1. IPSec(IP Security)에는 전송 모드(transport mode)와 터널 모드(tunnel mode)가 운영된다. IPSec에 대한 설명으로 가장 옳지 않은 것은?
① 전송 모드는 보통 호스트-대-호스트 데이터 보호를 필요로 할 때 사용된다.
② 터널 모드에서 IPSec은 가상 터널을 이용하며 새로운 IP패킷은 원래의 IP헤드와 정보를 포함한다.
③ 네트워크 레벨에서 패킷에 대한 보안을 제공하기 위해 IETF에 의해 설계된 프로토콜이다.
④ 전송 모드와 터널 모드에서 IPSec은 전송 계층에서 온 정보 즉, IP헤드를 포함한 IP패킷 전체를 보호한다.

2. 전자우편에 프라이버시, 무결성, 그리고 인증을 제공하기 위해 필 짐머만(Phil Zimmermann)에 의해 고안된 것으로, 안전한 전자우편 메시지를 생성하거나 향후에 검색한 파일을 안전하게 저장하기 위해 사용될 수 있다. 자신이 통신하기 원하는 각각의 사람들에 대한 공개키가 필요하고, 자신에게 속해 있는 개인키/공개키의 링이 필요한 프로토콜은?
① POP3 ② SMTP ③ PGP ④ S/MIME

3. 「전자서명법」상 공인인증서에 대한 설명으로 가장 옳지 않은 것은?
① 공인인증서에는 공인인증기관의 서명키가 포함되어야 한다.
② 가입자의 사망, 실종선고 또는 해산 사실을 인지한 경우에는 당해 공인인증서를 폐지하여야 한다.
③ 공인인증서의 유효기간이 경과한 경우에는 그 사유가 발생한 때에 그 효력이 소멸된다.
④ 공인인증기관은 공인인증서를 발급받고자 하는 자의 신청이 있는 경우에는 공인인증서의 이용범위 또는 용도를 제한하는 공인인증서를 발급할 수 있다.

4. 「개인정보 보호법」상 <보기> 안의 ㉠에 들어갈 숫자로 옳은 것은?

<보기>

개인정보에 관한 분쟁을 조정하는 개인정보 분쟁조정위원회는 위원장 1명을 포함한 ㉠ 명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.

① 10 ② 20 ③ 30 ④ 40

5. KDC(key distribution center) 없이 양쪽 통신 주체가 대칭 세션 키를 생성할 수 있는 프로토콜은?
① Otway-Rees 프로토콜
② Needham-Schroeder 프로토콜
③ Diffie-Hellman 프로토콜
④ Kerberos 프로토콜

6. 전자 서명의 기능과 가장 관계가 없는 것은?
① 인증성 ② 무결성
③ 부인봉쇄 ④ OTP 시간동기

7. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳지 않은 것은?
① 탐지분석 방법에는 오용 탐지 모델과 이상 탐지 모델이 있다.
② 침입탐지시스템의 구성요소로는 스크린 라우터, 베스천 호스트, 프록시 서버 등이 있다.
③ 호스트기반 IDS는 설치되어 있는 호스트 내의 침입 유형을 탐지한다.
④ 긍정오류(false positive)는 정상적인 행위를 침입으로 오인하여 탐지할 때를 말한다.

8. 공개키 암호화 알고리즘이 아닌 것은?
① ARIA
② RSA(Rivest, Shamir, Adleman)
③ ElGamal
④ ECC(Elliptic Curve Cryptosystem)

9. OECD 개인정보 보안 8원칙에 대한 내용으로 가장 옳지 않은 것은?
① 수집 제한의 원칙 ② 정보 정확성의 원칙
③ 비공개의 원칙 ④ 책임의 원칙

10. DoS(Denial of Service)는 공격 대상이 수용할 수 있는 능력 이상의 정보나 사용자 또는 네트워크의 용량을 초과시켜 정상적으로 작동하지 못하게 하는 공격이다. DoS공격 중 하나인, SYN Flooding에 대한 설명으로 가장 옳은 것은?
① TCP 프로토콜의 3way hand shaking을 이용하여 공격 대상 시스템을 마비시키기 위한 방법으로 클라이언트(공격자)가 SYN+ACK패킷만을 지속적으로 보내는 방법이다.
② 클라이언트(공격자)가 짧은 시간에 많은 수의 SYN 패킷을 서버에 보내 접속을 요청한 후, 클라이언트가 ACK패킷을 보내주지 않는 방법이다.
③ Ping of Death공격으로 클라이언트(공격자)가 ICMP ping을 이용하여 서버에 ACK패킷을 지속적으로 보내는 방법이다.
④ TCP패킷의 시퀀스 번호를 조작하여 서버를 공격하는 방법이다.

11. <보기>에서 설명하는 블록 암호(Block Cipher) 알고리즘은?

<보기>
- 2010년대 국내에서 개발한 경량 고속 블록 암호 알고리즘이다.
- 스마트폰, 사물인터넷 등 저전력 암호화에 널리 쓸 수 있다.
- AES를 개발한 벨기에 루벤대학 COSIC연구소에서 안전성을 검증받았다.

① SEED ② HIGHT ③ LEA ④ IDEA

12. 블록 암호 운용 모드인 CTR 모드에 대한 설명으로 가장 옳지 않은 것은?
① 블록을 암호화할 때마다 1씩 증가해 가는 카운터를 암호화해서 키 스트림을 만들어 낸다.
② 암호화와 복호화가 완전히 같은 구조가 되므로, 프로그램 구현이 간단하다.
③ 블록을 임의의 순서로 처리할 수 있다.
④ 암호화에서는 병렬처리를 할 수 없지만, 복호화에서는 병렬처리가 가능하다.

13. 메시지 인증 코드(MAC)에 대한 설명으로 가장 옳지 않은 것은?
① 일방향 해시 함수를 이용하여 MAC을 만들 수 있다.
② 블록 암호를 이용하여 MAC을 만들 수 있다.
③ 재전송 공격에 대응하기 위해서 순서번호, 타임스탬프, 임의의 비표(nonce) 등을 포함하여 MAC을 만들 수 있다.
④ MAC에는 부인방지 기능이 포함되어 있으나, 제3자에게 증명하는 기능은 포함되어 있지 않다.

14. 싱글 사인 온(SSO)에 대한 설명으로 가장 옳지 않은 것은?
① 하나의 시스템에서 인증을 받으면, 다른 시스템에 대한 접근 권한도 얻게 되는 편리한 인증 시스템이다.
② 기업에서는 회원에 대한 통합관리가 가능해 마케팅을 극대화시킬 수 있다는 장점이 있다.
③ 적절한 권한관리시스템과 함께 사용할 경우, 보안성과 효율성을 갖춘 통합인증시스템으로 활용할 수 있다.
④ 해킹을 통해서 한 번의 인증과정만 통과하면, 모든 시스템에 접속할 수 있다는 단점이 존재하기 때문에 국내에는 도입되지 않고 있다.

15. <보기>에서 DoS 공격에 해당하는 것을 모두 고른 것은?

<보기>
ㄱ. Land Attack ㄴ. 패킷 필터링
ㄷ. SMURF Attack

① ㄴ ② ㄱ, ㄴ ③ ㄱ, ㄷ ④ ㄱ, ㄴ, ㄷ

16. 난수에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 옳게 짝지은 것은?

<보기>
난수(random number)는 암호기술에서 중요한 역할을 담당하고 있다. 특히, 암호기술에 사용 가능한 난수는 다음의 두 가지 성질을 가져야 한다. ___㉠___은 과거의 수열로부터 다음 수를 예측할 수 없다는 성질이고, ___㉡___은 같은 수열을 재현할 수 없다는 성질이다.

	㉠	㉡
①	무작위성	예측 불가능성
②	예측 불가능성	재현 불가능성
③	재현 불가능성	예측 불가능성
④	무작위성	재현 불가능성

17. 일방향 해시함수의 성질로 가장 옳지 않은 것은?
① 정해진 길이의 입력 값을 받아 정해진 길이의 결과 값을 출력한다.
② 일반적으로 빠른 시간 내에 결과 값을 계산할 수 있다.
③ 일반적으로 입력 값이 다르면 결과 값도 다르다.
④ 결과 값으로부터 입력 값을 역산할 수 없다.

18. 「정보통신기반 보호법」 및 동법 시행령에서 규정한 정보통신기반보호위원회에 대한 설명으로 가장 옳지 않은 것은?
① 위원회의 위원장은 행정안전부장관이다.
② 위원회의 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 한다.
③ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.
④ 위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

19. 접근통제 보안 모델에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 옳게 짝지은 것은?

<보기>
___㉠___은 데이터 무결성에 초점을 둔 상업용 모델로서, 비인가자들의 데이터 변형 방지를 목적으로 한다. 주체는 보다 낮은 무결성 수준의 정보를 읽을 수 없고, 보다 높은 무결성 수준의 객체를 수정할 수 없다.
___㉡___도 무결성 모델의 하나로서, 허가받은 사용자가 허가받지 않고 데이터를 수정하는 것을 방지한다. 주체는 단지 허가된 프로그램을 통하여 객체에 접근할 수 있다.

	㉠	㉡
①	Bell-LaPadula Model	Biba Model
②	Biba Model	Bell-LaPadula Model
③	Biba Model	Clark-Wilson Model
④	Clark-Wilson Model	Biba Model

20. 데이터를 도청, 수집해서 데이터를 분석하는 것으로 직접적인 피해를 발생시키지 않는 공격에 해당하는 것은?
① 스니핑 ② 스미싱
③ ARP 스푸핑 ④ DDoS