

2023년10월29일년 인터넷보안전문가 2급 필기시험 기출문제 답안

【1과목 : 10문제】 정보보호개론	1	2	3	4	5	6	7	8	9	10
	④	④	④	②	③	①	②	②	③	④
【2과목 : 20문제】 운영체제	11	12	13	14	15	16	17	18	19	20
	④	②	③	①	③	④	③	①	④	④
	21	22	23	24	25	26	27	28	29	30
	②	③	④	①	①	②	③	④	②	③
【3과목 : 15문제】 네트워크	31	32	33	34	35	36	37	38	39	40
	③	②	②	①	④	④	④	③	①	②
	41	42	43	44	45					
	③	④	①	④	④					
【4과목 : 15문제】 보안	46	47	48	49	50	51	52	53	54	55
	②	④	③	②	②	④	②	④	③	④
	56	57	58	59	60					
	②	②	①	④	④					

전자문제집 CBT 홈페이지 : <https://www.cbtestpro.kr>

최신 수정 자료와 해설(오타 • 오답 • 규정변경)은 cbtestpro.kr 웹 및 앱에서 확인하세요.

기출문제의 저작권은 출제기관에 있습니다. cbtestpro.kr 및 관련 앱에서는 편집 및 재구성 작업만 하였음을 밝힙니다.



전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!



【1과목】 정보보호개론 (10문제)

1. IPSec 프로토콜에 대한 설명으로 옳지 않은 것은?

- ① 네트워크 계층인 IP 계층에서 보안 서비스를 제공하기 위한 보안 프로토콜이다.
- ② IP 스푸핑(Spoofing)이나 IP 스니핑(Sniffing)을 방지할 수 있다.
- ③ 인증, 무결성, 접근제어, 기밀성, 재전송 방지 등의 서비스를 제공한다.

④ 키 관리는 수동으로 키를 입력하는 수동방법(Manual)만이 존재한다.

2. 공개키 암호 알고리즘에 관한 설명 중 옳지 않은 것은?

- ① 공개키 암호화 방식은 암호화와 복호화하는데 비밀키와 공개키라는 서로 다른 두 개의 키를 사용한다.
- ② 공개키는 일반인에게 공개하고 비밀키는 오직 자신만이 알도록 한다.
- ③ 데이터 암호화 및 수신된 데이터의 부인 봉쇄 그리고 전자 서명에 있어서 효율적이다.

④ 비공개키 암호 알고리즘보다 암호화와 복호화 속도가 빠르고 키의 길이가 대칭키 알고리즘보다 작다.

3. 전용 해시 알고리즘 중 해시값을 128비트에서 256비트까지 32비트 단위로 가변적으로 할 수 있고, 라운드 수 역시 3에서 5사이를 선택할 수 있는 것은?

- ① MD4
- ② MD5
- ③ SHA-1
- ④ HAVAL

4. DES(Data Encryption Standard)에 대한 설명 중 옳지 않은 것은?

- ① 1970년대 초 IBM이 개발한 알고리즘이다.
- ② 2048 비트까지의 가변 키 크기가 지원되고 있다.
- ③ 미국표준기술연구소(NIST)에 의해 암호화 표준으로 결정됐다.
- ④ 암호화 방식의 전자 코드 복과 암호 피드백으로 이루어졌다.

5. 다음 중 암호화 알고리즘 성격이 다른 하나는?

- ① DES
- ② Skipjack
- ③ RSA
- ④ FEAL

6. 인적자원에 대한 보안 위협을 최소화하기 위한 방법으로 옳지 않은 것은?

기밀 정보를 열람해야 하는 경우에는 반드시 정보 담당자 한 명에게만 전담시키고 폐쇄된 곳에서 정보를 열람 시켜 정보 유출을 최대한 방지한다.

기밀 정보를 처리할 때는 정보를 부분별로 여러 명에게 나누어 업무를 처리하게 함으로써 전체 정보를 알 수 없게 한다.

보안 관련 직책이나 서버 운영 관리자는 순환 보직제를 실시하여 장기 담당으로 인한 정보 변조나 유출을 막는다.

프로그래머가 운영자의 직책을 중임하게 하거나 불필요한 외부 인력과의 접촉을 최소화 한다.

7. 보안과 관련된 용어의 정의나 설명으로 옳지 않은 것은?

① 프락시 서버(Proxy Server) - 내부 클라이언트를 대신하여 외부의 서버에 대해 행동하는 프로그램 서버

패킷(Packet) - 인터넷이나 네트워크상에서 데이터 전송을 위해 처리되는 기본 단위로 모든 인터페이스에서 항상 16KB의 단위로 처리

③ 이중 네트워크 호스트(Dual-Homed Host) - 최소한 두 개의 네트워크 인터페이스를 가진 범용 컴퓨터 시스템

④ 호스트(Host) - 네트워크에 연결된 컴퓨터 시스템

8. 다음 내용은 보안 운영체제의 특정한 보안기능에 대해 설명한 것이다. 어떤 기능인가?

일반적으로 보안 관련 사건 기록의 유지를 포함하며, 발생한 각각의 사건과 관련된 사용자의 정보가 수록된다. 모든 보안 관련 사건은 반드시 이 기록부(log file)에 기록되어야 한다. 또한 이 기록부는 명백하게 보호 되어야 한다.

① 사용자 식별 또는 인증

② 감사 및 감사 기록

③ 강제적/임의적 접근 통제

④ 침입탐지

9. 시스템관리자가 사용자의 인증을 위한 사용자 ID 발급 시에 주의할 점으로 옳지 않은 것은?

- ① 시스템에 의해 식별 될 수 있는 유일한 사용자 ID를 발급해야 한다.
- ② 사용자 ID와 패스워드의 두 단계 인증을 하는 ID를 발급해야 한다.
- ③ 일정기간 후에는 개별 사용자의 의지와는 관계없이 사용자 ID를 변경함을 제시한다.
- ④ 시스템에 허용되는 접근의 종류는 반드시 제시해야 한다.

10. 응용계층 프로토콜로 옳지 않은 것은?

- ① SMTP
- ② FTP
- ③ Telnet
- ④ TCP

【2과목】 운영체제 (20문제)

11. 파일 시스템의 기능으로 옳지 않은 것은?

- ① 여러 종류의 접근 제어 방법을 제공
- ② 파일의 생성, 변경, 제거
- ③ 파일의 무결성과 보안을 유지할 수 있는 방안 제공
- ④ 네트워크 제어

12. SSL 레코드 계층의 서비스를 사용하는 세 개의 특정 SSL 프로토콜 중의 하나이며 메시지 값이 '1'인 단일 바이트로 구성되는 것은?

- ① Handshake 프로토콜
- ② Change cipher spec 프로토콜
- ③ Alert 프로토콜
- ④ Record 프로토콜

13. Linux의 기본 디렉터리에 해당하지 않는 것은?

- ① /etc
- ② /root
- ③ /grep
- ④ /home

14. Linux 명령어에 대한 설명으로 옳지 않은 것은?

- ① ls : 디렉터리를 변경할 때 사용한다.
- ② cp : 파일을 다른 이름으로 또는 다른 디렉터리로 복사할 때 사용한다.
- ③ mv : 파일을 다른 파일로 변경 또는 다른 디렉터리로 옮길 때 사용한다.
- ④ rm : 파일을 삭제할 때 사용한다.

15. Linux에서 주어진 명령이나 유틸리티의 매뉴얼을 출력하기 위해 사용되는 명령어는?

- ① ps
- ② fine
- ③ man
- ④ ls

16. 사용자 그룹을 생성하기 위해 사용되는 Linux 명령어는?

- ① groups
- ② mkgroup
- ③ groupstart
- ④ groupadd

17. 퍼미션(Permission)에 대한 설명 중 옳지 않은 것은?

- ① 파일의 그룹 소유권을 바꾸기 위한 명령은 chgrp이다.
- ② 파일의 접근모드를 바꿀때는 chmod이다.
- ③ 모두가 사용할 수 있게 할려면 666이다.
- ④ 파일의 소유권을 다른 사람에게 변경할때는 chown이다.

18. Linux에서 VI(Visual Interface) 명령어 중 변경된 내용을 저장한 후 종료하고자 할 때 사용해야 할 명령어는?

- ① :wq
- ② :q!
- ③ :e!
- ④ \$

19. 일반적으로 다음 설명에 해당하는 프로세스는?

- 백그라운드로 실행한다.
- 고유한 기능에 해당되는 이벤트가 발생되면 동작한다.
- 서비스를 제공한 다음 대기 상태로 돌아간다.
- 시스템 서비스를 지원하는 프로세스이다.
- 서버의 역할을 수행하거나 그 기능을 도와준다.

- ① Shell
- ② Kernel
- ③ Program
- ④ Deamon

20. 이메일에서 주로 사용하는 프로토콜로 옳지 않은 것은?

- ① SMTP
- ② POP3
- ③ IMAP
- ④ SNMP

21. Linux에서 현재 위치한 디렉터리를 표시해 주는 명령어는?

- ① mkdir
- ② pwd
- ③ du
- ④ df

22. Windows Server 환경에서 기본 그룹계정의 설명 중 옳지 않은 것은?

- ① Users - 시스템 관련 사항을 변경할 수 없는 일반 사용자
- ② Administrators - 컴퓨터/도메인에 모든 액세스 권한을 가진 관리자
- ③ Guest - 파일을 백업하거나 복원하기 위해 보안 제한을 변경할 수 있는 관리자
- ④ Power Users - 일부 권한을 제외한 관리자 권한을 가진 고급 사용자

23. DHCP(Dynamic Host Configuration Protocol) Scope 범위 혹은 주소 풀(Address Pool)을 만드는데 주의할 점에 속하지 않는 것은?

- ① 모든 DHCP 서버는 최소한 하나의 DHCP 범위를 가져야 한다.
- ② DHCP 주소 범위에서 정적으로 할당된 주소가 있다면 해당 주소를 제외해야 한다.
- ③ 네트워크에 여러 DHCP 서버를 운영할 경우에는 DHCP 범위가 겹치지 않아야 한다.
- ④ 하나의 서브넷에는 여러 개의 DHCP 범위가 사용될 수 있다.

24. Windows Server에서 FTP 서비스에 대한 설명으로 옳지 않은 것은?

- ① 웹 사이트가 가지고 있는 도메인을 IP Address로 바꾸어 주는 서비스를 말한다.
- ② IIS에서 기본적으로 제공하는 서비스이다.
- ③ 기본 FTP 사이트는 마우스 오른쪽 버튼을 눌러 등록정보를 수정할 수 있다.
- ④ FTP 서비스는 네트워크를 통하여 파일을 업로드 및 다운로드 할 수 있는 서비스를 말한다.

25. Linux의 어떤 파일에 처음부터 끝까지 문자열 'her'를 문자열 'his'로 치환하되, 치환하기 전에 사용자에게 확인하여 사용자가 허락하면(y를 입력하면) 치환하고, 사용자가 허용하지 않으면 치환하지 않도록 하는 vi 명령어는?

- ① :1,\$s/her/his/gc
- ② :1,\$r/her/his/gc
- ③ :1,\$s/his/her/g
- ④ :1,\$r/his/her/g

26. Linux에서 사용자의 'su' 명령어 시도 기록을 볼 수 있는 로그는?

- ① /var/log/secure
- ② /var/log/messages
- ③ /var/log/wtmp
- ④ /var/log/lastlog

27. Linux 콘솔 상에서 네트워크 어댑터 'eth0'을 'ifconfig' 명령어로 '192.168.1.1' 이라는 주소로 사용하고 싶을 때 올바른 방법은?

- ① ifconfig eth0 192.168.1.1 activate
- ② ifconfig eth0 192.168.1.1 deactivate
- ③ ifconfig eth0 192.168.1.1 up
- ④ ifconfig eth0 192.168.1.1 down

28. Linux에서 이미 내린 shutdown 명령을 취소하기 위한 명령어는?

- ① shutdown -r
- ② shutdown -h
- ③ cancel
- ④ shutdown -c

29. Linux에서 'shutdown -r now' 와 같은 효과를 내는 명령어는?

- ① halt
- ② reboot
- ③ restart
- ④ poweroff

30. Linux 시스템 파일의 설명으로 옳지 않은 것은?

- ① /etc/passwd - 사용자 정보 파일
- ② /etc/fstab - 시스템이 시작될 때 자동으로 마운트 되는 파일 시스템 목록
- ③ /etc/motd - 텔넷 로그인 전 나타낼 메시지
- ④ /etc/shadow - 패스워드 파일

【3과목】 네트워크 (15문제)

31. 라우터 명령어 중 NVRAM에서 RAM으로 configuration file 을 copy하는 명령어는?

- ① copy flash start
- ② copy running-config startup-config
- ③ copy startup-config running-config
- ④ wr mem

32. IP Address '172.16.0.0'인 경우에 이를 14개의 서브넷으로 나누어 사용하고자 할 경우 서브넷 마스크는?

- ① 255.255.228.0
- ② 255.255.240.0
- ③ 255.255.248.0
- ④ 255.255.255.248

33. TCP와 UDP의 차이점 설명으로 옳지 않은 것은?

- ① 데이터 전송형태로 TCP는 Connection Oriented방식 이고 UDP는 Connectionless방식이다.
- ② TCP가 UDP보다 데이터 전송 속도가 빠르다.
- ③ TCP가 UDP보다 신뢰성이 높다.
- ④ TCP가 UDP에 비해 각종 제어를 담당하는 Header 부분이 커진다.

34. IP Address는 알고 MAC Address를 모를 경우 데이터 전송을 위해 Datalink 계층인 MAC Address를 알아내는 Protocol 은?

- ① ARP
- ② RARP
- ③ ICMP
- ④ IP

35. 다음 중 IP Address관련 기술들에 대한 설명으로 옳지 않은 것은?

- DHCP는 DHCP서버가 존재하여, 요청하는 클라이언트
- ① 들에게 IP Address, Gateway, DNS 등의 정보를 일괄 적으로 제공하는 기술이다.
- ② 클라이언트가 DHCP 서버에 DHCP Request를 보낼 때 브로드캐스트로 보낸다.
- ③ 192.168.10.2는 사설 IP Address이다.

- ④ 공인 IP Address를 다른 공인 IP로 변환하여 내보내는 기술이 NAT이다.

36. 다음 203.214.3.0/26 Subnet의 호스트에 사용할 수 있는 IP Address로 맞는 것은?

- ① 203.214.3.0
- ② 203.214.3.64
- ③ 203.214.3.63
- ④ 203.214.3.1

37. 다음 중에서 C Class인 IP Address는?

- ① 191.234.56.34
- ② 125.76.133.234
- ③ 131.15.45.120
- ④ 192.168.17.34

38. 다음 중 OSI 7 Layer의 각 Layer 별 Data 형태로서 옳지 않은 것은?

- ① Transport Layer : Segment
- ② Network Layer : Packet
- ③ Datalink Layer : Fragment
- ④ Physical Layer : bit

39. TCP 헤더 필드의 내용으로 옳지 않은 것은?

- ① TTL(Time To Live)
- ② 발신지 포트번호
- ③ 윈도우 크기
- ④ Checksum

40. 자신의 물리 주소(MAC Address)는 알고 있으나 자신의 IP Address를 모르는 호스트가 요청 메시지를 브로드 캐스팅하고, 이의 관계를 알고 있는 서버가 응답 메시지에 IP 주소를 되돌려 주는 프로토콜은?

- ① ARP(Address Resolution Protocol)
- ② RARP(Reverse Address Resolution Protocol)
- ③ ICMP(Internet Control Message Protocol)
- ④ IGMP(Internet Group Management Protocol)

41. 네트워크 관리자나 라우터가 IP 프로토콜의 동작 여부를 점검하고, 호스트로의 도달 가능성을 검사하기 위한 ICMP 메시지 종류는?

- ① Parameter Problem
- ② Timestamp Request/Response
- ③ Echo Request/Response
- ④ Destination Unreachable

42. 다음 프로토콜 중 OSI 7 Layer 계층이 다른 프로토콜은?

- ① ICMP(Internet Control Message Protocol)
- ② IP(Internet Protocol)
- ③ ARP(Address Resolution Protocol)
- ④ TCP(Transmission Control Protocol)

43. 통신 에러제어는 수신측이 에러를 탐지하여 송신자에게 재전송을 요구하는 ARQ(Automatic Repeat Request)를 이용하게 된다. ARQ 전략으로 옳지 않은 것은?

- ① Windowed Wait and Back ARQ
- ② Stop and Wait ARQ
- ③ Go Back N ARQ
- ④ Selective Repeat ARQ

44. Broadcast and Multicast의 종류와 그에 대한 설명으로 옳지 않은 것은?

- ① Unicast - 메시지가 임의의 호스트에서 다른 호스트로 전송되는 방식을 말한다.
- ② Broadcast - 메시지가 임의의 호스트에서 네트워크상의 모든 호스트에 전송되는 방식을 말한다.
- ③ Multicast - 메시지가 임의의 호스트에서 네트워크 상의 특정 호스트(Group)에 전송되는 방식을 말한다
- ④ Broadcast - 메시지가 네트워크 상의 모든 호스트로부터 임의의 호스트에 전송되는 방식을 말한다.

45. TCP/IP 프로토콜을 이용해 클라이언트가 서버의 특정 포트에 접속하려고 할 때 서버가 해당 포트를 열고 있지 않다면 응답 패킷의 코드 비트에 특정 비트를 설정한 후 보내 접근할 수 없음을 통지하게 된다. 다음 중 연결 문제 등의 상황 처리를 위한 특별한 초기화용 제어 비트는?

- ① SYN
- ② ACK
- ③ FIN
- ④ RST

【4과목】 보안 (15문제)

46. 다음은 어떤 보안 도구를 의미하는가?

회사의 사설 네트워크와 외부의 공중 네트워크 사이의 중립 지역으로써 삽입된 컴퓨터 호스트 또는 소형 네트워크를 말한다.

- ① IDS
- ② DMZ
- ③ Firewall
- ④ VPN

47. 다음 빈칸 []에 들어갈 용어는?

사용자가 원격 호스트에서 접속하며 ftp나 telnet 서비스를 이용할 경우, 데이터는 암호화되지 않는 상태로 전송된다. 이러한 데이터는 네트워크상에서 제3자의 네트워크 패킷도청에 그대로 노출된다. 즉, 제3자는 귀중한 데이터나 패스워드를 쉽게 얻을 수 있다. []은/는 원격 호스트로 전송되는 데이터를 Triple DES, IDEA나 RSA로 암호화함으로써 제3자의 네트워크 패킷도청으로부터 데이터를 보호한다.

① SSL(Secure Socket Layer)

② Nessus

③ HostSentry

④ SSH(Secure Shell)

48. Windows 명령 프롬프트 창에서 'netstat -an'을 실행한 결과이다. 옳지 않은 것은?(단, 로컬 IP Address는 211.116.233.104 이다.)

```
c:\W>netstat -an

TCP 127.0.0.1:80 127.0.0.1:1197 TIME_WAIT
TCP 127.0.0.1:80 127.0.0.1:1200 ESTABLISHED
TCP 127.0.0.1:1200 127.0.0.1:80 ESTABLISHED
TCP 211.116.233.104:139 0.0.0.0:0 LISTENING
TCP 211.116.233.104:22 211.116.233.98:22 ESTABLISHED
TCP 211.116.233.104:23 211.116.233.124:2212 TIME_WAIT
```

① http://localhost로 접속하였다.

② NetBIOS를 사용하고 있는 컴퓨터이다.

③ 211.116.233.124에서 Telnet 연결이 이루어져 있다.

④ 211.116.233.98로 ssh를 이용하여 연결이 이루어져 있다.

49. Linux 명령어 중 '/var/log/utmp'와 '/var/log/wtmp'를 모두 참조하는 명령어는?

① lastlog

② last

③ who

④ netstat

50. 라우터에 포함된 SNMP(Simple Network Management Protocol) 서비스의 기본 설정을 이용한 공격들이 많다. 이를 방지하기 위한 SNMP 보안 설정 방법으로 옳지 않은 것은?

① 꼭 필요한 경우가 아니면 읽기/쓰기 권한을 설정하지 않는다.

② 규칙적이고 통일성이 있는 커뮤니티 값을 사용한다.

③ ACL을 적용하여 특정 IP Address를 가진 경우만 SNMP 서비스에 접속할 수 있도록 한다.

SNMP를 TFTP와 함께 사용하는 경우, 'snmp-server
④ tftp-server-list' 명령으로 특정 IP Address만이 서비스에 접속할 수 있게 한다.

51. 라우터에서는 IP 및 패킷을 필터링하기 위한 Access Control List를 사용할 때 주의사항으로 옳바른 것은?

① 라우터에 연산 부담을 덜기 위하여 상세하고, 큰 용량의 ACL을 유지하여야 한다.

② 시스코 라우터는 입력 트래픽 보다 출력 트래픽에 ACL을 적용하는 것이 효율적이다.

③ 라우터 트래픽 감소를 위해 Netflow를 함께 작동시킨다.

④ ACL을 이용한 출력 트래픽 필터링은 위조된 IP가 유출되는 것을 방지한다.

52. 버퍼 오버플로우(Buffer Overflow)의 설명으로 옳지 않은 것은?

① 지정된 버퍼의 크기보다 더 많은 데이터를 입력해서 프로그램이 비정상적으로 동작하도록 만드는 것을 의미함

② 대부분의 경우 버퍼가 오버플로우 되면 프로그램이 비정상적으로 종료되면서 루트 권한을 획득할 수 있음

③ 버퍼가 오버플로우 되는 순간에 사용자가 원하는 임의의 명령어를 수행시킬 수 있음

④ 버퍼 오버플로우를 방지하기 위해서는 시스템에 최신 패치를 유지해야 함

53. 사용자의 개인 정보를 보호하기 위한 바람직한 행동으로 보기 어려운 것은?

① 암호는 복잡성을 적용하여 사용한다.

② 로그인 한 상태에서 자리를 비우지 않는다.

③ 중요한 자료는 따로 백업을 받아 놓는다.

④ 좋은 자료의 공유를 위해 여러 디렉터리에 대한 공유를 설정해 둔다.



전자문제집 CBT(App Store) : [다운로드](#)

전자문제집 CBT(Google Play) : [다운로드](#)

54. L2 스위칭 공격에 대한 설명으로 옳지 않은 것은?

① 하드웨어에 대한 공격과 트래픽 흐름을 변경하는 네트워크 공격으로 분류할 수 있다.

② MAC Flooding, ARP Spoofing, Spanning Tree Attack 등이 있다.

공격이 진행되고 있는 상태에서 스위치와 연결된 정상적인 호스트가 통신할 때, 스위치의 MAC 정보에는 영향을 미치지 않는다.

MAC Flooding은 한 포트에서 수 천 개의 호스트가 스위치와 연결되어 있는 것으로 보이지만 실제로는 변조된 MAC 정보를 공격 호스트에서 발생시키는 것이다.

55. 다음에서 설명하는 것은?

공격자의 컴퓨터로부터 표적 시스템과 그 시스템이 속한 네트워크에 과도한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 표적 시스템에서 제공하는 서비스들을 인터넷 사용자들이 이용하지 못하게 하는 기법

① Buffer Overflow

② Sniffing

③ IP Spoofing

④ Denial of Service

56. 다음에서 설명하는 기법은?

인터넷 프로토콜인 TCP/IP의 구조적 결함, 즉 TCP 시퀀스번호, 소스라우팅, 소스 주소를 이용한 인증(Authentication) 기능을 가지고 있는 시스템에 침입하기 위해 침입자가 사용하는 시스템을 원래의 호스트로 위장하는 방법이다.

① IP Sniffing

② IP Spoofing

③ Race Condition

④ Packet Filtering

57. Linux 파일 시스템에 대한 사용자에게 속하지 않는 것은?

① 소유자 : 파일이나 디렉터리를 처음 만든 사람

② 사용자 : 현재 로그인한 사용자

그룹 : 사용자는 어느 특정 그룹에 속하며 이 그룹에 속한 다른 사람들을 포함

④ 다른 사용자 : 현재 사용자 계정을 가진 모든 사람

58. 침입 탐지 시스템을 비정상적인 침입탐지 기법과 오용탐지 기법으로 구분할 경우, 오용탐지기법은?

① 상태 전이 분석

② 행위 측정 방식들의 결합

③ 통계적인 방법

④ 특징 추출

59. 방화벽의 주요 기능으로 옳지 않은 것은?

① 접근제어

② 사용자 인증

③ 로깅

④ 프라이버시 보호

60. SET(Secure Electronic Transaction)에 대한 설명으로 옳지 않은 것은?

① MasterCard사의 SEPP와 Visa사의 STT가 결합된 형태이다.

② RSA Data Security사의 암호기술을 기반으로 한 프로토콜이다.

③ 메시지의 암호화, 전자증명서, 디지털서명 등의 기능이 있다.

④ 비공개키 암호를 사용하여 안전성을 보장해 준다.