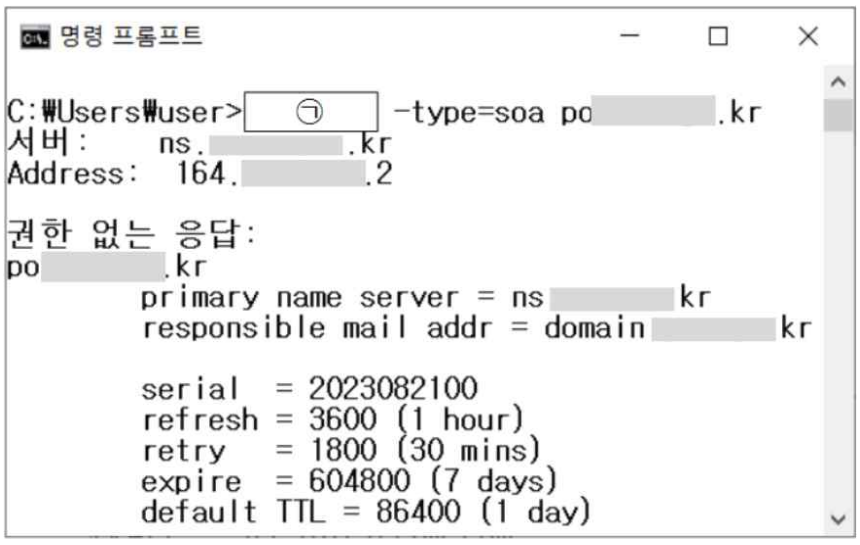
【정보보호론】

1. OSI 7 계층 모델의 네트워크 계층에서 제공하는 보안 서비스로 가장 적절한 것은?
 ① PPTP(Point-to-Point Tunneling Protocol)
 ② SSL(Secure Socket Layer)
 ③ IPSec(IP Security Protocol)
 ④ L2TP(Layer 2 Tunneling Protocol)

2. 스트림 암호에 관한 설명으로 가장 적절하지 **않은** 것은?
 ① 한 번에 1비트 혹은 1바이트의 데이터 흐름을 순차적으로 처리하는 암호 알고리즘을 총칭한다.
 ② 스트림 암호는 하드웨어 구현이 간편하고 속도가 빠르기 때문에 무선 통신 환경에 주로 사용된다.
 ③ 평문과 비밀키를 XOR 연산하여 암호화한다.
 ④ 대표적인 방식으로 RC5, IDEA 등이 있다.

3. OSI 보안 구조 권고안 X.800에서 정의하는 적극적 공격(active attack)에 관한 설명으로 가장 적절하지 **않은** 것은?
 ① 서비스 거부 공격을 한다.
 ② 인증된 사용자로 신분을 위장한다.
 ③ 전송 메시지를 수정한다.
 ④ 네트워크 트래픽을 분석한다.

4. 다음 그림은 DNS 진단 유틸리티 명령어를 실행한 결과의 일부이다. ㉠의 명령어로 옳은 것은?



① route ② ipconfig ③ ping ④ nslookup

5. TCP 프로토콜을 사용하는 서비스명과 일반적인 포트(well-known port) 번호가 바르게 연결된 것은?

	FTP	SMTP	HTTP	Telnet
①	21	25	80	23
②	23	25	80	21
③	21	80	25	23
④	80	23	21	25

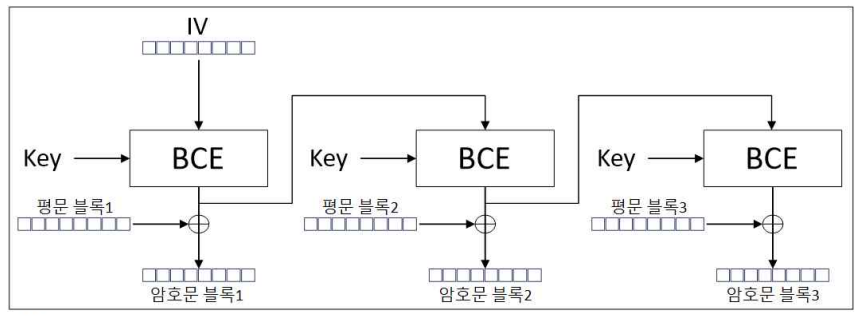
6. 다음 사례에 적용된 정보보호 기법으로 가장 적절한 것은?

> Alice는 우연히 오래된 지도를 발견하였다. 그 지도를 불빛에 비추어 보니, 보물이 숨겨져 있는 위치가 지도에 표시되었다.

 ① 스테가노그래피(steganography)
 ② 시저(caesar) 암호
 ③ 스키테일(scytale) 암호
 ④ 플레이페어(playfair) 암호

7. 클라우드 컴퓨팅에 관한 설명으로 가장 적절하지 **않은** 것은?
 ① 컨테이너(containers) 기술을 이용하면 호스트 운영체제를 공유하기 때문에 각기 다른 게스트 운영체제를 가지는 가상머신에 비해 오버헤드가 적은 이점이 있다.
 ② 클라우드 구현방식에 따른 배치 모델(deployment model) 중에 프라이빗 클라우드(private cloud) 모델은 특정 기관이 내부적으로 구축하여 이용하는 모형이다.
 ③ 클라우드 환경은 온프레미스(on-premises) 환경에 비해 많은 초기 구매 비용이 소요되는 단점이 있다.
 ④ 가상화를 위한 하이퍼바이저(hypervisor)는 각종 하드웨어 자원을 각각의 가상머신에 논리적으로 할당 및 스케줄링하는 기능을 담당한다.

8. 다음 그림은 특정한 블록 암호 운영 모드에 관한 암호화 과정이다. 키 스트림 영향으로 병렬처리가 불가능하고 암호문 블록 오류 발생 시 해당 평문 블록에만 영향을 주어 오류 영향의 전파를 최소화한 모드로 가장 적절한 것은?



** BCE : Block Cipher Encryption | IV : Initialization Vector

 ① ECB(Electronic CodeBook) 모드
 ② CBC(Cipher Block Chaining) 모드
 ③ CFB(Cipher FeedBack) 모드
 ④ OFB(Output FeedBack) 모드

9. RSA(Rivest-Shamir-Adleman) 암호 알고리즘에서 선택된 두 소수 (p, q)는 각각 7과 17이며 암호화 공개키(e)가 5로 선택된 경우, 공개키와 개인키가 바르게 짝지어진 것은?

	공개키={e, N}	개인키={d, N}
①	PU={ 5, 119}	PR={77, 119}
②	PU={77, 119}	PR={ 5, 119}
③	PU={77, 5}	PR={ 5, 77}
④	PU={ 5, 17}	PR={ 5, 119}

10. SHA(Secure Hash Algorithm)에 관한 설명으로 가장 적절하지 **않은** 것은?
 ① SHA-1과 SHA-2의 해시 길이는 모두 다르다.
 ② SHA-1과 SHA-256의 블록 길이는 동일하다.
 ③ SHA-384와 SHA-512의 워드 길이는 동일하다.
 ④ SHA-1과 SHA-512의 단계 수는 서로 다르다.

11. 패스워드 암호화 강도를 높이기 위해 사용하는 첨가값(salt)에 관한 설명으로 가장 적절하지 **않은** 것은?
 ① 사전(dictionary) 공격과 레인보우 테이블(rainbow table) 공격을 효과적으로 막을 수 있다.
 ② 첨가값을 사용하면 전사적(brute-force) 공격에 안전하다.
 ③ 의사난수생성기로 첨가값을 생성한다.
 ④ 비밀번호와 분리하여 안전한 장소에 저장한다.

12. 하이브리드 암호시스템에 관한 설명으로 가장 적절하지 **않은** 것은?

① 대칭키의 키 배송 문제를 공개키 암호로 해결하였다.
② 의사난수생성기, 대칭키 암호, 공개키 암호 기술이 사용된다.
③ 공개키 암호로 속도를 높이고 대칭키 암호로 세션키를 보호한다.
④ 대표적인 사용 예로 PGP(Pretty Good Privacy)가 있다.

13. 다음은 보안 알고리즘의 기능별 지원 여부(O, X)를 나타낸 표이다. ㉠~㉣에 해당하는 것으로 가장 옳게 짝지어진 것은?

알고리즘	암호/복호	디지털서명	키교환
SEED	O	㉠	X
DH(Diffie-Hellman)	㉡	X	O
ECC(Elliptic Curve Cryptography)	O	㉢	O
DSS(Digital Signature Standard)	X	O	㉣

① ㉠(X) ㉡(X) ㉢(O) ㉣(O)
② ㉠(O) ㉡(O) ㉢(X) ㉣(O)
③ ㉠(X) ㉡(X) ㉢(O) ㉣(X)
④ ㉠(X) ㉡(O) ㉢(X) ㉣(O)

14. DES(Data Encryption Standard) 암호화 알고리즘에 관한 설명으로 가장 적절하지 **않은** 것은?

① 암호화를 위한 라운드 함수는 16번의 라운드를 거친다.
② 6비트의 입력값과 4비트의 출력값을 갖는 선형함수로 구성된 8개 S-박스를 사용한다.
③ 라운드 키 생성기(round-key generator)는 48비트 암호화 키로부터 56비트 라운드 키를 생성한다.
④ 대표적인 대칭키 암호화 알고리즘으로 평문의 길이는 64비트 블록으로 구성된다.

15. 다음은 리눅스에서 ls -l 명령어를 실행한 결과이다. 파일의 접근권한을 소유자 외에는 읽기 권한만 부여하는 명령어로 옳은 것은?

```
-rwxrwxrwx 1 AAA BBB 120 Oct 2 10:10 CCC
```

① chmod 666 AAA
② chmod 666 CCC
③ chmod 744 BBB
④ chmod 744 CCC

16. 다음은 통합인증체계(SSO, Single Sign On)를 위한 커버로스(kerberos) 프로토콜에 관한 내용이다. ㉠~㉢에 들어갈 용어가 올바르게 짝지어진 것은?

실제 인증을 수행하는 인증 서버는 KDC(Key Distribution Center)의 부분 서비스로 각 서버와 유일한 (㉠)를 공유한다. 그리고 (㉡)는 인증 서버로부터 인증받은 사용자에게 티켓을 발행하는 서비스를 수행한다. 커버로스에서는 다른 사람이 티켓을 복사하여 실제 사용자로 위장하는 등의 재전송 공격을 막기 위해 발행된 티켓에 시간제한을 두는 (㉢)를 이용한다.

① ㉠ 비밀키 ㉡ AS(Authentication Server) ㉢ 쿠키
② ㉠ 비밀키 ㉡ TGS(Ticket Granting Server) ㉢ 타임스탬프
③ ㉠ 공개키 ㉡ TGS(Ticket Granting Server) ㉢ 쿠키
④ ㉠ 공개키 ㉡ AS(Authentication Server) ㉢ 타임스탬프

17. 시스템 침해 공격 유형 및 소프트웨어에 관한 설명으로 가장 적절하지 **않은** 것은?

① 크리덴셜 스터핑(credential stuffing)은 사전에 다른 곳에서 습득한 아이디나 패스워드로 로그인을 시도하는 공격이다.
② 스니핑 공격(sniffing attack)은 네트워크상에 전송되는 내용을 도청하여 중요한 정보를 가로채는 공격이다.
③ 랜드 공격(land attack)은 인위적으로 송신자 IP 주소 및 포트 주소를 수신자의 IP 주소 및 포트 주소와 같게 설정하여 시스템 부하를 발생시키는 공격이다.
④ 스파이웨어(spyware)는 컴퓨터 내부의 문서나 사진파일, 스프레드시트 등 사용자의 파일들을 암호화하여 파일을 열지 못하도록 한 뒤, 돈을 요구하는 악성 프로그램이다.

18. 네트워크상에서 안전한 개인금융정보 전송을 위한 SET (Secure Electronic Transaction) 프로토콜에 관한 설명으로 가장 적절하지 **않은** 것은?

① 거래인가와 지불기능을 위한 인터페이스 역할을 수행하고 상인의 지불 메시지를 처리하는 장치를 지불 게이트웨이(payment gateway)라고 한다.
② 이중서명은 사용자의 지불정보는 상점에 숨기고 주문정보는 은행에게 숨기는 기능을 제공한다.
③ 암호 프로토콜이 단순하고 RSA 동작으로 프로토콜의 속도가 매우 빠른 장점을 가진다.
④ 카드 소지자에게 전자지갑 소프트웨어를 요구하는 단점을 가진다.

19. 다음에서 설명하는 접근통제 보안 모델로 가장 적절한 것은?

자원마다 보안등급을 부여하는 수학적 접근통제 모델로서 군사용 보안구조의 요구사항을 충족하기 위해 설계되었다. 이 모델은 정보의 기밀성에 따라 보안등급을 구분하여 등급이 높은 정보가 등급이 낮은 사용자에게 유출되지 않도록 통제한다. 기밀성 유지에 매우 강한 특성을 가지지만 가용성과 무결성은 고려하지 않는다.

① Role-Based Model
② Task-Based Model
③ Bell-LaPadula Model
④ Lattice-Based Model

20. 대칭키 암호시스템을 분석하여 대칭키가 190개로 확인되었다. 현재보다 사용 인원을 2배로 확장하면 추가로 필요한 키의 수는 몇 개인가?

① 1,560 ② 590 ③ 380 ④ 190