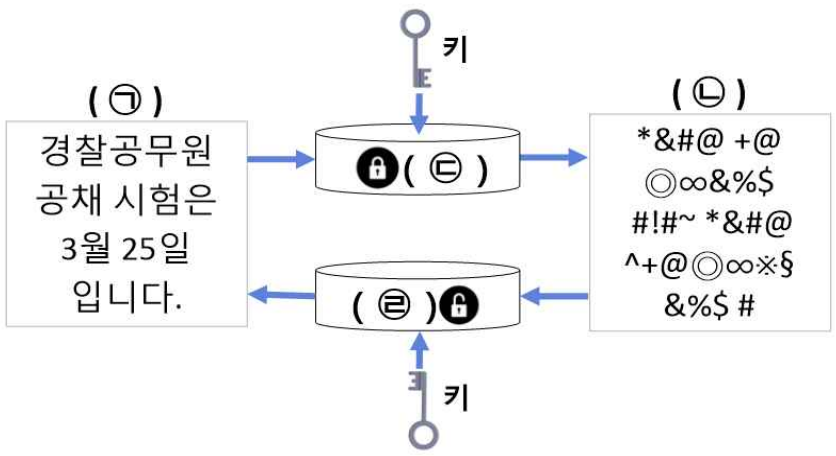
【정보보호론】

1. 다음 그림에서 빈칸 ㉠~㉣에 들어갈 용어를 올바르게 짝지은 것으로 가장 적절한 것은?

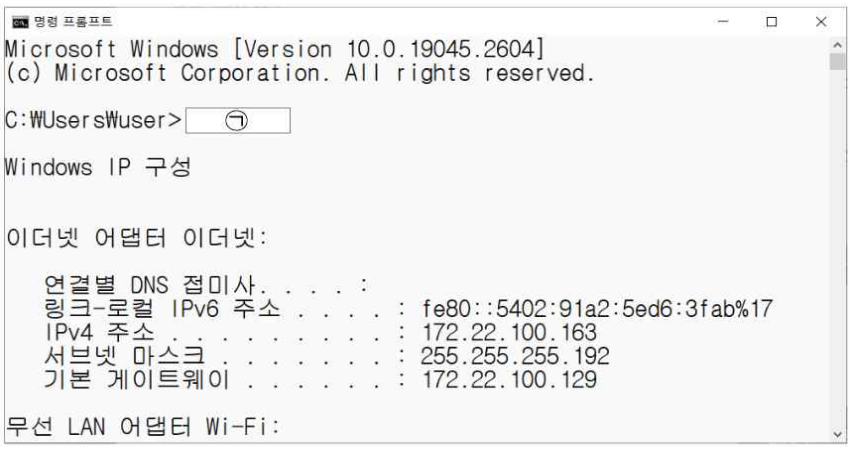


	㉠	㉡	㉢	㉣
①	평문	암호문	암호화	복호화
②	평문	암호문	복호화	암호화
③	암호문	평문	암호화	복호화
④	암호문	평문	복호화	암호화

2. 디지털콘텐츠에 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술로 가장 적절한 것은?

① 홀로그램(hologram)
② 스테가노그래피(steganography)
③ 디지털 사이니지(digital signage)
④ 디지털 핑거프린팅(digital finger printing)

3. 다음 그림은 빈칸 ㉠의 명령어를 실행한 결과의 일부이다. 빈칸 ㉠의 명령어로 옳은 것은?



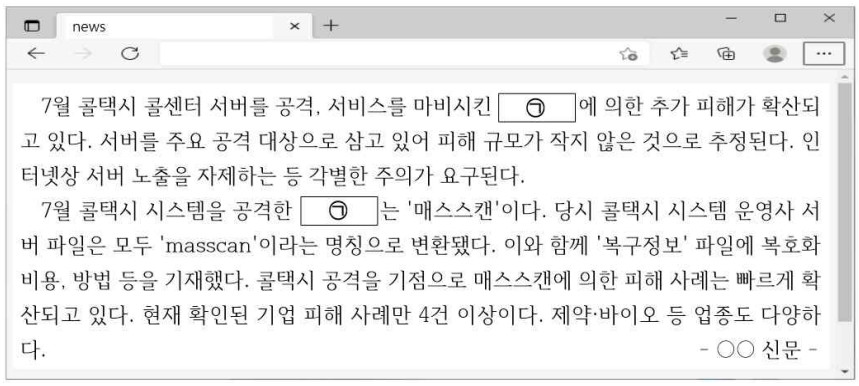
① ping ② protocol ③ ipmask ④ ipconfig

4. 다음 대칭키 암호 운영모드의 암호화 과정에서 병렬처리가 가능한 것을 모두 고른 것은?

㉠ CTR(CounTeR)
㉡ CFB(Cipher-FeedBack)
㉢ CBC(Cipher Block Chaining)
㉣ ECB(Electronic CodeBook)

① ㉠㉡ ② ㉠㉣ ③ ㉡㉢ ④ ㉢㉣

5. 다음은 악성 프로그램에 의한 피해 사례를 보도한 신문 기사이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?



① 애드웨어(adware)
② 라이트웨어(liteware)
③ 스파이웨어(spyware)
④ 랜섬웨어(ransomware)

6. 다음 AES와 RSA 암호화 알고리즘에 관한 설명으로 옳은 것을 모두 고른 것은?

㉠ AES는 56bits 키 크기를 갖는 암호화 알고리즘이다.
㉡ AES는 암호화 키와 복호화 키가 같은 대칭키 암호화 알고리즘이다.
㉢ RSA는 소인수분해 기반의 공개키 암호화 알고리즘이다.
㉣ RSA는 암호화 키와 복호화 키가 다른 대칭키 암호화 알고리즘이다.

① ㉠ ② ㉠㉣ ③ ㉡㉢ ④ ㉡㉢㉣

7. 인증서 폐기 목록(CRL, Certificate Revocation List)에 관한 설명으로 가장 적절하지 **않은** 것은?

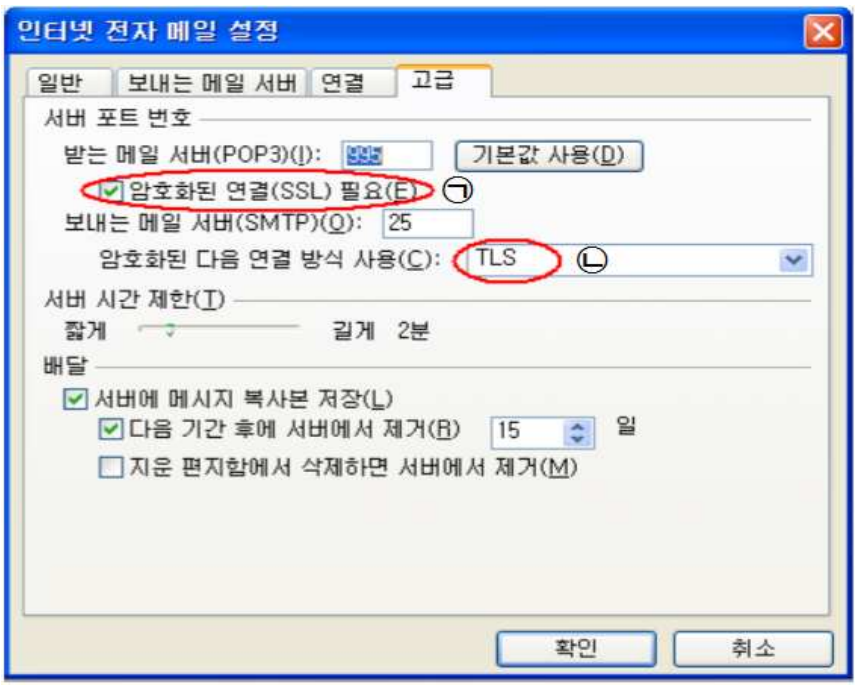
① CRL은 더 이상 사용할 수 없는 인증서들의 목록이다.
② 인증서를 발행한 인증기관(CA)은 정기적으로 CRL을 발행한다.
③ Version, Authority key identifier는 CRL의 기본 필드이다.
④ Issuer alternative name, CRL number는 CRL의 확장 필드이다.

8. DES(Data Encryption Standard)에서 입력값 $101100_{(2)}$이 다음 S-Box를 통과할 때 출력값으로 옳은 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 $0011_{(2)}$ ② $0111_{(2)}$ ③ $1000_{(2)}$ ④ $1111_{(2)}$

9. 다음 그림은 인터넷 전자메일 설정화면이다. ㉠과 ㉡에 관한 설명으로 가장 적절하지 **않은** 것은?



① ㉠의 SSL과 ㉡의 TLS는 기밀성, 무결성, 인증을 보장하는 프로토콜이다.

② ㉠의 SSL과 ㉡의 TLS는 메일 송·수신을 위한 SMTP, POP3, IMAP4 프로토콜의 상위계층에 위치한다.

③ ㉠의 SSL과 ㉡의 TLS는 대칭키 암호화 알고리즘을 이용해서 기밀성을 제공하고, 메시지 인증코드를 이용하여 메시지 무결성을 제공한다.

④ ㉡의 TLS는 ㉠의 SSL 3.0을 기반으로 IETF가 만든 프로토콜로서 클라이언트-서버 환경에서 TCP 기반의 애플리케이션에 대한 보안 서비스를 제공한다.

10. SSO(Single Sign On)의 구성요소에 관한 설명으로 가장 적절하지 **않은** 것은?

① 인증 서버는 ACL을 통한 통합 인증 서비스를 제공한다.

② SSO Agent는 각 정보시스템에 자동 인증 정보를 송·수신한다.

③ LDAP는 네트워크 자원을 식별하고, 사용자와 애플리케이션들이 자원에 접근할 수 없도록 하는 네트워크 디렉토리 서비스이다.

④ 사용자는 SSO를 구현한 포털(Portal)에 자신의 ID와 Password로 한 번만 로그인하면 연동된 시스템에 재인증 절차없이 편리하게 접근할 수 있다.

11. 다음 C언어 소스 코드를 실행할 때 발생하는 시스템 자원 고갈 공격으로 가장 적절한 것은?

```
#include <stdio.h>
#include <stdlib.h>

void main()
{
   char *chM;
   while(1)
      chM = (char *)malloc(1000);
}
```

① 가용 메모리 자원 고갈 공격

② 가용 디스크 자원 고갈 공격

③ 가용 프린터 자원 고갈 공격

④ 가용 네트워크 자원 고갈 공격

12. 커버로스(Kerberos)의 구성요소에 관한 설명으로 가장 적절하지 **않은** 것은?

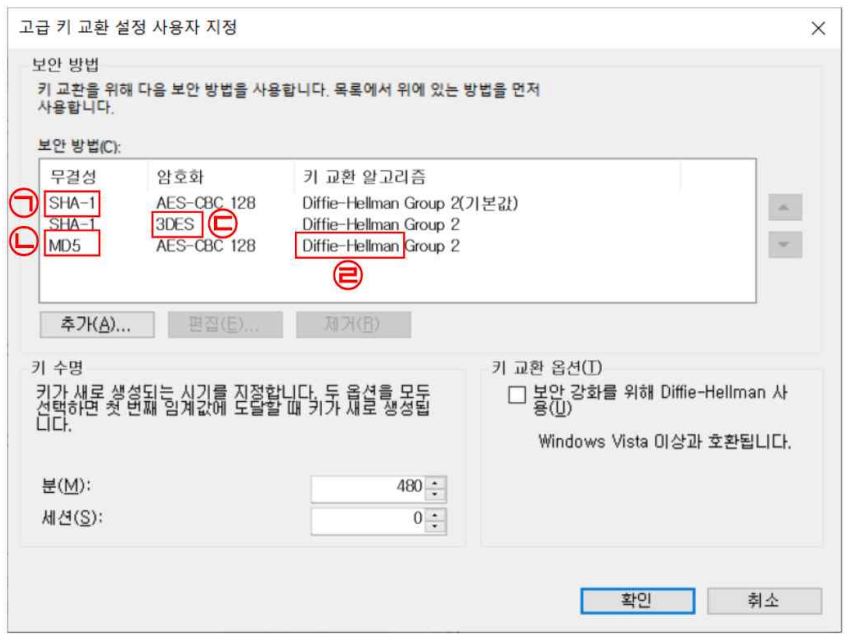
① Ticket은 사용자의 인증을 확인하는 토큰이다.

② TGS(Ticket Granting Service)는 모든 사용자에게 Ticket을 발행한다.

③ AS(Authentication Service)는 각 서버와 유일한 비밀키를 공유한다.

④ KDC(Key Distribution Center)는 모든 사용자와 서비스의 비밀키를 보관한다.

13. 다음 그림은 Windows Defender 방화벽의 IPsec 설정화면이다. ㉠~㉣에 관한 설명으로 가장 적절하지 **않은** 것은?



① ㉠ SHA-1의 해시값 길이는 160bits 이다.

② ㉡ MD5의 해시값 길이는 128bits 이다.

③ ㉢ 3DES는 256bits의 키 크기를 갖는 일방향 해시함수이다.

④ ㉣ Diffie-Hellman은 두 사용자 간에 공통키를 안전하게 공유할 수 있는 키 교환 알고리즘이다.

14. 다음은 네트워크 공격에 대한 설명이다. 빈칸 ㉠에 들어갈 용어로 옳은 것은?

> 스니핑 공격의 주된 종류로는 ARP 우회공격(ARP redirect), ICMP 우회공격(ICMP redirect), 포트 미러링(Port mirroring), 스위치 재밍(Switch Jamming) 등이 있다.
>
> [㉠] 공격은 위조된 매체 접근 제어(MAC) 주소를 지속적으로 네트워크로 흘려보내 스위치 저장 기능을 혼란시켜 더미 허브(dummy hub)처럼 작동토록 하는 공격이다.
>
> 스위치를 직접 공격하며, MAC 테이블을 위한 캐시 공간에 버퍼 오버플로우 공격을 실시하는 것과 같다. 스위치는 자신이 가지고 있는 MAC 테이블 저장 공간이 가득 차면 네트워크 패킷을 브로드캐스트하는 특성이 있는데 이를 이용한 공격 방법이라고 할 수 있다.

① ARP 우회공격(ARP redirect)

② ICMP 우회공격(ICMP redirect)

③ 포트 미러링(Port mirroring)

④ 스위치 재밍(Switch Jamming)

15. 사물인터넷에 사용되는 무선통신 프로토콜로 가장 적절하지 **않은** 것은?

① NFT ② LoRA ③ ZigBee ④ Bluetooth

16. i-PIN(Internet Personal Identification Number)에 관한 설명으로 가장 적절하지 **않은** 것은?

① i-PIN 노출시 폐지/신규 발급이 가능하다.
② 주민등록번호 유출의 위험을 예방할 수 있다.
③ 주민등록번호는 개별 웹사이트에 저장된다.
④ 신원 확인 후 본인 확인 기관에서 i-PIN을 발급한다.

17. 다음 설명에 해당하는 것으로 가장 적절한 것은?

• 시스템에 설치되어 그 존재의 흔적을 최대한 숨기면서 공격자가 언제든지 시스템에 관리자 권한으로 접근할 수 있도록 비밀통로를 지속적으로 유지 시켜 주는 프로그램 집합이다. • 프로세스/스레드 감추기, 프로세스 보안 설정 변경 및 제거, 파일/폴더 감추기, 레지스트리/서비스 감추기 등의 기능을 가진다.

① 쿠키(cookie)　② 루트킷(rootkit)
③ 스파이웨어(spyware)　④ 블록체인(blockchain)

18. 국내에서 개발한 암호 알고리즘에 관한 설명으로 가장 적절하지 **않은** 것은?

① ARIA(Academy Research Institute Agency)는 ISPN 구조의 128bits 블록 암호로 키의 길이에 따라 ARIA-128, ARIA-192, ARIA-256으로 구분한다.
② HIGHT(HIGh security and light weigHT)는 비교적 간단한 연산으로 빠른 암호화 복호화 기능을 제공하며 32bits, 64bits, 128bits 블록 크기를 가진 블록 암호 알고리즘이다.
③ LEA(Lightweight Encryption Algorithm)는 128bits 경량 블록 암호 알고리즘으로 스마트폰 보안, 사물인터넷(IoT) 등 저전력 암호화에 널리 사용된다.
④ SEED는 암호전문가들이 개발한 알고리즘으로 2005년 국제표준화기구인 ISO/IEC 및 IETF에서 국제 블록 암호 알고리즘 표준으로 제정되었다.

[19~20] 다음은 암호 알고리즘의 키 쌍 생성 과정이다. 물음에 답하시오.

- 공개키 : E, N
- 개인키 : D, N
- 최소공배수(LCM, Least Common Multiple)
- 최대공약수(GCD, Greatest Common Division)

단계 1 : N을 구한다.
의사난수 생성기로 p와 q를 구한다.　(p와 q는 소수) $N = p \times q$
단계 2 : L을 구한다.
$L = LCM(p-1, q-1)$　(L은 p-1과 q-1의 최소공배수)
단계 3 : E를 구한다.
$1 < E < L$ $GCD(E, L) = 1$
단계 4 : D를 구한다.
$1 < D < L$ $E \times D \bmod L = 1$

19. 위의 키 쌍 생성 과정을 적용한 암호 알고리즘으로 가장 적절한 것은?

① ECC　② RSA　③ ElGamal　④ Diffie-Hellman

20. 다음과 같이 값과 식이 주어질 때 위의 암호 알고리즘의 키 쌍 생성 과정에 따라 평문 M을 암호화한다. 암호문 C의 값으로 옳은 것은?

p=3,　q=11　E=7,　평문 M=4,　암호문 C = ?

① 13　② 14　③ 15　④ 16