2018-지방직-정보보호론-B형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)

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.
정답 체크 :
(4) DoS 공격을 받아 데이터 서버가 다운되면 권한을 가진 사용자가 원하는 정보를 얻을 수 없어 가용성을 위협하게 된다.
오답 체크 :
(1) 무결성에 대한 설명이다.
(2) 기밀성에 대한 설명이다.
(3) 정보를 암호화하여 저장하면 기밀성이 보장된다.

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
정답 체크 :
(4) Act : ISMS 관리(유지)와 개선을 수행한다.
오답 체크 :
(1) Plan : ISMS 수립(설립)을 수행한다.
(2) Do : ISMS 구현(실행)과 운영을 수행한다.
(3) Check : ISMS 모니터링(감시)과 검토를 수행한다.
Tip! : ISO/IEC 27001과 27002는 세부 항목이 약간 다르므로 버전에 주의한다.
Tip! : ISMS에서 PDCA 모델을 테이블로 정리하면 다음과 같다.

Plan(계획)	ISMS 설립 : ISMS 정책, 목적, 프로세스, 위험을 관리하여 조직의 전체적인 정책 및 목적에 따른 결과를 산출하도록 정보 보안을 개선하는 적절한 절차를 수립
Do(실행)	ISMS 실행 및 운영 : ISMS 정책과 통제, 프로세스와 절차의 운영
Check(평가)	ISMS 감시와 검토 : ISMS 정책, 목적, 실질적인 경험을 평가 및 측정하고 검토하기 위하여 관리에 대한 결과를 보고
Act(개선)	ISMS 유지 및 개선 : ISMS의 지속적인 개선을 위한 내부 ISMS 감사와 검토 또는 다른 관련 정보를 기반으로 시정이 가능하고 예방적인 행동들을 선택

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

정답 체크 :

(2)

(ㄱ) 로그 : 운영 체제나 다른 소프트웨어가 실행 중에 발생하는 이벤트나 각기 다른 사용자의 통신 소프트웨어 간의 메시지를 기록한 것을 의미한다. 로그를 활용하면 공격자를 추적할 수 있다.

(ㄴ) 세션 : 연결 설정 과정(로그인)을 통해 연결을 맺고 있는 상태를 의미한다. 연결 해제 과정(로그오프)을 하지 않고 웹브라우저를 닫으면 세션은 남아 있는 상태가 되어 공격자가 이를 악용할 수 있다.

(ㄷ) 위협 : 정보자산의 보안에 부정적 영향을 줄 수 있는 외부의 환경 또는 사건(이벤트)을 의미한다.

오답 체크 :

(1) 위험 : 자산의 취약한 부분에 위협요소가 발생하여 자산의 손실, 손상을 유발한 잠재성(가능성)을 의미한다. 위험은 자산, 취약점, 위협의 상관관계(함수)로 표현할 수 있다.

(3) 백업 : 백업 센터나 백업 장비를 이용해서 자신이 처리하고 있는 데이터를 백업하는 것을 의미한다. 백업을 하게 되면 가용성 공격(DoS)을 막을 수 있다.

(4) 쿠키 : 고객이 특정 홈페이지를 접속할 때 생성되는 정보를 담은 임시 파일로 크기는 4KB 이하로 작다. 쿠키는 애초 인터넷 사용자들의 홈페이지 접속을 돕기 위해 만들어졌다. 특정 사이트를 처음 방문하면 아이디와 비밀번호를 기록한 쿠키가 만들어지고 다음에 접속했을 때 별도 절차 없이 사이트에 빠르게 연결할 수 있다.

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

정답 체크 :

(3) chmod a+r : 소유자, 그룹, 기타 사용자에게 읽기 권한 추가

오답 체크 :

(1) chmod u-w : 소유자에게 쓰기 권한 제거
(2) chmod g+wx : 그룹 사용자에게 쓰기와 실행 권한 추가
(4) chmod o-w : 기타 사용자에게 쓰기 권한 제거
Tip! : 파일의 접근모드 변경에 사용되는 사용자 기호와 설정 기호는 다음과 같다.

[사용자 기호]

기호		설명
u	user	파일/디렉토리의 소유자
g	group	파일/디렉토리의 그룹
o	other	다른 사용자
a	all	소유자, 그룹, 다른 사용자 모두 (아무 표시 안할 경우 기본적으로 설정 됨)

[설정 기호]

기호		설명
+	퍼미션 허가	지정한 퍼미션을 허가한다.
-	퍼미션 금지	지정한 퍼미션을 금지시킨다.
=	퍼미션 지정	지정한 퍼미션만 허가하고 나머지는 금지 시킨다.

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
정답 체크 :
(1) A 등급 : Verified Design(검증된 설계)
오답 체크 :
(2) B 등급 : Security Domains(보안 영역), Structured Protection(구조적 보호), Labeled Security(규정된 보호)
(3) C 등급 : Controlled Access Protection(통제된 접근 보호), Discretionary Security Protection(임의적 보호)
(4) D 등급 : Minimal Protection(최소한의 보호)

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)

정답 체크 :

(3) 부채널 공격 : 알고리즘의 약점을 찾거나(암호 해독과는 다름) 무차별 공격을 하는 대신에 암호 체계의 물리적인 구현 과정의 정보를 기반으로 하는 공격 방법이다. 예를 들어, 소요 시간 정보, 소비 전력, 방출하는 전자기파, 심지어는 소리를 통해서 시스템 파괴를 위해 악용할 수 있는 추가 정보를 얻을 수 있다.

오답 체크 :

(1) 차분 암호 분석 공격 : 평문의 일부를 변경할 때 암호문이 어떻게 변화하는지 관찰하여 조사한다.

(2) 중간자 공격 : 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다. 중간자 공격은 통신을 연결하는 두 사람 사이에 중간자가 침입하여, 두 사람은 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달한다.

(4) 재전송 공격 : 보존해 준 정당한 값을 다시 송신하는 공격이다. 예를 들어, 암호화된 패스워드를 저장해 두었다가 다시 사용할 수 있다.

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	Smurf

정답 체크 :

(1)

(ㄱ) Smurf : 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.

(ㄴ) Land : 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이다.

오답 체크 :

(2), (3), (4) Ping of Death : 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).

8. 전자서명법 상 용어의 정의로 옳지 않은 것은?
① ‘전자서명’이라 함은 서명자를 확인하고 서명자가 당해 전자 문서에 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.
정답 체크 :
(3) 서명자 : “전자서명법” 제2조(용어) 상 "서명자"라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.
오답 체크 :
(1) 전자서명 : “전자서명법” 제2조(용어) 상 "전자서명"이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
(2) 인증서 : “전자서명법” 제2조(용어) 상 "인증서"라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
(4) 전자서명생성정보 : “전자서명법” 제2조(용어) 상 "전자서명생성정보"라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

9. 전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드 상 분석·설계 단계 보안요구항목 과 구현 단계 보안 약점을 연결한 것으로 옳지 않은 것은?

분석·설계 단계 보안요구항목	구현 단계 보안 약점
① DBMS 조 회 및 결과 검증	SQL 삽입
② 디렉터리 서비스 조회 및 결과 검증	LDAP 삽입
③ 웹 서비스 요청 및 결과 검증	크로스사이트 스크립트
④ 보안기능 동작에 사용되는 입력값 검증	솔트 없이 일방향 해시함수 사용

정답 체크 :
(4) 보안기능 동작에 사용되는 입력값 검증의 구현 단계 보안 약점은 보안기능 결정에 사용되는 부적절한 입력값, 정수형 오버플로우, Null Pointer 역참조이다. 솔트 없이 일방향 해시함수 사용의 분석·설계 단계 보안요구항목은 암호연산이다.
오답 체크 :
(1) DBMS 조회 및 결과 검증 : SQL 삽입
(2) 디렉토리 서비스 조회 및 결과 검증 : LDAP 삽입
(3) 웹서비스 요청 및 결과 검증 : 크로스사이트 스크립트
Tip! : “전자정보 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드” 상 분석·설계 단계 보안요구항목과 구현 단계 보안약점을 테이블로 정리하면 다음과 같다.

구분	분석·설계 단계 보안요구항목	구현 단계 보안약점
입력 데이터 검증 및 표현	DBMS 조회 및 결과 검증	SQL 삽입
	XML 조회 및 결과 검증	XQuery 삽입 XPath 삽입
	디렉터리 서비스 조회 및 결과 검증	LDAP 삽입
	시스템 자원 접근 및 명령어 수행 입력값 검증	경로조작 및 자원삽입 운영체제 명령어 삽입
	웹 서비스 요청 및 결과 검증	크로스사이트 스크립트
	웹 기반 중요기능 수행 요청 유효성 검증	크로스사이트 요청 위조
	HTTP프로토콜 유효성 검증	신뢰되지 않은 URL 주소로 자동접속 연결 HTTP 응답분할
	허용된 범위내 메모리 접근	포맷스트링 삽입 메모리 버퍼 오버플로우
	보안기능 동작에 사용되는 입력값 검증	보안기능 결정에 사용되는 부적절한 입력값 정수형 오버플로우 Null Pointer 역참조
	업로드·다운로드 파일 검증	위험한 형식 파일 업로드 무결성 검사 없는 코드 다운로드
보안 기능	인증대상 및 방식	적절한 인증 없는 중요기능 허용 DNS lookup에 의존한 보안결정
	인증수행 제한	반복된 인증시도 제한기능 부재
	비밀번호 관리	하드코드된 비밀번호 취약한 비밀번호 허용
	중요자원 접근통제	부적절한 인가 중요한 자원에 대한 잘못된 권한 설정
	암호키 관리	하드코드된 암호화 키 주석문 안에 포함된 시스템 주요 정보
	암호연산	취약한 암호화 알고리즘 사용 충분하지 않은 키 길이 사용 적절하지 않은 난수 값 사용 솔트없이 일방향 해시함수 사용
	중요정보 저장	중요정보 평문저장 사용자 하드디스크에 저장되는 쿠키를 통한 정보노출
	중요정보 전송	중요정보 평문전송
에러 처리	예외처리	오류메시지를 통한 정보노출 시스템 데이터 정보노출
세션 통제	세션통제	잘못된 세션에 의한 데이터 정보노출

10. 개인정보 보호법령상 영업 양도 등에 따른 개인정보의 이전 제한에 대한 내용으로 옳지 않은 것은?

① 영업 양수자등은 영업의 양도·합병 등으로 개인정보를 이전 받은 경우에는 이전 당시의 본래 목적으로 만 개인정보를 이용하거나 제3자에게 제공할 수 있다.

② 영업 양수자등이 과실 없이 서면 등의 방법으로 개인정보를 이전 받은 사실 등을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 10일 이상 게재하여야 한다.

③ 개인정보 처리자는 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 영업 양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 서면 등의 방법에 따라 정보주체에게 알려야한다. 다만, 개인정보 처리자가 개인정보 보호법 제27조제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.
정답 체크 :
(2) “개인정보 보호법 시행령” 제29조(영업양도 등에 따른 개인정보 이전의 통지) 상 ① "개인정보 보호법" 제27조제1항 각 호 외의 부분과 같은 조 제2항 본문에서 "대통령령으로 정하는 방법"이란 서면등의 방법을 말한다. ② "개인정보 보호법" 제27조제1항에 따라 개인정보를 이전하려는 자(이하 이 항에서 "영업양도자등"이라 한다)가 과실 없이 제1항에 따른 방법으로 "개인정보 보호법" 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 영업양도자등의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.
오답 체크 :
(1) “개인정보 보호법” 제27조(영업양도 등에 따른 개인정보의 이전 제한) 상 영업양수자등은 영업의 양도ㆍ합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.
(3) “개인정보 보호법” 제27조(영업양도 등에 따른 개인정보의 이전 제한) 상 개인정보처리자는 영업의 전부 또는 일부의 양도ㆍ합병 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
(4) 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 “개인정보 보호법” 제27조제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

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
정답 체크 :
(3)
(ㄱ) AES : 128비트 블록 길이, 128/192/256 비트 키 길이를 가진다. 키의 길이에 따라

12/14/16 라운드가 결정되며 SPN 구조(별도의 복호화기가 필요)를 가진다.
(ㄴ) DES : 16라운드 Feistel 구조(별도의 복호화기가 필요 없음)를 가진다.
(ㄷ) ARIA : 128비트 블록 길이, 128/192/256 비트 키 길이를 가진다. 키의 길이에 따라 12/14/16 라운드가 결정되며 Involutional SPN 구조(SPN 구조임에도 별도의 복호화기가 필요 없음)를 가진다.
오답 체크 :
(1), (4)
(ㄹ) SEED : 16라운드 Feistel 구조(별도의 복호화기가 필요 없음)를 가진다.
(2) ㄱ이 없다.

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)
정답 체크 :
(4) WEP : 1997년 재정된 802.11 표준에서 도입되었던 WEP는 전통적인 유선 네트워크와 비슷한 데이터 보안성을 제공하기 위해 만들어졌다. 64비트 또는 128비트 키값을 사용하는 WEP는, 한때 매우 보편적으로 사용되었으며 라우터의 보안 설정에서 가장 우선적으로 표시되는 옵션이었다. 2001년 초, 암호학자들이 몇 가지 치명적인 취약점을 발견하였으며, 이를 이용하면 누구나 구할 수 있는 소프트웨어를 사용해 몇 십 분만에 WEP 연결을 크랙할 수 있다. 암호화를 위해 RC4를 사용한다.
오답 체크 :
(1) AH : IPSec에서 인증과 무결성을 제공하기 위해서 사용된다.
(2) SSH : 두 호스트(Host) 사이의 통신 암호화 관련 인증 기술들을 사용하여, 안전한 접속과 통신을 제공하는 프로토콜을 의미한다. 안전한 ftp 혹은 telnet을 사용할 수 있다.
(3) WAP : 휴대 전화 등의 장비에서 인터넷을 하는 것과 같은, 무선 통신을 사용하는 응용 프로그램의 국제 표준이다. WAP은 매우 작은 이동 장비에 웹 브라우저와 같은 서비스를 제공하기 위해 설계되었다. WAP의 구조는 네트워크, 전송, 보안(기존 유선 구조에서는 없음), 세션, 응용 계층 등으로 구성된다.

13. 기밀성을 제공하는 암호 기술이 아닌 것은?
① RSA
② SHA-1
③ ECC
④ IDEA
정답 체크 :
(2) SHA-1 : 해시로 무결성을 제공한다.
오답 체크 :

(1) RSA : 공개키로 기밀성을 제공한다.
(3) ECC : 공개키로 기밀성을 제공한다.
(4) IDEA : 대칭키로 기밀성을 제공한다.

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.
정답 체크 :
(1) 전송계층과 응용계층 사이에서 동작한다.
오답 체크 :
(2) 인증(인증서-상대, MAC-데이터), 기밀성(대칭암호), 무결성(MAC)을 제공한다.
(3) Handshake : 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유키를 결정한다. 인증서를 이용한 인증을 수행한다.
(4) Record : 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.

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.
정답 체크 :
(1) DSA는 디지털 서명(부인 방지)에만 사용된다. 즉, 암호화(기밀성)에 사용되지 않는다.
오답 체크 :
(2) NIST가 1991년에 제정한 디지털 서명 알고리즘이다.
(3) SHA-1, SHA-2의 해시 함수가 사용된다.
(4) DSA는 이산대수문제에 기반 한다.

16. 무의미한 코드를 삽입하고 프로그램 실행 순서를 섞는 등 악성 코드 분석가의 작업을 방해하는 기술은?
① 디스어셈블(Disassemble)
② 난독화(Obfuscation)
③ 디버깅(Debugging)
④ 언패킹(Unpacking)
정답 체크 :
(2) 난독화 ; 무의미한 코드를 삽입하거나 goto 문을 사용해서 프로그램 실행 순서를 섞어서 역공학(리버싱 또는 리버스 엔지니어링, 기계어를 소스코드로 변환하는 것)을 방해하는 것이다.

오답 체크 :
(1) 디스어셈블 : 기계어(이진 파일, 실행 파일)를 어셈블리어를 변환하는 것을 의미한다.
(3) 디버깅 : 컴퓨터 프로그램이나 시스템의 정확성 또는 논리적인 오류(버그)를 검출하여 제거하는 과정이다. 디버깅을 통해 코드 흐름과 메모리 상태 등을 자세히 볼 수 있어 역공학에 이용된다.
(4) 언패킹 : 역공학을 어렵게 만들기 위해 패킹(압축 및 암호화)을 하고, 이를 사용하기 위해 복원하는 것을 언패킹이라고 한다.

17. 윈도우즈 용 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.
정답 체크 :
(2) arp : IP 주소(논리 주소)에 대한 MAC 주소(물리 주소)를 제공한다. 참고로, rarp는 MAC 주소에 대한 IP 주소를 제공한다.
오답 체크 :
(1) ping : tracert에 대한 설명을 의미한다.
(3) tracert : ipconfig에 대한 설명을 의미한다.
(4) ipconfig : ping에 대한 설명을 의미한다.

18. 정보자산에 대한 위험분석에서 사용하는 ALE(Annualized Loss Expectancy, 연간예상손실액), SLE(Single Loss Expectancy, 1회 손실 예상액), ARO(Annualized Rate of Occurrence, 연간발생빈도) 사이의 관계로 옳은 것은?
① ALE = SLE + ARO
② ALE = SLE × ARO
③ SLE = ALE + ARO
④ SLE = ALE × ARO
정답 체크 :
(2)
ALE는 보안 투자로부터 얻을 수 있는 최대 편익을 의미한다. ALE를 넘어가는 연간 보안 투자는 비효율적이다. ALE가 20만 달러이고 연간 보안 예산이 25만 달러이면 비효율적이다. ALE는 SLE x ARO로 계산한다.
Tip! : ALE를 테이블로 정리하면 다음과 같다.

Concept	Derivation Formula	설 명
Exposure Factor (EF)	% of Asset loss caused by threat	위협에 의해 야기 될 수 있는 자산 손실률 (0~100%의 백분율로 표시)
Single Loss Expectancy (SLE)	Asset Value x (EF)	단일 위협으로부터 발생되는 조직의 손실 기대치 (1회 손실액) (단일 예산 손실)
Annualized Rate of Occurrence (ARO)	Frequency of threat occurrence per year	위협 실현의 년간 빈도 수 (연간 발생 비율) (역사적 기록, 통계적 분석, 추측 등)
Annualized Loss Expectancy (ALE)	(SLE) x (ARO)	위협에 의한 조직의 년간 재정적 손실 (연간 예산 손실)

19. 개인정보 보호법 상 개인정보 보호원칙으로 옳지 않은 것은?
① 개인정보 처리자는 개인정보의 처리 목적을 명확하게 하여야하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보 처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야하며, 그 목적 외의 용도로 활용하여서는 아니된다.
③ 개인정보 처리자는 개인정보의 익명 처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록하여야 한다.
④ 개인정보 처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비밀로하여야 한다.
정답 체크 :
(4) “개인정보 보호법” 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
오답 체크 :
(1) “개인정보 보호법” 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
(2) “개인정보 보호법” 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
(3) “개인정보 보호법” 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
Tip! : 이외에도 “개인정보 보호법” 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다. 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다. 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다. 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

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

정답 체크 :

(4) CTR : 아래 그림에서 보는 바와 같이 암호화/복호화 병렬 처리가 가능하다(이전 단계의 영향을 받지 않는다). 암호화/복호화시에 암호화 로직만 사용한다(즉, 복호화 로직을 사용하지 않는다). 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다(즉, 에러가 전파되지 않는다).

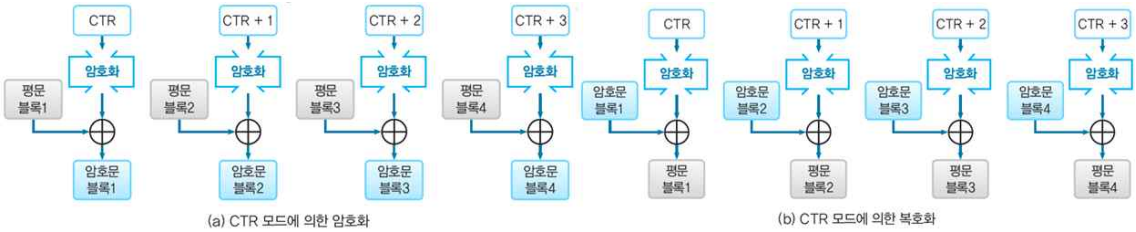


그림 5-15 • CTR 모드(카운터 모드)

오답 체크 :

(1) ECB : 아래 그림에서 보는 바와 같이 암호화/복호화 병렬 처리가 가능하다(이전 단계의 영향을 받지 않는다). 암호화시에 암호화 로직을 사용하고 복호화시에 복호화 로직을 사용한다. 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다(즉, 에러가 전파되지 않는다).

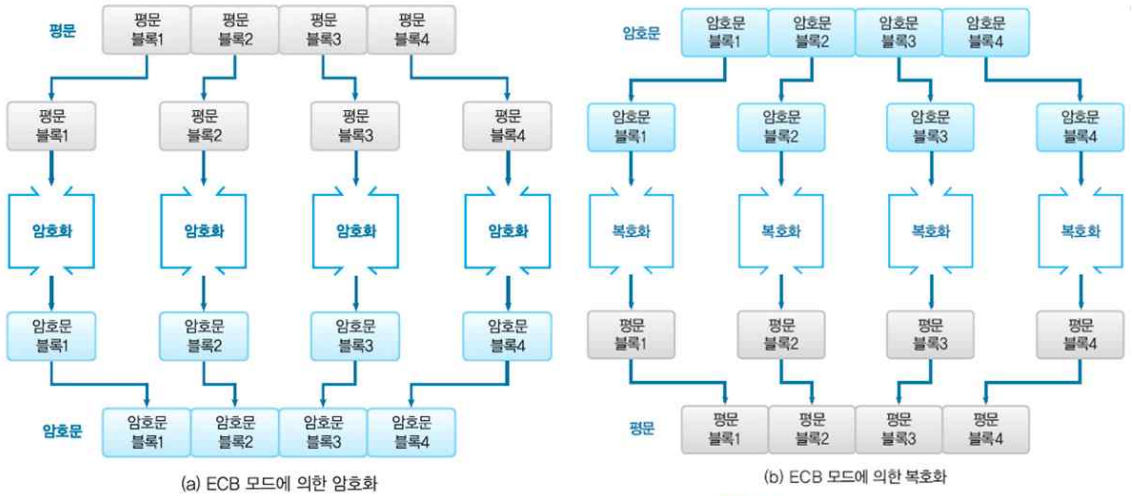
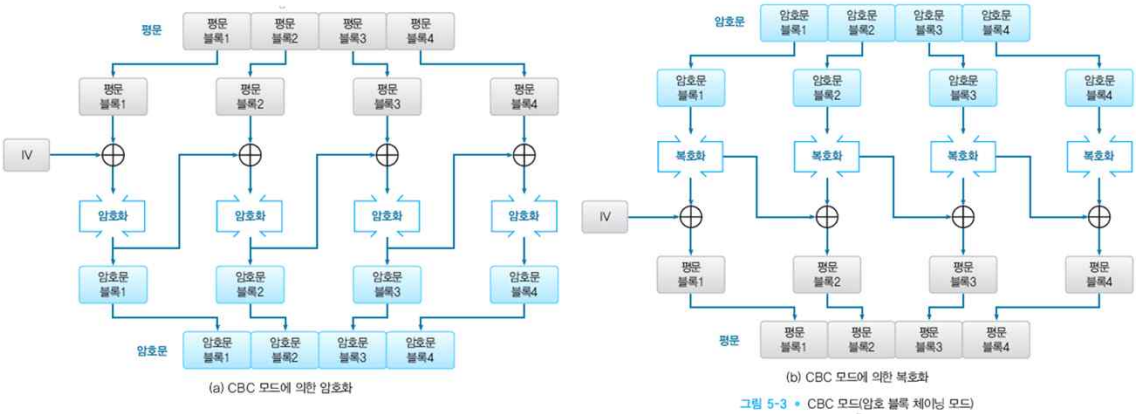


그림 5-2 • ECB 모드(전자 코드북 모드)

(2) CBC : 아래 그림에서 보는 바와 같이 복호화는 병렬 처리가 가능하지만 암호화는 병렬 처리가 가능하지 않다(즉, 이전 단계의 영향을 받는다). 암호화시에 암호화 로직을 사용하고 복호화시에 복호화 로직을 사용한다. 암호문의 한 비트 오류는 복호화되는 평문의 한 비트와 다음 복호화되는 평문에 영향을 준다(즉, 에러가 전파된다).

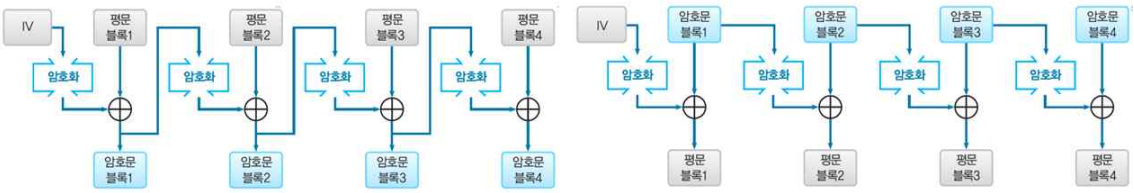


(a) CBC 모드에 의한 암호화

(b) CBC 모드에 의한 복호화

그림 5-3 • CBC 모드(암호 블록 체이닝 모드)

(3) CFB : 아래 그림에서 보는 바와 같이 복호화는 병렬 처리가 가능하지만 암호화는 병렬 처리가 가능하지 않다(즉, 이전 단계의 영향을 받는다). 암호화/복호화시에 암호화 로직만 사용한다(즉, 복호화 로직을 사용하지 않는다). 암호문의 한 비트 오류는 복호화되는 평문의 한 비트와 다음 복호화되는 평문에 영향을 준다(즉, 에러가 전파된다).



(a) CFB 모드에 의한 암호화

(b) CFB 모드에 의한 복호화

그림 5-9 • CFB 모드(암호 피드백 모드)