

※ 답안지에 한 번 표기한 답을 수정테이프 등으로 정정하거나 칼 등으로 긁어 변형할 경우 그 문항은 무효로 처리함.

1. 다음 지문에서 설명하는 기술과 바르게 짝지은 것은?

(가) 디지털콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.

(나) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털콘텐츠에 삽입하는 기술이다.

(다) 공격자가 공격전에 공격대상에 대한 다양한 정보를 수집하는 기술이다.

- ① (가) 워터마킹      (나) 핑거프린팅      (다) 워터링 홀
- ② (가) 핑거프린팅      (나) 워터링 홀      (다) 풋프린팅
- ③ (가) 풋프린팅      (나) 워터마킹      (다) 핑거프린팅
- ④ (가) 핑거프린팅      (나) 워터마킹      (다) 풋프린팅

2. 암호학적 해시함수(Cryptographic Hash Function)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

- ① 어떤 입력 x 에 대해 h(x) 를 계산하기 어려워야 한다.
- ② 주어진 값 y 에 대해 h(x)=y 의 x 값을 찾는 계산이 어려워야 한다.
- ③ 생일역설(Birthday Paradox)은 충돌 저항성 공격(Collision Resistance Attack)과 관련한 수학적 분석 결과이다.
- ④ 입력 길이에 상관없이 고정된 길이를 출력한다.

3. MD5(Message Digest 5)는 널리 쓰는 해시함수이며, 최종적으로 ( )비트의 해시코드를 출력한다. ( ) 안에 들어갈 적합한 숫자는 무엇인가?

- ① 64                      ② 128                      ③ 256                      ④ 512

4. 공개키 암호 시스템을 이용하여 Alice가 Bob에게 암호문을 전달하고 이를 복호화하는 과정에 관한 다음 설명 중 ( ) 안에 들어갈 내용으로 바르게 짝지은 것은 무엇인가?

1. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.

2. Bob은 ( 가 )를 Alice에게 전송한다.

3. Alice는 ( 나 )를 사용하여 메시지를 암호화한다.

4. Alice는 생성된 암호문을 Bob에게 전송한다.

5. Bob은 ( 다 )를 사용하여 암호문을 복호화한다.

- ① (가) Bob의 공개키 (나) Alice의 공개키 (다) Alice의 개인키
- ② (가) Bob의 개인키 (나) Bob의 공개키 (다) Bob의 개인키
- ③ (가) Bob의 개인키 (나) Alice의 공개키 (다) Alice의 개인키
- ④ (가) Bob의 공개키 (나) Bob의 공개키 (다) Bob의 개인키

5. 임의적 접근통제(DAC : Discretionary Access Control)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

- ① 객체(데이터)의 소유주에 의하여 접근권한 변경이 가능하다.
- ② 일반적으로 ACL(Access Control List)을 통해서 이루어진다.
- ③ 민감도 레이블(Sensitivity Label)에 따라 접근을 허용할 지 결정한다.
- ④ ID기반 접근통제이다.

6. 대칭키와 공개키 암호화 방식에 관한 다음 설명 중 옳은 것은 모두 몇 개인가?

가. 일반적으로 안전한 키 길이는 대칭키 방식의 키가 공개키 방식의 키보다 길다.

나. 대칭키 방식의 암호화키와 복호화키는 동일하며, 모두 비밀이다.

다. 공개키 방식의 암호화키와 복호화키는 모두 공개이다.

라. 일반적으로 암호화 속도는 대칭키 방식이 공개키 방식보다 빠르다.

마. 대칭키 방식의 알고리즘에는 AES, SEED, ECC 등이 있다.

- ① 2개                      ② 3개                      ③ 4개                      ④ 5개

7. 다음 지문에서 설명하는 접근통제모델은 무엇인가?

접근통제모델 중 효율적인 업무처리(Well-formed transactions)와 직무분리(Separation of duties) 두 가지 원칙을 통해 좀 더 정교하게 무결성을 보장하는 모델이다.

- ① 벨-라파둘라(Bell-LaPadula)
- ② 비바(Biba)
- ③ 테이크 그랜트(Take Grant)
- ④ 클락-윌슨(Clark-Wilson)

8. 생체인증기술의 정확도는 부정거부율(FRR : False Rejection Rate)과 부정허용율(FAR : False Acceptance Rate)로 측정할 수 있다. 생체인증기술의 정확도에 관한 다음 설명 중 옳은 것끼리 짝지은 것은 무엇인가?

가. 사용자 편의성을 요구하는 경우 FAR이 높아지고 FRR은 낮아진다.

나. 사용자 편의성을 요구하는 경우 FRR이 높아지고 FAR은 낮아진다.

다. 보안성을 강화할 경우 FRR은 높아지고 FAR은 낮아진다.

라. 보안성을 강화할 경우 FAR은 높아지고 FRR은 낮아진다.

- ① 가, 다                      ② 가, 라                      ③ 나, 다                      ④ 나, 라

9. 다음 중 취약점 점검 도구가 아닌 것은 무엇인가?

- ① SARA                      ② NIKTO
- ③ TCP WRAPPER                      ④ NESSUS

10. 윈도우 파일 시스템 NTFS(New Technology File System)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

- ① NTFS는 기본 NTFS 보안의 공유 보안과 동일하게 Everyone 그룹에 대해서는 모든 권한이 '허용'이다.
- ② 기본 NTFS 보안을 변경하면 사용자마다 서로 다른 NTFS 보안을 적용시킬 수 있다.
- ③ 파일과 폴더에 대한 보안강화 및 접근제어가 가능하다.
- ④ 저장량 볼륨에 최적화되어 있다.

11. 다음 중 윈도우 레지스트리 키가 아닌 것은 무엇인가?

- ① HKEY\_CLASSES\_ROOT
- ② HKEY\_CURRENT\_USER
- ③ HKEY\_MACHINE\_SAM
- ④ HKEY\_USERS





36. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제70조 (벌칙) 내용이 아닌 것은 모두 몇 개인가?

- 가. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
- 나. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.
- 다. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 다른 사람을 모욕한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
- 라. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 사자의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 3천만원 이하의 벌금에 처한다.

- ① 1개                    ② 2개                    ③ 3개                    ④ 4개

37. 「전자서명법」 제21조(전자서명생성정보의 관리) 제4항의 내용 중 (    ) 안에 들어갈 단어로 바르게 짝지은 것은 무엇인가?

공인인증기관은 자신이 이용하는 전자서명( 가 )정보를 안전하게 보관·관리하여야 한다. 이 경우 당해 전자서명( 나 )정보가 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 지체없이 그 사실을 ( 다 )에(게) 통보하고 인증업무의 안전성과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.

- ① (가) 생성            (나) 생성            (다) 인터넷진흥원
- ② (가) 검증            (나) 생성            (다) 인터넷진흥원
- ③ (가) 생성            (나) 생성            (다) 이용자
- ④ (가) 생성            (나) 검증            (다) 이용자

38. 다음 지문은 무엇에 관한 설명인가?

- 가. 자신에게 불리한 증거자료를 사전에 차단하려는 활동이나 기술
- 나. 데이터 복구 회피기법
- 다. 데이터 은닉(Steganography)

- ① Anti Forensic                    ② Digital Forensic
- ③ Root Kit                            ④ Stealth Scan

39. 1998년 Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 소프트웨어인 엔케이스(EnCase) 고유의 포렌식 디스크 이미지 파일형식은 무엇인가?

- ① FTK                    ② dd                    ③ SHA                    ④ E01

40. 다음 지문에서 설명하는 디지털포렌식의 원칙은 무엇인가?

증거는 획득하고 난 뒤 이송, 분석, 보관, 법정 제출이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다.

- ① 정당성의 원칙
- ② 재현의 원칙
- ③ 연계 보관성의 원칙
- ④ 무결성의 원칙