 변조되었는지 확인한다.
④ 스택과 라이브러리의 데이터 영역 주소를 암호화하고, strcat() 함수 사용 시 복호화하여 변조되었는지 확인한다.

26. OWASP TOP 10 LIST, 2021의 A01, A02, A03 내용으로 가장 적절하지 <u>않은</u> 것은?

① Security Misconfiguration
② Injection
③ Cryptographic Failures
④ Broken Access Control

27. 실시간 위험탐지 및 대응을 위해 이벤트 로그(event log) 데이터를 실시간으로 수집하고 분석하는 기능을 가지고 있으며, 공격 로그의 포렌식(Forensic) 분석을 위한 데이터 검색 및 리포트 기능을 제공하는 것으로 가장 적절한 것은?

① SIEM(Security Information Event Management)
② PGP(Pretty Good Privacy)
③ PPTP(Point-to-Point Tunneling Protocol)
④ L2F(Layer 2 Forwarding)

28. '소프트웨어 개발 보안'의 적용 사례로 가장 적절하지 <u>않은</u> 것은?

① CLASP(Comprehensive, Lightweight Application Security Process)
② CMVP(Cryptographic Module Validation Program)
③ Seven Touchpoints
④ MSDL(Microsoft Secure Development Lifecycle)

29. GDPR(General Data Protection Regulation)에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① EU 내 사업장을 운영하며 개인정보를 처리하는 기업에 적용
② EU 거주자의 행동을 모니터링하는 기업에 적용
③ 전자상거래를 통해 해외에서 EU 주민의 개인정보를 처리하는 기업에 적용
④ 최대 과징금은 중요한 위반사항인 경우, 전 세계 매출액의 5% 혹은 3천만 유로 중 높은 금액

30. ISMS-P(정보보호 및 개인정보보호 관리체계) 인증 기준에서 정하고 있는 관리체계 수립 및 운영 영역의 분야로 가장 적절하지 <u>않은</u> 것은?

① 관리체계 기반 마련
② 위험관리
③ 관리체계 점검 및 개선
④ 정책, 조직, 자산 관리

31. 'ISO 27001:2022 Annex A 정보보안 통제'에서 기술적 보안(Technological Controls) 항목으로 가장 적절하지 <u>않은</u> 것은?

① 시스템 네트워크 보안
② 애플리케이션 보안
③ 물리적 보안
④ 보안 구성

32. 정보보호 시스템 공통평가 기준(Common Criteria)의 보증 요구사항으로 'Methodically Designed, Tested and Reviewed(방법론적 설계, 시험, 검토)'에 해당되는 평가보증등급(EAL)으로 가장 적절한 것은?

① EAL2
② EAL3
③ EAL4
④ EAL5

33. 다음은「개인정보보호법」제2조(정의)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

> 1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
> 가. (㉠), 주민등록번호 및 (㉡) 등을 통하여 개인을 알아볼 수 있는 정보
> 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 (㉢)하여 알아볼 수 있는 정보

① ㉠ 성명 ㉡ 전화번호 ㉢ 연계
② ㉠ 성별 ㉡ 전화번호 ㉢ 연계
③ ㉠ 성명 ㉡ 영상 ㉢ 결합
④ ㉠ 성별 ㉡ 영상 ㉢ 연동

34. 「개인정보 보호법 시행령」에서 명시하는 개인정보 영향평가의 대상에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 구축·운용 또는 변경하려는 개인정보파일로서 10만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
③ 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
④ 영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

35. 「개인정보보호법」에서 명시하는 영상정보처리기기의 설치·운영 제한과 관련하여 정보주체가 쉽게 인식하도록 설치하는 안내판의 기재 항목으로 가장 적절하지 <u>않은</u> 것은?

① 설치 목적
② 촬영 범위
③ 저장 방식
④ 관리책임자 연락처

36. 다음은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2(클라우드컴퓨팅서비스의 보안인증)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 내용으로 가장 적절한 것은?

> ① (㉠)은 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 대통령령으로 정하는 바에 따라 인증(이하 "보안인증"이라 한다)을 할 수 있다.
> ② 보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 (㉡) 내의 범위로 하고, 보안인증의 유효기간을 연장받으려는 자는 대통령령으로 정하는 바에 따라 유효기간의 갱신을 신청하여야 한다.

① ㉠ 한국인터넷진흥원장 ㉡ 3년
② ㉠ 한국인터넷진흥원장 ㉡ 5년
③ ㉠ 과학기술정보통신부장관 ㉡ 3년
④ ㉠ 과학기술정보통신부장관 ㉡ 5년

37. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증)에 대한 내용이다. 가장 적절한 것은?

① 과학기술정보통신부는 정보통신망의 안정성·신뢰성 확보를 위하여 정보통신망 보호조치를 포함한 관리체계를 수립·운영하고 있는 자에 대하여 인증을 할 수 있다.
② 연간 매출액 또는 세입 등이 1,000억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자는 인증을 받아야 한다.
③ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시한다.
④ 정보보호 관리체계 인증의 유효기간은 2년으로 한다.

38. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」에서 명시하는 집적정보통신시설 사업자등의 서비스 중단 보고 방법에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 연속해서 30분 이상 서비스 중단 시 보고한다.
② 24시간 이내에 2회 이상 중단된 경우에는 그 중단된 기간의 합이 45분 이상 시 보고한다.
③ 보고 시 발생한 일시 및 장소, 발생 원인 및 피해내용, 응급조치 사항, 대응 및 복구대책, 향후 조치계획 등을 포함해야 한다.
④ 집적정보통신시설 사업자등은 정보통신서비스 제공의 중단이 발생하였을 때에는 과학기술정보통신부장관에게 즉시 유선으로 보고해야 한다.

39. 「정보통신기반 보호법」에서 지정한 주요정보통신기반시설로 가장 적절하지 <u>않은</u> 것은?

① 도로, 철도, 지하철, 공항, 항만 등 주요 교통시설
② 전력, 가스, 석유 등 에너지·수자원 시설
③ 인터넷 포털, 전자상거래의 정보통신시설
④ 원자력, 국방과학, 첨단방위산업관련 정부출연연구기관의 연구시설

40. 다음은 「정보통신기반 보호법 시행령」에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 내용으로 가장 적절한 것은?

> 제8조(주요정보통신기반시설보호대책의 수립)에서는 주요정보통신기반시설보호대책을 수립하여 매년 (㉠)까지 (㉡)의 장에게 제출하여야 한다.

① ㉠ 5월 31일 ㉡ 관계중앙행정기관
② ㉠ 8월 31일 ㉡ 관계중앙행정기관
③ ㉠ 5월 31일 ㉡ 위원회
④ ㉠ 8월 31일 ㉡ 위원회