2018년 지방직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
④	④	②	③	①	③	①	③	④	②
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
③	④	②	①	①	②	②	②	④	④

문 1. 정보보호의 3대 요소 중 가용성에 대한 설명으로 옳은 것은?

① 권한이 없는 사람은 정보자산에 대한 수정이 허락되지 않음을 의미한다.
② 권한이 없는 사람은 정보자산에 대한 접근이 허락되지 않음을 의미한다.
③ 정보를 암호화하여 저장하면 가용성이 보장된다.
④ DoS(Denial of Service) 공격은 가용성을 위협한다.

답 ④

가용성(Availability)이란 정당한 권한이 있는 사용자는 서비스를 이용할 수 있어야 한다는 것을 말한다.
④ DoS(Denial of Service, 서비스 거부 공격)은 해당 시스템의 자원을 고갈시켜 제대로 사용하지 못하도록 만드는 공격이다.
정당한 권한이 있는 사용자도 서비스를 이용하지 못하게 되므로 가용성을 침해하는 위협요소이다.

<오답 체크> ① 무결성에 대한 설명이다.
② 기밀성에 대한 설명이다.
③ 암호화는 기밀성을 보장하기 위한 보안 방법이다.
가용성을 보장하기 위한 방법은 데이터 백업 및 복원 등이 있다.

문 2. ISO/IEC 27001에서 제시된 정보보안관리를 위한 PDCA 모델에서 ISMS의 지속적 개선을 위해 시정 및 예방 조치를 하는 단계는?

① Plan
② Do
③ Check
④ Act

답 ④

◈ **PDCA 모델**
Plan(계획): 보안 정책, 목적 프로세스 및 절차 수립
Do(실행): 통제, 프로세스 및 절차 구현, 운영
Check(점검): 성과 측정, 평가, 보고
Act(처리): 검토, 유지보수, 개선

문 3. 보안 관리 대상에 대한 설명으로 ㉠~㉢에 들어갈 용어는?

> ○ (㉠) - 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.
> ○ (㉡) - 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.
> ○ (㉢) - 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인이나 행위자를 말한다.

㉠	㉡	㉢
① 로그	세션	위험
② 로그	세션	위협
③ 백업	쿠키	위험
④ 백업	쿠키	위협

답 ②

㉠ **로그**(log): 운영 체제나 소프트웨어 실행 중에 발생하는 이벤트나 각기 다른 사용자의 통신 간의 메시지를 기록하는 것
㉡ **세션**(session): 둘 이상의 통신 장치 및 시스템이 상호작용을 위해 연결이 활성화된 것
㉢ **위협**(threat): 자산에 손실을 발생시킬 수 있는 원인이나 행위, 공격자 등
<오답 체크> ① **위험**(risk): 위협이 취약점을 이용하여 자산에 손실을 일으킬 가능성
▷ **취약점**(vulnerability): 위협에 이용될 수 있는 자산이 가진 약점이나 속성. 보안에 해를 끼치는 행동이나 사건
③ **백업**(backup): 데이터를 미리 별도의 공간에 복사해두어, 문제가 발생했을 때 데이터를 복구할 수 있도록 준비해 두는 것
▷ **쿠키**(cookie): 인터넷 사용자가 웹사이트를 방문할 경우, 사용자 편의를 제공하기 위해 사용자의 계정정보와 환경설정 값 등을 기록하는 정보 파일. 서버가 아니라 클라이언트의 컴퓨터에 저장된다.

문 4. 유닉스 시스템에서 파일의 접근모드 변경에 사용되는 심볼릭 모드 명령어에 대한 설명으로 옳은 것은?

① chmod u-w: 소유자에게 쓰기 권한 추가
② chmod g+wx: 그룹, 기타 사용자에게 쓰기와 실행 권한 추가
③ chmod a+r: 소유자, 그룹, 기타 사용자에게 읽기 권한 추가
④ chmod o-w: 기타 사용자에게 쓰기 권한 추가

답 ③

▷ **chmod**(change mode)는 파일이나 디렉터리에 대한 권한을 변경하는 명령어다.
③ a+ : 모두(all)에게 권한을 부여(+)한다.
a+r : 모든 사용자(all, 소유자+그룹+기타 사용자)들에게 읽기(r) 권한을 부여
<오답 체크> ① u-w : 소유자(user)에게서 쓰기(w) 권한 제거
② g+wx : 그룹(group)에 쓰기(w)와 실행(x) 권한을 부여
④ o-w : 기타 사용자(other)에게서 쓰기(w) 권한을 제거

문 5. 정보가 안전한 정도를 평가하는 TCSEC(Trusted Computer System Evaluation Criteria)의 보안등급 중에서 검증된 설계(Verified Design)를 의미하는 보안등급은?

① A 등급
② B 등급
③ C 등급
④ D 등급

답 ①

◈ **TCSEC 보안 등급** ◈
▷ **A1** Verified Design(검증된 설계)
수학적으로 완벽한 시스템
▷ **B3** Security Domains(보안 영역)
운영체제에서 보안에 불필요한 부분을 모두 제거
모듈에 따른 분석 및 테스트가 가능
시스템 파일 및 디렉터리에 대한 접근 방식을 지정하고, 위험 동작을 하는 사용자의 활동에 대해서는 백업까지 자동으로 이루어짐
▷ **B2** Structured Protection(계층 구조화된 보호)
시스템에 정형화된 보안 정책이 존재
일부 유닉스 시스템이 B2인증에 성공
▷ **B1** Labeled Security(레이블된 보호)
시스템 내의 보안 정책을 적용할 수 있으며 각 데이터에 대해 보안 레벨 설정이 가능
시스템 파일이나 시스템에 대한 권한을 설정
▷ **C2** Controlled Access Protection(통제된 보호)
각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템
보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있음
윈도우NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 이 등급에 해당
상용 프로그램을 위한 최소한의 요구 등급
▷ **C1** Discretionary Security Protection(임의적 보호)
일반적인 로그인 과정이 존재하는 시스템.
사용자간 침범이 차단되어 있고 모든 사용자가 자신이 생성한 파일에 대해 권한을 설정할 수 있으며, 특정 파일에 대해서만 접근이 가능
초기의 유닉스 시스템이 C1등급
▷ **D** Minimal Protection(최소한의 보호)
보안 설정이 이루어지지 않은 단계

문 6. 다음에서 설명하는 공격 기술은?

> 암호 장비의 동작 과정 중에 획득 가능한 연산시간, 전력 소모량, 전자기파 방사량 등의 정보를 활용하여 암호 알고리즘의 비밀 정보를 찾아내는 기술

① 차분 암호 분석 공격(Differential Cryptanalysis Attack)
② 중간자 공격(Man-In-The-Middle Attack)
③ 부채널 공격(Side-Channel Attack)
④ 재전송 공격(Replay Attack)

답 ③

③ **부채널 공격**(Side-Channel Attack)
암호 체계의 물리적인 구현 과정의 정보를 기반으로 하는 공격 방법이다.
소요 시간 정보, 소비 전력, 방출하는 전자기파 또는 소리 등 암호 시스템 하드웨어의 작동 과정에서 발생하는 물리적인 특성을 분석하여 시스템을 파괴하거나 암호 알고리즘의 비밀 정보를 찾아내는 기술이다.

<오답 체크> ① **차분 공격**(differential cryptanalysis)은 입력값의 변화에 따른 출력값의 변화를 이용하는 방법이다.
일반적으로 선택 평문 공격(chosen-plaintext attack)에서 이용하는 암호 해독 방법으로, 2개의 평문 블록들의 비트 차이에 대하여 대응되는 암호문 블록들의 비트 차이를 비교하여 암호키를 추측하는 방법이다.

② **중간자 공격**(Man-In-The-Middle Attack, MITM)
연결하는 두 송수신자 사이에 중간자가 침입하여 한쪽에서 전달된 정보를 도청한 뒤 이를 다른 쪽에 전달하는 공격이다.
두 송수신자는 상대방에게 연결했다고 생각하지만 실제로는 가운데 중간자와 연결되어 있으며, 중간자는 해당 정보를 도청만 한 뒤 그대로 보낼 수도 있고, 조작하여 보낼 수도 있다.

④ **재전송 공격**(Replay Attack)
프로토콜 상에서 유효 메시지를 골라 복사한 후 나중에 재전송함으로써 정당한 사용자인 척하는 공격이다.

문 7. DoS(Denial of Service) 공격의 대응 방법에 대한 설명으로 ㉠, ㉡에 들어갈 용어는?

> ○ 다른 네트워크로부터 들어오는 IP broadcast 패킷을 허용하지 않으면 자신의 네트워크가 (㉠) 공격의 중간 매개지로 쓰이는 것을 막을 수 있다.
> ○ 다른 네트워크로부터 들어오는 패킷 중에 출발지 주소가 내부 IP 주소인 패킷을 차단하면 (㉡) 공격을 막을 수 있다.

㉠	㉡
① Smurf	Land
② Smurf	Ping of Death
③ Ping of Death	Land
④ Ping of Death	Smur

답 ①

㉠ **Smurf**(ICMP flooding) 공격은 출발지 IP주소를 공격대상의 IP 주소로 위장하여 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상으로 많은 양의 ICMP Echo 응답 패킷이 몰리게 만들어 시스템 자원이 고갈되도록 만드는 공격이다.
외부에서 들어오는 IP 브로드캐스트 패킷을 무시하도록 설정하면, ICMP Echo 응답 패킷을 보내지 않으므로 Smurf 공격에 악용되지 않는다.

㉡ **Land 공격**(Land Attack)은 패킷의 출발지 IP 주소와 목적지 IP 주소 값을 모두 공격자의 IP 주소 값으로 만들어 전송하는 공격이다. 출발지 주소와 목적지 주소가 같기 때문에 이 패킷의 응답은 공격대상을 떠났다가 그대로 다시 공격대상에게 들어가는데, SYN Flooding처럼 동시 사용자 수를 점유해버리며 CPU 자원을 고갈시킨다.
외부 네트워크에서 들어오는 패킷의 출발지 주소가 내부 IP 주소라는 것은 이 패킷이 Land 공격을 위해 위조된 패킷이라는 말이다.

문 8. 「전자서명법」상 용어의 정의로 옳지 않은 것은?

① '전자서명'이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

② '인증서'라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.

③ '서명자'라 함은 전자서명검증정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.

④ '전자서명생성정보'라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

답 ③

③ **「전자서명법」** 제2조

12. "서명자"라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.

전자서명생성정보는 전자서명을 생성하는 개인키이며,
전자서명검증정보는 전자서명을 검증하는 공개키이다.

<오답 체크> ① 전자서명법 제2조 2.
② 전자서명법 제2조 7.
④ 전자서명법 제2조 5.

「전자서명법」 제2조(정의)

이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "전자문서"라 함은 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
2. "전자서명"이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
3. "공인전자서명"이라 함은 다음 각목의 요건을 갖추고 공인인증서에 기초한 전자서명을 말한다.

가. 전자서명생성정보가 가입자에게 유일하게 속할 것
나. 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것
다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것
라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것

4. "전자서명생성정보"라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.
5. "전자서명검증정보"라 함은 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말한다.
6. "인증"이라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말한다.
7. "인증서"라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
8. "공인인증서"라 함은 제15조의 규정에 따라 공인인증기관이 발급하는 인증서를 말한다.
9. "공인인증업무"라 함은 공인인증서의 발급, 인증관련 기록의 관리 등 공인인증역무를 제공하는 업무를 말한다.
10. "공인인증기관"이라 함은 공인인증역무를 제공하기 위하여 제4조의 규정에 의하여 지정된 자를 말한다.
11. "가입자"라 함은 공인인증기관으로부터 전자서명생성정보를 인증받은 자를 말한다.
12. "서명자"라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.
13. "개인정보"라 함은 생존하고 있는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

문 9. 「전자정부 SW 개발·운영자를 위한 소프트웨어 개발 보안 가이드」상 분석·설계 단계 보안요구항목과 구현 단계 보안약점을 연결한 것으로 옳지 않은 것은?

분석·설계 단계 보안요구항목	구현 단계 보안약점
① DBMS 조회 및 결과 검증	SQL 삽입
② 디렉터리 서비스 조회 결과 점증	LDAP 삽입
③ 웹서비스 요청 및 결과 검증	크로스사이트 스크립트
④ 보안기능 동작에 사용되는 입력값 검증	솔트 없이 일방향 해시 해시함수 사용

답 ④

(기존에 출제된 적이 없는 기준서에 대한 문제인데, 가이드 기준서의 내용을 알 필요 없이 정보보호론 이론적 내용을 토대로 풀 수 있는 문제이다.)

④ 시스템에 입력되는 입력값을 검증하는 것과 취약한 해시함수 사용은 관련이 없다.
입력값을 검증하는 것은 오버플로우나 Null Pointer 역참조에 대한 보안 약점을 예방하기 위한 보안 요구사항이다.

「안전한 SW 개발을 위한 소프트웨어 개발보안 가이드」 개정본은 아래에서 다운받아 볼 수 있다.
문제의 내용은 40페이지에 나와있다.
http://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=57473

문 10. 개인정보 보호법령상 영업양도 등에 따른 개인정보의 이전 제한에 대한 내용으로 옳지 않은 것은?

① 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다.
② 영업양수자등이 과실 없이 서면 등의 방법으로 개인정보를 이전받은 사실 등을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 10일 이상 게재하여야 한다.
③ 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 개인정보를 이전하려는 사실 등을 서면 등의 방법에 따라 해당 정보주체에게 알려야 한다.
④ 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 서면 등의 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 「개인정보보호법」 제27조제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

답 ②

② 없는 내용이다.
<오답 체크> ① 「개인정보보호법」 제27조 3항
③ 「개인정보보호법」 제27조 1항
④ 「개인정보보호법」 제27조 2항

제27조(영업양도 등에 따른 개인정보의 이전 제한)
① 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.
1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

② 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

③ 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.

문 11. 대칭키 암호 알고리즘에 대한 설명으로 옳은 것만을 모두 고르면?

> ㄱ. AES는 128/192/256 비트 키 길이를 지원한다.
> ㄴ. DES는 16라운드 Feistel 구조를 가진다.
> ㄷ. ARIA는 128/192/256 비트 키 길이를 지원한다.
> ㄹ. SEED는 16라운드 SPN(Substitution Permutation Network) 구조를 가진다.

① ㄱ, ㄹ
② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄷ
④ ㄱ, ㄴ, ㄹ

답 ③

ㄱ. **AES**(Advanced Encryption Standard)
SPN구조
블록 128비트(16바이트)
키 길이 128비트 – 10라운드
키 길이 192비트 - 12라운드
키 길이 256비트 - 14라운드

ㄴ. **DES**(Data Encryption Standard)
페이스텔(Feistel) 구조 16라운드
블록 64비트
키 길이 56비트 + 패리티 8비트 = 64비트

ㄷ. **ARIA** (국산)
128비트 블록
Involutional SPN 구조 12/14/16라운드
키 길이 128/192/256 비트
KS 국가 표준, 효율성에 맞게 최적화, 다양한 환경에 적합

<오답 체크> ㄹ. **SEED** (국산)
128비트 블록 크기
128 또는 256 비트 키
16라운드의 페이스텔 구조
1999년 한국정보보호진흥원(KISA)와 국내 암호전문가들이 개발

문 12. 다음에서 설명하는 프로토콜은?

> ○ 무선랜 통신을 암호화하는 프로토콜로서 IEEE 802.11 표준에 정의되었다.
> ○ 암호화를 위해 RC4 알고리즘을 사용한다.

① AH(Authentication Header)
② SSH(Secure SHell)
③ WAP(Wireless Application Protocol)
④ WEP(Wired Equivalent Privacy)

답 ④

④ **WEP** 방식
암호화를 위해 RC4 사용(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용

▷ **WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용

▷ **WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증

<오답 체크> ① **AH**(Authentication Header, 인증 헤더)는 메시지 무결성과 인증 기능은 제공하는 IPSec의 프로토콜

② **SSH**(Secure Shell)은 FTP와 telnet을 보호하기 위한 보안 프로토콜

③ **WAP**(Wireless Application Protocol, 무선 애플리케이션 프로토콜)
휴대 전화 등의 장비에서 인터넷 등 무선 통신을 사용하는 응용 프로그램의 국제 표준이다.
(스마트폰이 아닌 피처폰에서의 인터넷 응용 프로그램을 의미한다. 고로 지금은 망한 것이나 다름없다.)
WAP은 매우 작은 이동 장비에 웹 브라우저와 같은 서비스를 제공하기 위해 설계되었으며, XML을 기반으로 설계된 WML(무선 마크업 언어)를 사용한다.

문 13. 기밀성을 제공하는 암호 기술이 아닌 것은?

① RSA
② SHA-1
③ ECC
④ IDEA

답 ②

② SHA-1은 무결성을 제공하는 해시 알고리즘으로, 160비트의 해시 값을 출력한다.

<오답 체크> ① RSA: 소인수분해 계산의 어려움에 기반한 공개키 암호 알고리즘

③ ECC: 타원곡선 상의 이산대수 계산의 어려움을 이용한 공개키 암호 알고리즘

④ IDEA
대칭키 암호 알고리즘 중 하나로, 암호화 알고리즘은 블록 암호 알고리즘 중 가장 안전하다고 알려져 있다.
64비트 블록 크기 / 128비트 키 / 8라운드
상이한 대수 그룹으로부터의 세 가지 연산(XOR, add mod 216, multiply mod 216+1)을 혼합하는 방식

문 14. SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① 전송계층과 네트워크계층 사이에서 동작한다.
② 인증, 기밀성, 무결성 서비스를 제공한다.
③ Handshake Protocol은 보안 속성 협상을 담당한다.
④ Record Protocol은 메시지 압축 및 암호화를 담당한다.

답 ①

▶ **SSL**(Secure Sockets Layer, 보안 소켓 레이어) 또는 **TLS**(Transport Layer Security, 전송 계층 보안)
응용 계층과 전송 계층 사이에서 통신 과정에서 종단간 보안과 클라이언트와 서버 간 상호 인증, 기밀성, 무결성 서비스를 제공하는 보안 프로토콜
인터넷 전자상거래를 위해 넷스케이프사가 개발한 것으로, 웹 브라우저와 웹 서버 간의 전자상거래 정보를 안전하게 전송하기 위한 프로토콜이다. SSL 3.0버전이 TLS 1.0버전이 된다.

① SSL은 OSI 4계층 전송 계층에서 동작한다.

◈ **SSL/TLS 구조**
▷ 핸드셰이크 프로토콜(handshake protocol)
서버와 클라이언트가 서로를 인증하고 암호, MAC알고리즘 레코드 데이터 보호에 사용될 암호화 키를 협상
▷ 암호 사양 변경 프로토콜(change cipher spec protocol)
핸드쉐이크 프로토콜의 일부로 암호 방법을 변경
▷ 경고 프로토콜(alert protocol)
에러 코드를 전송
▷ 애플리케이션 데이터 프로토콜(application data protocol)
HTTP를 포함한 다양한 상위계층의 보안 서비스 제공
▷ 레코드 프로토콜(record protocol)
SSL의 실제 데이터를 다루며, 데이터를 단편화 및 압축하고 MAC을 적용하고 암호화하여 이를 TCP에 전달

문 15. DSA(Digital Signature Algorithm)에 대한 설명으로 옳지 않은 것은?

① 기밀성과 부인방지를 동시에 보장한다.
② NIST에서 발표한 전자서명 표준 알고리즘이다.
③ 전자서명의 생성 및 검증 과정에 해시함수가 사용된다.
④ 유한체상의 이산대수문제의 어려움에 그 안전성의 기반을 둔다.

답 ①

① 전자서명 알고리즘만으로는 기밀성을 보장할 순 없다.
전자서명을 생성할 땐 메시지가 아닌 메시지의 해시값에 DSA 알고리즘을 적용하기 때문에 메시지는 평문 그대로 남아있다.
만약 DSA 알고리즘을 메시지에 직접 적용하여 전자서명을 생성한다 하여도, 그건 서명자의 공개키를 이용해 누구나 복호화할 수 있기 때문에 기밀성이 보장될 순 없다.

<오답 체크> ② DSA(Digital Signature Algorithm)는 디지털 서명을 위한 연방 정보 처리 표준이다. 1991년 8월 미국 국립표준기술연구소(NIST)에서 DSA를 제안했으며 1993년 FIPS 186로 채택되었다.

③ 메시지에 직접 전자서명을 하는 방식이 아닌, 메시지의 해시값에 서명하는 방식을 취하고 있다.
송신자(서명자)의 개인키를 이용해 서명을 생성하고, 송신자의 공개키를 이용해 서명을 검증한다.

④ DSA는 ElGamal을 응용한 방식으로, 유한체에서의 이산대수 문제의 어려움에 기반하고 있다.

문 16. 무의미한 코드를 삽입하고 프로그램 실행 순서를 섞는 등 악성코드 분석가의 작업을 방해하는 기술은?

① 디스어셈블(Disassemble)
② 난독화(Obfuscation)
③ 디버깅(Debugging)
④ 언패킹(Unpacking)

답 ②

② **난독화**(Obfuscation)
프로그래밍 언어로 작성된 코드에 대해 읽기 어렵게 만드는 작업으로, 코드의 가독성을 낮춰 역공학에 대한 대비하는 방법이다.
난독화를 적용하는 범위에 따라 소스 코드 난독화와 바이너리 난독화로 나눌 수 있다.
난독화 방법으로는
ⅰ 필요 이상으로 복잡하거나 아무 의미 없는 코드를 작성하는 방법
ⅱ 관련이 없는 여러 함수들을 뒤섞는 방법
ⅲ 데이터를 알아보기 힘들게 인코딩하는 방법 등이 있다.

<오답 체크> ① **디스어셈블**(Disassemble, 역어셈블)은 기계어를 어셈블리어로 변환하는 것
비슷한 말로 **디스컴파일**(Decompile, 역컴파일)은 기계어를 고급언어로 변환하는 것

③ **디버깅**(Debugging)은 컴퓨터 프로그램의 정확성이나 논리적인 오류(버그)를 찾아내는 테스트 과정

④ **패킹**(Packing)
프로그램의 코드를 분석하기 어렵도록 암호화하거나 정크 코드(불필요한 쓰레기 코드)를 삽입하여 압축하는 것

▷ **언패킹**(Unpacking) 패킹된 파일을 다시 언팩 상태로 만드는 것

문 17. 윈도우즈용 네트워크 및 시스템 관리 명령어에 대한 설명으로 옳은 것은?

① ping - 원격 시스템에 대한 경로 및 물리 주소 정보를 제공한다.
② arp - IP 주소에서 물리 주소로의 변환 정보를 제공한다.
③ tracert - IP 주소, 물리 주소 및 네트워크 인터페이스 정보를 제공한다.
④ ipconfig - 원격 시스템의 동작 여부 및 RTT(Round Trip Time) 정보를 제공한다.

답 ②

② arp는 시스템이 가지고 있는 ARP 테이블의 목록을 확인, 추가, 삭제하는 명령어이다.
-a 옵션은 ARP 테이블 보기
-d 옵션은 ARP 테이블에서 해당 IP 삭제
-s 옵션은 ARP 테이블에 해당 IP와 MAC 주소 추가
ARP는 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 변환하기 위해 사용되는 프로토콜이다.

<오답 체크> ① ping 명령어는 네트워크상의 원격지 호스트의 연결 상태를 확인한다.
③ tracert 명령어는 특정 IP에 도달할 때까지의 전체 경유 경로 내역을 보여준다.
④ ipconfig 명령어는 물리적, 논리적으로 연결된 네트워크 장치들과 해당 장치에 연결된 IP 주소 정보를 표시해주는 명령어이다.

문 18. 정보자산에 대한 위험분석에서 사용하는 ALE(Annualized Loss Expectancy, 연간예상손실액), SLE(Single Loss Expectancy, 1회손실예상액), ARO(Annualized Rate of Occurrence, 연간발생 빈도) 사이의 관계로 옳은 것은?

① ALE = SLE + ARO
② ALE = SLE × ARO
③ SLE = ALE + ARO
④ SLE = ALE × ARO

답 ②

예를 들어, 1회 손실 예상액(ALE)이 10억 원이고,
연간 평균 4회 발생(ARO)한다면,
연간 예상 손실액(ALE)은 10 X 4 = 40억 원이라 추정할 수 있다.

문 19. 「개인정보 보호법」상 개인정보 보호 원칙으로 옳지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
④ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비밀로 하여야 한다.

답 ④

④ **「개인정보 보호법」** 제3조 5항
개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 **공개하여야 하며,** 열람청구권 등 정보주체의 권리를 보장하여야 한다.

<오답 체크> ①「개인정보 보호법」 제3조 1항
②「개인정보 보호법」 제3조 2항
③「개인정보 보호법」 제3조 3항

제3조(개인정보 보호 원칙)
① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

문 20. 다음에서 설명하는 블록암호 운용 모드는?

> ○ 암·복호화 모두 병렬 처리가 가능하다.
> ○ 블록 암호 알고리즘의 암호화 로직만 사용한다.
> ○ 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다.

① ECB
② CBC
③ CFB
④ CTR

암호 모드	병렬 처리	복호화 로직	오류 전파
ECB	가능	필요	X
CBC	불가능	필요	O
CFB	불가능	불필요	O
OFB	?	불필요	X
CTR	가능	불필요	X

▶ OFB모드에서 어떤 것을 병렬 처리로 보느냐에 따라 **병렬 처리가 가능하다는 의견도 있고, 불가능하다는 의견도 있다.**
전처리를 통해 미리 키스트림을 생성해놓으면 한꺼번에 여러 블록을 암·복호화 처리할 수 있어 그것을 병렬 처리로 보는 의견도 있고,
키스트림을 만들기 시작하는 것부터 암·복호화 과정이라고 본다면 앞 블록부터 차례로 키스트림을 생성해야 하기 때문에 병렬 처리가 불가능하다는 얘기가 된다.

답 ④

암·복호화 모두 병렬 처리가 가능하며, 복호화 과정에서도 암호화 로직을 사용하며, 오류 전파가 없는 블록암호 모드를 고르라는 문제이다.

④ **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.
각각의 블록들은 독립적으로 처리가 가능하기 때문에 병렬 처리가 가능하며 오류 전파가 없다.
복호화 과정에서도 카운터 값을 암호화한 스트림 암호와 암호문 블록을 XOR하기 때문에 복호화 로직이 필요 없이, 암호화 로직만 사용된다.

<오답 체크> ① **ECB**(electronic codebook, 전자 코드북) 모드
가장 간단한 구조로, 암호화하려는 메시지를 여러 블록으로 나누어 각각 암호화하는 방식이다.
병렬 처리가 가능하며, 오류 전파가 없지만, 복호화 과정에서 복호화 로직을 사용한다.

② **CBC**(cipher-block chaining, 암호 블록 체인) 모드
평문 블록을 이전 단계의 암호문 블록과 XOR 한 후 암호화한다. 첫 번째 평문 블록의 경우에는 초기화 벡터(IV)와 XOR 한 후 암호화한다.
이전 단계의 암호문 블록이 필요하기 때문에 병렬 처리도 불가능하며, 암호문 한 비트의 오류가 다음 불록에도 영향을 주게 된다.
또한 복호화 과정에서 이전 단계의 암호문 블록롸 XOR한 후 복호화 로직을 사용한다.

③ **CFB**(cipher feedback, 암호 피드백) 모드
이전 단계의 암호문 블록을 암호화한 후 현재의 평문 블록과 XOR 한다. 첫 번째 평문 블록의 경우에는 초기화 벡터(IV)를 암호화한 것과 XOR 한다.
이전 단계의 암호문 블록이 필요하기 때문에 병렬 처리도 불가능하며, 암호문 한 비트의 오류가 다음 불록에도 영향을 주게 된다.
또한 복호화 과정에서는 이전 단계의 암호문 블록을 암호화한 것과 지금 단계의 암호문 블록을 XOR하여 평문을 생성하기 때문에 복호화 로직은 사용하지 않는다.

▶ **OFB**(output feedback, 출력 피드백) 모드
초기화 벡터(IV)를 매 단계마다 반복적으로 암호화해가며 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.
미리 초기화 벡터를 이용해 스트림 암호를 생성해두는 전처리가 가능하며, 오류 전파도 없다.
또한 복호화 과정에서도 CTR 모드와 마찬가지로 별도로 생성된 스트림 암호와 암호문 블록을 XOR하기만 하면 되기 때문에 복호화 로직이 필요 없다.