【정보보호론】

1. 다음에서 설명하는 정보보호의 보안 서비스로 가장 적절한 것은?

> 기관 내부의 중요 데이터를 외부로 전송하는 행위가 탐지된 경우, 전송자가 전송하지 않았음을 주장하지 못하도록 확실한 증거를 제시할 수 있는 보안 서비스이다.

① 무결성(Integrity) ② 가용성(Availability)
③ 기밀성(Confidentiality) ④ 부인방지(non-Repudiation)

2. 암호분석 중 암호기에 접근할 수 있어, 평문 P를 선택하여 이에 대응하는 암호문 C를 얻어 키 K나 평문 P를 추정하여 암호를 해독하는 방법으로 가장 적절한 것은?

① 암호문 단독 공격(COA, Ciphertext Only Attack)
② 기지 평문 공격(KPA, Known Plaintext Attack)
③ 선택 평문 공격(CPA, Chosen Plaintext Attack)
④ 선택 암호문 공격(CCA, Chosen Ciphertext Attack)

3. 대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(Error Propagation)가 발생하는 모드만을 묶은 것으로 가장 적절한 것은? (단, ECB : Electronic Code Book, CBC : Cipher Block Chaining, CFB : Cipher FeedBack, OFB : Output FeedBack)

① CBC, CFB ② CFB, OFB
③ CBC, ECB ④ OFB, ECB

4. 블록 암호 모드의 암호화 수식은 다음과 같다.

블록 암호 모드	암호화 수식
CBC(Cipher Block Chaining)	$C_i = E_K(C_{i-1} \oplus P_i)$
CFB(Cipher FeedBack)	$C_i = E_K(C_{i-1}) \oplus P_i$
CTR(CounTeR mode)	$C_i = E_K(counter) \oplus P_i$

이 모드들의 복호화 수식으로 가장 적절한 것은? (단, P_i : i번째 평문, C_i : i번째 암호문, $E_K(P_i)$: 암호화, $D_K(C_i)$: 복호화, $\oplus$: XOR, K : 키)

	CBC	CFB	CTR
①	$P_i = E_K(C_{i-1}) \oplus C_i$	$P_i = D_K(C_i) \oplus C_{i-1}$	$P_i = D_K((counter) \oplus C_i)$
②	$P_i = D_K(C_i) \oplus C_{i-1}$	$P_i = E_K(C_{i-1}) \oplus C_i$	$P_i = E_K(counter) \oplus C_i$
③	$P_i = C_i \oplus E_K(C_{i-1})$	$P_i = E_K(C_{i-1}) \oplus C_i$	$P_i = E_K(counter) \oplus C_i$
④	$P_i = D_K(C_i) \oplus C_{i-1}$	$P_i = D_K(C_i) \oplus C_{i-1}$	$P_i = D_K((counter) \oplus C_i)$

5. Triple-DES(Data Encryption Standard)에서는 DES 암호화와 복호화를 섞어서 암호화한다. 다음 중 순서를 가장 적절하게 나열한 것은?

① 암호화 → 암호화 → 복호화
② 암호화 → 복호화 → 암호화
③ 복호화 → 암호화 → 복호화
④ 암호화 → 복호화 → 복호화

6. DES(Data Encryption Standard)에서 입력값 $101111_{(2)}$이 다음과 같은 S-Box를 통과할 때 출력값으로 가장 적절한 것은?

S-Box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	07	02	12	05	10	14	01
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

① $0001_{(2)}$ ② $0011_{(2)}$ ③ $0111_{(2)}$ ④ $1110_{(2)}$

7. 전자서명이 제공하는 기능 중 가장 적절하지 **않은** 것은?

① 서명자만이 서명문을 생성할 수 있다.
② 서명자가 전자 서명한 후에는 서명한 사실을 부인할 수 없다.
③ 서명문의 서명자를 확인할 수 있다.
④ 해시값이 포함된 전자서명을 다른 문서에 반복 서명할 수 있다.

8. 메시지 인증 코드(MAC)에 대한 설명 중 가장 적절하지 **않은** 것은?

① 메시지와 송·수신자만이 공유하는 비밀키를 입력받아 생성된다.
② 메시지 무결성 검증이 가능하다.
③ 부인방지(non-Repudiation)를 위해 사용한다.
④ 인증(Authentication)이 가능하다.

9. 다음 중 사용자 인증(User Authentication)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 지식기반 인증의 가장 큰 문제는 오인식(False Acceptance), 오거부(False Rejection)가 존재한다는 것이다.
② 패스워드를 저장할 때 해시를 이용하는데, 안전도를 높이기 위해 솔트(Salt)를 사용한다.
③ 비밀번호로 사용되는 PIN(Personal Identification Number)은 지식기반 인증이다.
④ OTP(One Time Password)는 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.

10. 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로, 객체의 소유자가 접근 여부를 결정하는 접근 통제 정책으로 가장 적절한 것은?

① 강제적 접근 통제(Mandatory Access Control)
② 임의적 접근 통제(Discretionary Access Control)
③ 역할기반 접근 통제(Role Based Access Control)
④ 문맥 의존성 접근 통제(Context-dependent Access Control)

11. 다음에서 설명하는 것으로 가장 적절한 것은?

> · Brewer-Nash 모델이라고도 한다.
> · 이익충돌을 방지하기 위한 모델이다.
> · 서로 대립 관계에 있는 객체 간의 정보 접근을 통제하는 모델이다.

① 벨라파듈라(Bell-Lapadula) 모델
② 비바(Biba) 모델
③ 클락 윌슨(Clark-Wilson) 모델
④ 만리장성(Chinese Wall) 모델

12. 난수의 성질을 분류하는 데 사용되는 항목 중 가장 적절하지 **않은** 것은?

① 무작위성 ② 예측 불가능성
③ 재현 불가능성 ④ 주기성

13. 대칭키 암호화 알고리즘으로만 묶은 것으로 가장 적절한 것은?

① RC4, SKIPJACK, DSA ② DES, Blowfish, LEA
③ DES, ECC, Rabin ④ IDEA, ElGamal, HIGHT

14. 두 소수 p는 3, q는 11이고, 공개키 e는 3, 암호문 C는 3일 때, RSA 암호 알고리즘을 사용하여 평문 P의 값을 구한 것으로 가장 적절한 것은? (단, 개인키 d의 값은 계산될 수 있는 최소의 자연수로 한다.)

① 7 ② 8 ③ 9 ④ 10

15. 다음에서 설명하는 것으로 가장 적절한 것은?

· 인터넷상에서 신용카드를 이용한 상품구매 시 안전한 대금결제 과정 처리를 위해 RSA 암호화와 인증기술을 이용한다. · 전자봉투와 이중서명을 사용한다.

① SET(Secure Electronic Transaction)
② PGP(Pretty Good Privacy)
③ OTP(One Time Password)
④ SSO(Single Sign On)

16. PGP(Pretty Good Privacy)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 공개키의 정당성을 확인하는 방법이다.
② 전자우편에서 프라이버시(Privacy), 무결성(Integrity), 그리고 인증(Authentication)을 제공한다.
③ 인증기관의 인증서가 필요하지 않다.
④ 계층적인 신뢰 구조에 따라 X.509 인증서는 사용할 수 없다.

17. 다음에서 설명하는 SSL 프로토콜로 가장 적절한 것은?

· 연결을 위해 기밀성과 메시지 무결성 서비스를 제공한다. · 신뢰하는 전송서비스를 필요로 하므로 TCP 프로토콜을 사용한다. · 수신된 데이터는 복호화를 하고, MAC을 확인하고, 압축을 풀고, 재조립하여 상위 계층으로 전달한다.

① Handshake 프로토콜
② ChangeCipherSpec 프로토콜
③ Alert 프로토콜
④ Record 프로토콜

18. 다음에서 ㉠, ㉡, ㉢에 들어갈 용어로 가장 적절하게 연결한 것은?

· (㉠) 공격은 패킷 헤더 정보를 조작하여, 올바른 재조합을 불가능하게 만드는 것을 이용한다. · (㉡) 공격 사례로 Trinoo, TFN, Stacheldraht 공격 등이 있다. · (㉢) 공격은 IP 위장과 ICMP의 특성을 이용한다.

	㉠	㉡	㉢
①	Teardrop	DDoS	Smurf
②	Land	DDoS	SYN flooding
③	Boink	SYN flooding	Teardrop
④	Teardrop	SYN flooding	Land

19. 리눅스의 /etc/shadow 파일에서 확인할 수 있는 정보로 가장 적절하지 **않은** 것은?

① 사용자의 UID
② 사용자 계정이 만료되는 날짜
③ 암호를 사용할 수 있는 최대 기간
④ 암호가 마지막으로 변경된 날짜

20. 침입탐지시스템(Intrusion Detection System)에서 가장 적절하지 **않은** 것은?

① 합법적 사용자를 침입자로 판단하게 되는 긍정오류(False Positive)가 발생할 수 있다.
② 침입자를 합법적 사용자로 판단하게 되는 부정오류(False Negative)가 발생할 수 있다.
③ 침입탐지시스템은 데이터 수집원에 따라 네트워크 기반과 호스트 기반 등으로 분류한다.
④ 침입탐지시스템은 패킷을 차단하며, DMZ(DeMilitarized Zone)에서만 설치가 가능하다.