정보보호론

B형

※ 다음 각 물음에 알맞은 답을 골라 답안지의 같은 번호에 컴퓨터용 수성 사인펜으로 정확히 표기하시오.

정보보호론

1. 다음은 신문 기사의 일부이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?

> **○○ 일보**
>
> ㉠ 은(는) 널리 활용되고 있는 암호화 화폐로서 디지털 비트와 암호화를 이용해 개방된 네트워크에서 결제를 처리하는 수단이다. 가상화폐 지갑은 가상화폐를 관리하고 주고받을 수 있는 일종의 계좌이다. 사용자는 가상화폐를 송금할 때 계좌번호에 해당하는 '공개키(public key)'를 입력하고 송금액을 적은 다음, 계좌 비밀번호에 해당하는 '개인키(private key)'를 사용한다. 최근에는 컴퓨터에 담긴 데이터 파일을 암호화한 뒤 사용자에게 300달러를 ㉠ (으)로 지불하라고 요구하며, 3일 안에 지불하지 않으면 금액은 두 배로 늘어나고, 7일 내에 지불하지 않게 되면 암호화된 파일은 삭제된다고 경고하고 있는 악의적인 공격 사례들이 증가하고 있다.
>
> – 2017년 ○월 ○일자 –

① 비트코인(bitcoin)
② 허니 팟(honey pot)
③ 랜섬웨어(ransomware)
④ 비트 채움(bit padding)

2. 정보보호의 목표와 그에 대한 설명 (가)~(다)를 바르게 짝지은 것은?

> (가) 내부 정보 및 전송되는 정보에 대하여 허가되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 한다.
> (나) 정보에 대한 접근 권한이 있는 사용자가 방해받지 않고 언제든지 정보와 정보시스템을 사용할 수 있도록 보장한다.
> (다) 접근 권한이 없는 사용자에 의해 정보가 변경되지 않도록 보호하여 정보의 정확성과 완전성을 확보한다.

	(가)	(나)	(다)
①	기밀성	가용성	무결성
②	기밀성	무결성	가용성
③	무결성	가용성	기밀성
④	무결성	기밀성	가용성

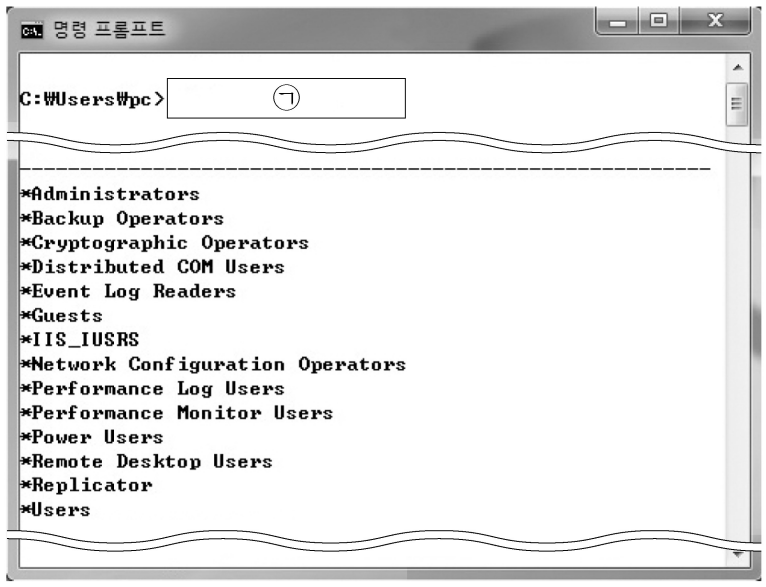
3. 유닉스 시스템에 대한 설명으로 옳지 <u>않은</u> 것은?

① who 명령어는 utmp 로그의 내용을 사용한다.
② wtmp 로그의 내용은 ps 명령어로 확인할 수 있다.
③ 파일의 접근 권한은 ls -l 명령어로 확인할 수 있다.
④ syslog에서 서비스의 동작과 에러를 확인할 수 있다.

4. 암호 시스템의 키 관리에 대한 설명으로 옳은 것은?

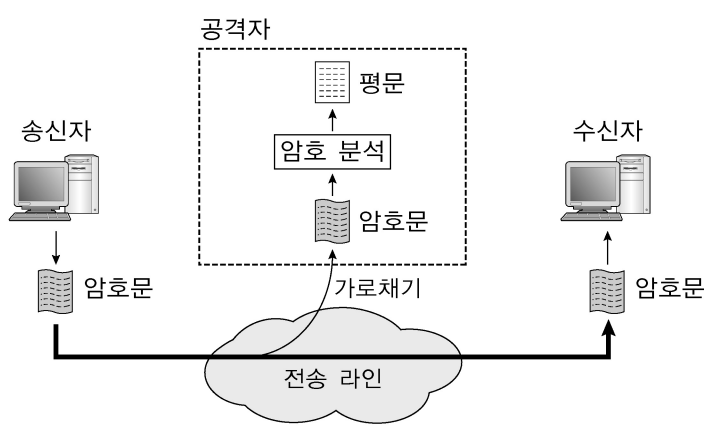
① X.509 인증서는 개인키를 포함한다.
② PKI(Public Key Infrastructure) 환경에서 사용자는 공개키를 생성하여 배포한다.
③ 대칭키를 사용하는 환경에서 키 배포 센터와 구성원 간의 통신은 세션키를 사용한다.
④ PKI 환경에서 공개키 암호를 이용할 경우 CA(Certification Authority)는 인증서를 발급한다.

5. 시스템 관리자는 새로운 사용자를 추가하고 권한을 부여하기 위해 현재 시스템의 그룹을 확인하고자 한다. MS 윈도 명령 프롬프트에서 시스템의 그룹을 확인하기 위한 그림의 빈칸 ㉠에 들어갈 명령어로 옳은 것은?



① net localgroup
② ping localgroup
③ netstat localgroup
④ tracert localgroup

6. 그림에서 공격자의 암호 해독 방법으로 옳은 것은?



① 선택 평문 공격
② 선택 암호문 공격
③ 암호문 단독 공격
④ 알려진(기지) 평문 공격

7. 네트워크 기반의 공격과 그에 대한 설명 (가)~(다)를 바르게 짝지은 것은?

> (가) 대량의 패킷을 이용하여 특정 서비스의 수행을 방해하는 공격
> (나) 네트워크상에서 자신이 아닌 다른 상대방들의 패킷 교환을 도청하는 공격
> (다) 공격자가 자신의 IP(Internet Protocol) 주소를 변조한 후 다른 사용자나 시스템처럼 위장하여 공격

(단, DoS는 Denial of Service의 약어이다.)

	(가)	(나)	(다)
①	DoS	sniffing	spoofing
②	DoS	spoofing	sniffing
③	sniffing	DoS	spoofing
④	spoofing	sniffing	DoS

8. 다음은 디지털 콘텐츠 저작권 보호에 활용되는 기술에 대한 설명이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?

> 디지털 [㉠]은 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다. 이 기술을 사용하면 판매되는 콘텐츠마다 구매자의 정보가 들어 있으므로, 불법적으로 재배포된 콘텐츠 내에서 [㉠]된 정보를 추출하여 구매자를 식별할 수 있다.

① 스미싱(smishing)
② 노마디즘(nomadism)
③ 패러다임(paradigm)
④ 핑거프린팅(fingerprinting)

9. 다음은 SQL 삽입(injection) 공격을 위한 SQL 명령문이다. 빈칸 ㉠에 들어갈 명령어로 옳은 것은?

> [㉠] user_id FROM member WHERE (user_id=' ' OR '1'='1') AND (user_pw=' ' OR '1'='1');
>
> ◦ member: 테이블명
> ◦ user_id: 필드명
> ◦ user_pw: 필드명

① DROP ② CREATE
③ INSERT ④ SELECT

10. 메시지 인증 코드(MAC: Message Authentication Code)를 이용하여 제공할 수 있는 보안 서비스로 옳은 것을 <보기>에서 고른 것은?

<보기>

ㄱ. 트래픽 패딩 ㄴ. 메시지 무결성
ㄷ. 메시지 복호화 ㄹ. 메시지 송신자에 대한 인증

① ㄱ, ㄴ ② ㄱ, ㄷ ③ ㄴ, ㄹ ④ ㄷ, ㄹ

11. 공개키를 이용하는 전자서명에 대한 설명으로 옳지 <u>않은</u> 것은?

① 전자서명은 위조 불가능해야 한다.
② 전자서명은 부인봉쇄(nonrepudiation)에 사용된다.
③ DSS(Digital Signature Standard)는 전자서명 알고리즘이다.
④ 한 문서에 사용한 전자서명은 다른 문서의 전자서명으로 재사용할 수 있다.

12. 침입 탐지 시스템의 탐지 단계를 순서대로 바르게 나열한 것은?

> ㄱ. 데이터 수집(data collection)
> ㄴ. 침입 탐지(intrusion detection)
> ㄷ. 보고 및 대응(reporting and response)
> ㄹ. 데이터 필터링 및 축약(data filtering and reduction)

① ㄱ – ㄴ – ㄷ – ㄹ
② ㄱ – ㄹ – ㄴ – ㄷ
③ ㄹ – ㄴ – ㄱ – ㄷ
④ ㄹ – ㄷ – ㄱ – ㄴ

13. 응용 계층에서 사용되는 보안 프로토콜로 옳은 것을 <보기>에서 고른 것은?

<보기>

ㄱ. FTP ㄴ. PGP ㄷ. S/MIME ㄹ. UDP

① ㄱ, ㄷ ② ㄱ, ㄹ ③ ㄴ, ㄷ ④ ㄴ, ㄹ

14. 일방향 해시 함수(one-way hash function)에 대한 설명으로 옳은 것은?

① 데이터 암호화에 사용된다.
② 주어진 해시값으로 원래의 입력 메시지를 구할 수 있다.
③ 임의 길이의 메시지를 입력받아 고정 길이의 해시값을 출력한다.
④ IDEA(International Data Encryption Algorithm)는 일방향 해시 함수이다.

15. 다음은 방화벽 규칙 집합(rule set)이다. 이에 대한 설명으로 옳은 것은?

정책	출발지(source)		목적지(destination)		동작
	IP 주소	포트	IP 주소	포트	
1	external	any	192.168.100.100	5553	allow
2	any	any	any	any	deny

① 정책 2는 모든 접근에 대하여 허용하는 정책이다.
② 방화벽은 정책 2를 적용한 후 정책 1을 적용하게 된다.
③ 방화벽은 접근제어를 수행하기 위하여 포트만을 사용한다.
④ 외부 IP 주소를 사용하여 접근하는 경우 내부 시스템(192.168.100.100)의 5553번 포트에 접근을 허용한다.

16. 다음의 내용을 목적으로 규정하고 있는 법은?

> **제1조(목적)** 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.

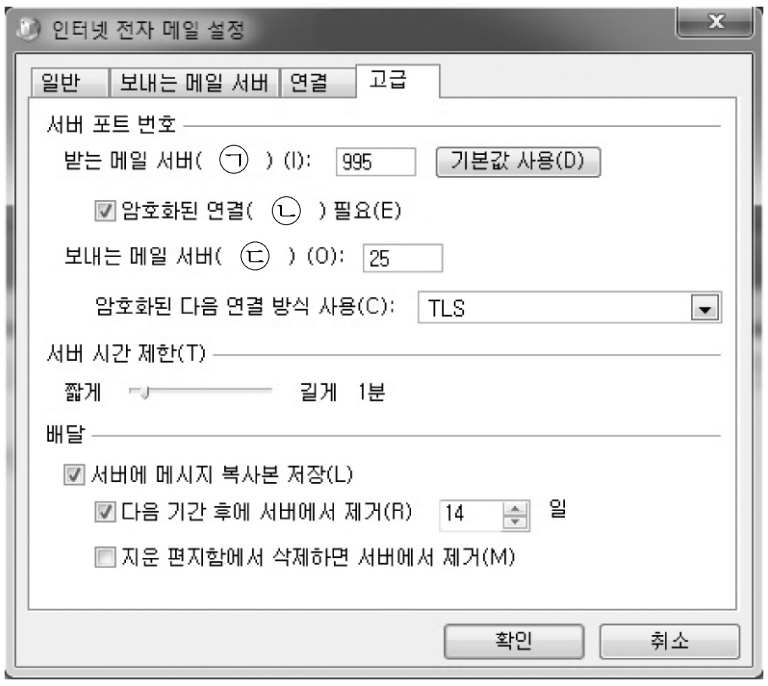
① 개인정보 보호법
② 국가인권위원회법
③ 공공기관의 정보공개에 관한 법률
④ 정보보호 산업의 진흥에 관한 법률

17. 다음은 RSA 공개키 알고리즘에서 공개키와 개인키를 구하는 과정이다. 단계 4의 e 값으로 적절한 것은?

> [알고리즘]
> ◦ 단계 1: 두 소수 $p=5$, $q=11$을 선정한다.
> ◦ 단계 2: $n=p\times q$를 계산한다.
> ◦ 단계 3: $\phi(n)=(p-1)\times(q-1)$을 계산한다.(단, $\phi(n)$은 오일러의 Totient 함수이다.)
> ◦ 단계 4: $\phi(n)$과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
> ◦ 단계 5: $e\times d \bmod \phi(n)=1$의 관계를 갖는 d를 계산한다.(단, mod는 나머지를 구하는 연산자이다.)
> ◦ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

① 12 ② 13 ③ 15 ④ 18

18. 그림은 인터넷 전자 메일 설정 화면이다. ㉠~㉢에 들어갈 프로토콜로 바르게 짝지은 것은?



	㉠	㉡	㉢
①	SSL	POP3	SMTP
②	POP3	SSL	SMTP
③	POP3	SMTP	SSL
④	SMTP	SSL	POP3

19. 다음 설명을 모두 만족하는 암호화 알고리즘은?

> ◦ 공개키 암호 알고리즘이다.
> ◦ 이산대수 문제의 어려움에 기반을 둔다.
> ◦ Diffie-Hellman 키 교환 프로토콜의 확장이다.

① SEED 암호 ② Rabin 암호
③ ElGamal 암호 ④ Blowfish 암호

20. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 내용 중 일부이다. 빈칸 ㉠에 공통으로 들어갈 내용으로 옳은 것은?

> **제45조의3(㉠ 의 지정 등)** ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 ㉠ 을(를) 지정할 수 있다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 ㉠ 을(를) 지정하고 미래창조과학부장관에게 신고하여야 한다.

① 개인정보 처리자 ② 정보보호 담당관
③ 정보보호 정책관 ④ 정보보호 최고책임자