정보보호론

1. 일방향 해시 함수의 응용으로 적합하지 않은 것은?
   ① 전자서명
   ② 의사난수 생성
   ③ 데이터 암복호화
   ④ 소프트웨어 변경 검출

2. RSA 암호 알고리즘에 대한 설명으로 옳지 않은 것은?
   ① 공개키 기반 암호 방식이다.
   ② 개인키는 공개하지 않고 비밀로 유지한다.
   ③ 큰 수의 소인수분해가 어렵다는 특성을 이용한다.
   ④ 공개키로 암호화한 메시지는 전자서명 기능을 제공한다.

3. DBMS에서 데이터베이스 객체에 대한 권한 부여를 위해 사용하는 SQL 명령어는?
   ① ALTER
   ② GRANT
   ③ INSERT
   ④ COMMIT

4. SSLv3(Secure Sockets Layer version 3)의 레코드 프로토콜에서 응용 프로그램으로부터 획득한 데이터를 송신하기 위해 수행하는 과정을 순서대로 바르게 나열한 것은?
   ① 압축(옵션) → MAC 추가 → 암호화 → 단편화 → 헤더 추가
   ② 압축(옵션) → 헤더 추가 → 암호화 → 단편화 → MAC 추가
   ③ 단편화 → 압축(옵션) → MAC 추가 → 암호화 → 헤더 추가
   ④ 단편화 → 암호화 → MAC 추가 → 압축(옵션) → 헤더 추가

5. 조직의 자산 및 정보를 보호하기 위한 정보보호 관리체계의 국제 인증 규격은?
   ① CC
   ② ITSEC
   ③ TCSEC
   ④ ISO/IEC 27001

6. 시스템 보안에서 사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속을 관리하는 것은?
   ① 세션 관리
   ② 권한 관리
   ③ 로그 관리
   ④ 취약점 관리

7. 다음 설명에 해당하는 정보보호 위험 분석 방법은?

> 정성적 위험 분석 방법으로, 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.

   ① 확률 분포법
   ② 델파이법
   ③ 과거 자료 분석법
   ④ 수학 공식 접근법

8. CAPTCHA에 대한 설명으로 옳지 않은 것은?
   ① 컴퓨터와 사람을 구분하기 위한 자동화된 공개 튜링 테스트라 할 수 있다.
   ② 기밀성을 보장하기 위한 암호의 한 형태이다.
   ③ 다양한 이미지, 왜곡된 문자, 잡음 섞인 소리를 사용할 수 있다.
   ④ 대부분의 사람들이 통과하기에는 쉽지만 컴퓨터가 통과하기에는 불가능하거나 어려워야 한다.

9. 다음 설명에 해당하는 보안 솔루션은?

> IP 관리 시스템에서 발전한 것으로, MAC 주소를 기반으로 접근 제어 및 인증을 수행하여, 보안 정책에 부합되는 단말기에만 네트워크 자원의 이용을 허용한다.

   ① NAC
   ② DLP
   ③ VPN
   ④ PIMS

10. SSH 프로토콜(RFC 4251)의 구성요소에 해당하지 않는 것은?
   ① 핸드셰이크(Handshake) 프로토콜
   ② 사용자 인증(User Authentication) 프로토콜
   ③ 전송 계층(Transport Layer) 프로토콜
   ④ 연결(Connection) 프로토콜

11. 「(대검찰청) 디지털 증거의 수집·분석 및 관리 규정」상 전자정보 압수·수색·검증의 기본원칙이 아닌 것은?
   ① 적법절차의 준수
   ② 디지털 증거의 신뢰성 유지
   ③ 디지털 증거의 기밀성 유지
   ④ 디지털 증거의 원본성 유지

12. 국내 정보보호 관리체계(ISMS)에서 '관리체계 수립 및 운영'의 PDCA 사이클을 바르게 나열한 것은?

(가) 위험관리
(나) 관리체계 운영
(다) 관리체계 기반 마련
(라) 관리체계 점검 및 개선

P	D	C	A

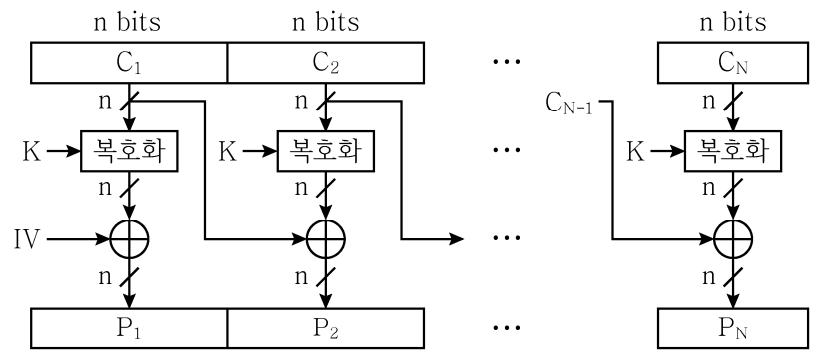
① (가) → (나) → (라) → (다)
② (가) → (다) → (나) → (라)
③ (다) → (가) → (나) → (라)
④ (다) → (나) → (가) → (라)

13. 다음 설명에 해당하는 DoS/DDoS 공격기법은?

순서 번호에 오류가 있게 조작된 IP 패킷 조각(fragments)을 전송하여, 이 패킷 조각을 전달받은 시스템의 IP 패킷 재조합 과정에서 오류가 발생되도록 하는 공격기법

① Smurf
② Teardrop
③ ICMP Flooding
④ Buffer Overflow

14. 복호화 과정이 다음 그림에 해당하는 블록 암호 운영 모드는?



P_i: 평문 블록, C_i: 암호문 블록, IV: 초기벡터, K: 키, ⊕: XOR 연산

① ECB(Electronic CodeBook)
② CBC(Cipher Block Chaining)
③ CFB(Cipher FeedBack)
④ CTR(CounTeR)

15. RSA 암호 알고리즘은 키를 생성하는 과정에서 법(modulus) 연산의 곱셈에 대한 역원(multiplicative inverse)을 찾아야 한다. 법 26에 관한 완전잉여계 집합 $Z_{26} = \{0, 1, \cdots, 25\}$에 속한 원소 중에서 곱셈에 대한 역원이 존재하지 않는 것은?

① 7
② 11
③ 13
④ 23

16. ISMS-P의 '보호대책 요구사항' 분야에 해당하지 않는 것은?

① 정보주체 권리보호
② 재해 복구
③ 외부자 보안
④ 정책, 조직, 자산 관리

17. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

IPSec(RFC 2401)에서 (가)는 기밀성(confidentiality), 데이터 발신 인증(data origin authentication), 비연결 무결성(connectionless integrity) 등을 제공하는 프로토콜이다. 이 프로토콜은 기밀성을 제공하기 위해 (나) 암호 알고리즘을 사용하여 데이터를 암호화한다.

(가)	(나)

① AH 공개키
② AH 대칭키
③ ESP 공개키
④ ESP 대칭키

18. 「개인정보 보호법」상 개인정보 보호위원회의 위원 자격 요건에 해당하지 않는 사람은?

① 공공기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람
② 개인정보 보호 업무를 담당하는 3급 이상 공무원의 직에 있었던 사람
③ 판사·검사·변호사의 직에 10년 이상 있었던 사람
④ 대학 부교수 이상으로 3년 이상 재직하였던 사람

19. 「개인정보 보호법」상 정보주체의 개인정보 열람 요구 시에, 개인정보처리자가 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있는 경우가 아닌 것은?

① 법률에 따라 열람이 금지되거나 제한되는 경우
② 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
③ 공공기관이 조세의 부과·징수 또는 환급에 관한 업무를 수행할 때 중대한 지장을 초래하는 경우
④ 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우

20. 「보안관제 전문기업 지정 등에 관한 공고」상 보안관제 전문기업 지정기준으로 옳지 않은 것은?

① 법인 설립 이후 5년 이상일 것
② 자기 자본이 20억원 이상일 것
③ 보안관제 수행능력 평가기준에 따라 실시한 심사에서 70점 이상을 받을 것
④ 자격기준을 갖춘 기술인력을 15명 이상 보유할 것(고급기술자 3명 이상, 중급기술자 6명 이상을 포함하여야 한다)