

정보시스템보안

1. 암호화에 대한 다음 설명 중 가장 옳지 않은 것은?

- ① 대칭 블록 암호화에서 한 블록의 크기는 일정 비트 길이로 설정된다.
- ② 대칭 블록 암호화에서 단위 블록의 크기가 커지면 보안성이 높아진다.
- ③ One-Time Pad의 키 크기는 64 또는 128비트 길이로 설정한다.
- ④ 스트림 암호에서 일부 암호문 비트가 손상되어도 에러 전파가 나타나지 않는다.

2. 정보 보안 방법에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 핑거프린팅(Fingerprinting)은 디지털 콘텐츠에 판매자 정보를 삽입, 해당 콘텐츠의 판매량을 집계하기 위한 방법이다.
- ② 디지털 워터마킹(Digital Watermarking)은 디지털 콘텐츠에 저작권 정보를 추가, 권리정보를 포함하기 위한 방법이다.
- ③ 스테가노그래피(Steganography)는 콘텐츠에 전달하려는 정보를 은닉, 삽입하는 방법이다.
- ④ DRM(Digital Rights Management)은 콘텐츠의 사용에 대한 권한을 통제, 관리하기 위한 방법이다.

3. Shannon의 확산(Diffusion)과 혼돈(Confusion)에 대한 다음 <보기> 중 가장 옳은 내용을 모두 선택한 것은?

< 보기 >

- ㉠ 확산에 의하여 평문에서의 통계적 분포 성질이 암호문에도 보존된다.
- ㉡ 확산에 의하여 암호문에서의 통계적 분포 성질로 키값 추출이 어렵다.
- ㉢ 혼돈에 의하여 평문에서의 통계적 분포 성질이 암호문과 무관해진다.
- ㉣ 혼돈에 의하여 키값 1비트의 변화로도 암호문이 크게 달라진다.

- ① ㄱ, ㄷ ② ㄴ
- ③ ㄹ, ㅈ ④ ㅊ

4. 키의 대칭성에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 대칭키 암호화는 키의 전달 방법에 대한 보안성 유지 방안을 별도로 마련하여야 한다.
- ② 비대칭키 방법으로 상호간 양방향 원문 송수신이 필요할 때, 비대칭 복호화 키를 공유하고, 암호화 키를 공개하는 방법을 사용한다.
- ③ 대칭키 암호화는 비대칭키 암호화 방법에 비하여 처리 성능이 높다.
- ④ 상호간 통신 참여 구성원의 증가에 따라, 대칭키 암호화는 비대칭키 암호화에 비하여 키의 총 갯수가 점차 많아진다.

5. 다음 <보기>는 어떤 형태의 공격에 대하여 설명한 것인가?

< 보기 >

“A 직원이 큰 실수를 했습니다. 연말정산 시스템에 민감정보가 있어서 조심했어야 했는데, 관리 접근 암호를 집 현관문 비밀번호 숫자와 함께 한 모양입니다.

A 직원이 집을 내놓으면서 부동산에 비밀번호를 알려줬고, 해커가 부동산을 통해 번호를 알게 되었습니다. 개인정보가 외부로 유출되어 직원들이 불안해하고 있습니다.”

- ① 해커는 은닉 채널(Covert Channel)을 사용했다.
- ② 해커는 레인보우 테이블(Rainbow Table)을 사용했다.
- ③ 해커는 패스워드 솔트(Salt)를 사용했다.
- ④ 해커는 인간 기반 사회공학(Social Engineering)을 사용했다.

6. OTP(One-Time Password) 기기를 이용한 패스워드 인증방식에서 다음 설명 중 가장 옳은 것은?

- ① 이벤트(계수기) 동기화 방식은 토큰장치가 네트워크에 연결되어 계수값을 서버에 전송한다.
- ② 시간 동기화 방식은 토큰장치가 네트워크에 연결되어 시간 정보를 전송한다.
- ③ 질의응답 방식은 서버에서 요구한 질의값을 토큰에 입력하고, 나타나는 응답값을 서버에 입력하여 검증한다.
- ④ FRR(False Rejection Rate)값으로 오인증을 관리한다.

7. 생체인증에 관련한 다음 <보기> 중 가장 옳은 내용을 선택한 것은?

< 보 기 >

- ㉠ 획득성(Collectability)은 대상 특성이 정량적으로 측정 가능한지를 의미한다.
- ㉡ 보편성(Universality)은 측정된 특성값이 각 개인마다 구분되게 나타나는지를 의미한다.
- ㉢ 수용성(Acceptability)은 시간에 따라 변화하지 않는 특성이 유지되는지를 의미한다.
- ㉣ 성능(Performance)은 환경변화와 무관하게 높은 정확성을 지속할 수 있는가를 의미한다.

- [illegible]

8. 클라우드 컴퓨팅의 특징으로 가장 옳은 것은?

- ① 가상기계와 달리 컨테이너(Container) 기술은 호스트 운영체제(Host OS)를 공유하여 성능을 높인다.
- ② 클라우드의 가상기계는 구축형에 비해 고성능이다.
- ③ SecaaS(Security as a Service)는 클라우드 수준에서 제공하는 보안 서비스로, 가상기계의 운영체제에 설치하여 사용하여야 한다.
- ④ 클라우드는 처리 부하를 예상하여 필요한 자원을 정적으로 계획, 구성하여야 한다.

9. TPM(Trusted Platform Module)에 관련된 내용으로 가장 옳지 않은 것은?

- ① 운영체제의 부팅이 완료된 후 응용 프로그램의 실행을 제한한다.
- ② 물리적인 컴퓨터 도난으로부터 데이터의 보안을 제공한다.
- ③ 암호화 키의 생성과 저장, 패스워드 저장, 무결성 검증 측정값의 저장, 인증서 관련 신뢰 연산 제공을 포함한다.
- ④ 신뢰 컴퓨팅(Trusted Computing)을 위한 핵심 요소로써 하드웨어/소프트웨어로 구성된 TPM을 필요로 한다.

10. 다음 <보기>는 정보보호의 목표이다. 가장 올바르게 짝지어진 것은?

< 보기 >

- ㉠ 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질.
 - ㉡ 오직 인가된 사람, 인가된 프로세스, 인가된 시스템만이 접근해야 한다는 원칙.
 - ㉢ 정당한 사용자가 정보시스템의 데이터 또는 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있는 성질.

구분	㉠	㉡	㉢
①	기밀성	인증성	가용성
②	기밀성	가용성	인증성
③	무결성	기밀성	가용성
④	무결성	가용성	기밀성

11. 다음 <보기> 설명에 해당하는 유형의 바이러스를 가장 옳게 짝지은 것은?

· < 보기 >

- ㉠ 바이러스가 랜덤 암호화키를 생성하고 스스로 암호화한다.
- ㉡ 안티 바이러스 소프트웨어에 의해 탐지되지 않기 위해 자신을 감추도록 설계된 바이러스를 말한다.
- ㉢ 감염시킬 때마다 변형되므로 특징을 이용한 탐지가 불가능해진다.
- ㉣ 감염시킬 때마다 형태뿐만 아니라 행동 패턴 까지 변화가 일어난다.

구분	㉠	㉡	㉢	㉣
①	폴리모픽 바이러스	메타모픽 바이러스	스텔스 바이러스	암호화된 바이러스
②	폴리모픽 바이러스	암호화된 바이러스	메타모픽 바이러스	스텔스 바이러스
③	암호화된 바이러스	스텔스 바이러스	폴리모픽 바이러스	메타모픽 바이러스
④	암호화된 바이러스	스텔스 바이러스	메타모픽 바이러스	폴리모픽 바이러스

12. 윈도우즈 시스템이 동작하기 위한 프로세스와 그에 대한 설명으로 가장 옳지 않은 것은?

- ① mstask.exe - 사용자가 미리 지정한 시간에 작업을 실행시키는 스케줄을 담당.
- ② svchost.exe - DLL(Dynamic Link Libraries)에 의해 실행되는 프로세스의 기본 프로세스.
- ③ lsass.exe - 윈도우 운영체제 내에서의 보안 정책의 시행을 담당하며 시스템에 접근하려는 모든 사용자를 체크.
- ④ smss.exe - 윈도우 콘솔을 관장하고, 스레드를 생성/삭제하며, 32비트 가상 MS-DOS 모드를 지원하는 프로세스.

13. 다음 <보기>의 ㉠, ㉡ 에 들어갈 말로 가장 옳은 것은?

— < 보 기 > —

두 프로세스 간에 자원을 사용하기 위해서 경쟁하는 것을 이용한 공격은 ㉠ 이라 하고, 시스템 프로그램과 공격 프로그램을 경쟁 상태에 이르게 하여 시스템 프로그램 권한으로 ㉡ 가 Root로 설정된 파일에 접근을 가능하게 하는 방법을 말한다.

구분	㉠	㉡
①	힙 오버플로우 공격	SetGID
②	레이스 컨디션 공격	SetUID
③	스택 오버플로우 공격	Finger
④	코드 기반 공격	Shadow

14. FTP(File Transfer Protocol)에 대한 설명으로 가장 옳지 않은 것은?

- ① FTP 모드에는 Active와 Passive 모드가 있다.
- ② TCP 포트 20은 제어 연결을 위해, 21은 데이터 연결을 위해 사용된다.
- ③ Passive 모드에서 데이터 전송을 하기 위해서는 1024번 이상의 포트를 사용한다.
- ④ 클라이언트는 FTP를 이용하여 서버의 파일을 읽고 저장할 수 있을 뿐만 아니라 파일목록을 볼 수도 있다.

15. CSRF(Cross Site Request Forgery)의 특징에 대한 설명으로 가장 옳지 않은 것은?

- ① 사이트에 방문하는 사용자가 정상적인 요청이 아닌 임의의 요청을 하도록 위조하는 방법이다.
- ② 특정 웹사이트가 사용자의 웹 브라우저를 실행하는 상태를 악용하는 방법이다.
- ③ 기본적으로 XSS 공격과 마찬가지로 웹 브라우저를 이용한 공격의 일종이다.
- ④ 악성 스크립트를 웹게시판에 등록하여 이를 웹 페이지 방문자의 브라우저 내에서 적절한 검증 없이 실행되도록 한다.

16. 「개인정보 보호법」상 개인정보 분쟁조정위원회에 대한 설명으로 가장 옳지 않은 것은?

- ① 위원장과 위촉위원의 임기는 2년으로 하되 1차에 한하여 연임할 수 있다.
- ② 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 국무총리령으로 정한다.
- ③ 개인정보에 대한 분쟁을 위하여 개인정보 분쟁조정위원회를 둔다.
- ④ 분쟁조정위원회는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

17. AES(Advanced Encryption Standard) 암호화 라운드 수행시 마지막 라운드를 제외한 각 라운드 수행의 4단계 처리 순서로 가장 옳은 것은?

- ① Substitute bytes → Add round key → Mix columns → Shift rows
- ② Substitute bytes → Shift rows → Mix columns → Add round key
- ③ Mix columns → Add round key → Substitute bytes → Shift rows
- ④ Add round key → Mix columns → Shift rows → Substitute bytes

18. 다음 중 Unix와 관련된 설명으로 가장 옳지 않은 것은?

- ① /etc/passwd : 사용자 기본 정보 파일을 저장하고 있음.
- ② /etc/group : 그룹 기본 정보 파일을 저장하고 있음.
- ③ /var : 프로그램 실행 및 설치 시 생성되는 임시 파일을 담고 있음.
- ④ /etc/login.defs : 사용자 계정 설정과 관련된 기본값을 정의한 파일.

19. 다음 <보기> 빈칸에 들어갈 용어를 가장 바르게 나열한 것은?

- < 보 기 >
- ☐ ㉠

는 공개적으로 알려진 소프트웨어의 보안 취약점을 가리키는 고유 표기를 의미한다.
- ☐ 취약점명은 ㉠ - ㉡ - ㉢ 형식으로 구성되어 있다.

구분	㉠	㉡	㉢
①	CVE	연도	일련번호
②	CVSS	연도	일련번호
③	CVE	일련번호	소프트웨어버전
④	CWE	일련번호	소프트웨어버전

20. 검색엔진이 사이트를 수집하기 위해 사용하는 크롤러(Crawler)에 대하여 사이트의 수집·허용 여부를 표시하는 파일은?

- ☐ ① access.conf
- ☐ ② httpd.conf
- ☐ ③ robots.txt
- ☐ ④ crawler.txt