2018 국가직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

문 1. 전자우편 보안 기술이 목표로 하는 보안 특성이 아닌 것은?

① 익명성
② 기밀성
③ 인증성
④ 무결성

답 ①

① 익명성(anonymity)은 정보를 전달하는 주체의 신원을 숨기는 것을 의미하는데, 전자우편에서는 굳이 송신자의 신원을 숨길 필요가 없다. 오히려 송신자의 신원을 확인할 수 없다면 수신자는 전자우편을 읽지도 않고 폐기 처분할 것이다.

<오답 체크> ② 기밀성(Confidentiality): 비인가자에게는 메시지를 숨겨야 함

③ 인증(authentication): 정당한 상대방인지, 진짜인지 가짜인지를 확인하는 것

④ 무결성(Integrity): 데이터가 위·변조되지 않아야 함

문 2. 프로그램이나 손상된 시스템에 허가되지 않는 접근을 할 수 있도록 정상적인 보안 절차를 우회하는 악성 소프트웨어는?

① 다운로더(downloader)
② 키 로거(key logger)
③ 봇(bot)
④ 백도어(backdoor)

답 ④

④ **백도어**(backdoor)
인증 과정을 거치지 않고, 접근할 수 있도록 만든 비밀 통로 또는 그러한 프로그램을 의미한다. = 트랩도어(Trapdoor)

<오답 체크> ① **다운로더**(downloader)
다운로더는 이용자의 적절한 동의 없이 소프트웨어를 다운로드하여 설치하는 프로그램을 말한다.

② **키로거**(key logger)
사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록하는 소프트웨어를 말한다.

③ **봇**(bot)
로봇의 준말로서, 사용자나 다른 프로그램 또는 사람의 행동을 흉내내어 대리자로 동작하는 프로그램을 의미한다.
정보보호에서 악성 봇은 해커에 의해 악성 프로그램에 감염되어 DDoS(분산 서비스 거부 공격) 등에 이용되는 좀비PC 등을 의미한다.

문 3. 프로그램을 감염시킬 때마다 자신의 형태뿐만 아니라 행동 패턴까지 변화를 시도하기도 하는 유형의 바이러스는?

① 암호화된(encrypted) 바이러스
② 매크로(macro) 바이러스
③ 스텔스(stealth) 바이러스
④ 메타모픽(metamorphic) 바이러스

답 ④

④ **메타모픽**(metamorphic) 바이러스
다형성 바이러스의 발전된 형태로, 감염될 때마다 암호화 루틴만 랜덤한 형태로 변하는 게 아닌 바이러스 코드 자체를 새로 만들어내는 바이러스.
자신의 행태뿐 아니라 행동 패턴까지 변화를 시도한다는 점에서 단순 암호화 루틴뿐 아니라 코드 자체를 변화시키는 메타모픽 바이러스에 해당한다.

▷ **다형성**(polymorphic) 바이러스(**폴리모픽** 바이러스)
감염될 때마다 암호를 푸는 루틴이 달라지는 다형성 기법(Polymorphic Technique)이 적용된 바이러스

<오답 체크> ① **암호화**(encrypted) 바이러스
바이러스 프로그램의 일부 또는 대부분을 암호화시켜 저장한 바이러스

② **매크로**(macro) 바이러스
MS 사 오피스 제품군(워드, 엑셀, 파워포인트) 이외에 비지오(Visio), 오토캐드(AutoCAD) 등 매크로 기능이 있는 응용 소프트웨어 안에서 실행되는 바이러스
실행 파일이 아닌 문서 파일에 감염되고 실행 파일보다 빈번하게 교환이 이뤄지는 문서의 특성상 보다 빨리 퍼지게 된다.

③ **은폐형**(stealth) 바이러스(**스텔스** 바이러스)
자신을 은폐하고 사용자나 백신 프로그램에 거짓 정보를 제공하기 위해서 다양한 기법을 사용하는 바이러스.
기억 장소에 존재하면서 감염된 파일의 길이가 증가하지 않은 것처럼 보이게 하고, 백신 프로그램이 감염된 부분을 읽으려고 할 때 감염되기 전의 내용을 보여줘 바이러스가 없는 것처럼 백신 프로그램이나 사용자를 속인다.

문 4. 증거의 수집 및 분석을 위한 디지털 포렌식의 원칙에 대한 설명으로 옳지 않은 것은?

① 정당성의 원칙 - 증거 수집의 절차가 적법해야 한다.
② 연계 보관성의 원칙 - 획득한 증거물은 변조가 불가능한 매체에 저장해야 한다.
③ 신속성의 원칙 - 휘발성 정보 수집을 위해 신속히 진행해야 한다.
④ 재현의 원칙 - 동일한 조건에서 현장 검증을 실시하면 피해 당시와 동일한 결과가 나와야 한다.

답 ②

② 변조를 방지한다는 내용은 **무결성의 원칙**에 대한 내용이다.
연계 보관성의 원칙은 증거의 이송/분석/보관/법정 제출이라는 일련의 과정에 대한 추적이 가능해야 한다는 것이다.

◈ 포렌식의 원칙
▷ **재현**의 원칙
증거를 복구하는 과정에서 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함
▷ **정당성**의 원칙
모든 증거는 적법한 절차를 거쳐서 획득하여야 함
▷ **신속성**의 원칙
시스템 안의 디스크 또는 메모리 정보가 휘발되기 전에 빠르게 획득하여야 함
▷ **연계보관성**의 원칙
증거의 이송/분석/보관/법정 제출이라는 일련의 과정에 대한 추적이 가능해야 함
▷ **무결성**의 원칙
증거가 위조/변조되어서는 안 됨

문 5. 웹 애플리케이션의 대표적인 보안 위협의 하나인 인젝션 공격에 대한 대비책으로 옳지 않은 것은?

① 보안 프로토콜 및 암호 키 사용 여부 확인
② 매개변수화된 인터페이스를 제공하는 안전한 API 사용
③ 입력 값에 대한 적극적인 유효성 검증
④ 인터프리터에 대한 특수 문자 필터링 처리

답 ①

SQL 삽입(SQL 인젝션, SQL injection) 공격은 클라이언트의 입력값을 조작하여 관리자가 예상하지 못한 명령을 실행하거나, 정당한 권한을 획득하지 않고 부정한 방법으로 데이터베이스에 접근하는 공격이다.

① 인젝션 공격은 입력값을 조작하는 방법으로 이루어지기 때문에, 입력되는 값을 검사하고 서버의 구조가 드러나지 않도록 통제하는 것이 중요하다.
프로토콜과 암호 키를 사용하는 것은 서버와 클라이언트 사이에 안전한 연결 및 인증을 위한 보안 방법으로, 인젝션 공격과는 관계가 없다.

◈ SQL 삽입에 대한 대책
▷ 스크립트의 모든 파라미터들을 점검하여 사용자의 입력 값이 SQL injection을 발생시키지 않도록 수정
▷ 입력 시 특수문자가 포함되어 있는지 검사하여 허용되지 않은 문자열이나 문자가 포함된 경우에는 에러로 처리
▷ SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정
공격자는 에러 메시지를 분석하여 공격법을 찾는 데 활용하기 때문이다.
▷ 매개변수화 된 인터페이스를 제공하는 안전한 API 사용

문 6.「개인정보 보호법」상의 개인정보의 수집·이용 및 수집 제한에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

② 개인정보처리자는「개인정보 보호법」에 따라 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

③ 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.

④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니하는 경우 정보주체에게 재화 또는 서비스의 제공을 거부할 수 있다.

답 ④

「개인정보 보호법」

제2조(정의) 5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. **정보주체의 동의**를 받은 경우
2. 법률에 특별한 규정이 있거나 **법령상 의무를 준수하기 위하여 불가피**한 경우
3. 공공기관이 법령 등에서 정하는 소관 **업무의 수행을 위하여 불가피**한 경우
4. 정보주체와의 **계약의 체결 및 이행을 위하여 불가피**하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 **정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요**하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 **명백하게 정보주체의 권리보다 우선**하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

제16조(개인정보의 수집 제한)

① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 **입증책임은 개인정보처리자**가 부담한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 **동의하지 아니할 수 있다는 사실**을 구체적으로 알리고 개인정보를 수집하여야 한다.

③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 **재화 또는 서비스의 제공을 거부하여서는 아니 된다.**

문 7. <보기 1>은 리눅스에서 일반 사용자(hello)가 'ls –al'을 수행한 결과의 일부분이다. <보기 2>의 설명에서 옳은 것만을 모두 고른 것은?

〈 보 기 1 〉

-rwxr-xr-x 1 hello world 4096 Nov 21 15:12 abc.txt
ⓐ ⓑ

〈 보 기 2 〉

ㄱ. ⓐ는 파일의 소유자, 그룹, 이외 사용자 모두가 파일을 읽고 실행할 수 있지만, 파일의 소유자만이 파일을 수정할 수 있음을 나타낸다.
ㄴ. ⓑ가 모든 사용자(파일 소유자, 그룹, 이외 사용자)에게 읽기, 쓰기, 실행 권한을 부여하려면 'chmod 777 abc.txt'의 명령을 입력하면 된다.
ㄷ. ⓑ가 해당 파일의 소유자를 root로 변경하려면 'chown root abc.txt'의 명령을 입력하면 된다.

① ㄱ ② ㄱ, ㄴ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

답 ②

ls 명령어는 파일 목록을 보여주는 명령어이다.
옵션으로 -a은 디렉토리 내의 모든 파일 출력, -l은 파일의 권한, 소유자, 그룹, 크기, 날짜 등을 출력한다.

-rwxr-xr-x 1 hello world 4096 Nov 21 15:12 abc.txt를 살펴보자.
ⓐ -rwxr-xr-x : 파일 종류 및 권한.
d는 디렉터리, -는 일반 파일. r 읽기, w 쓰기 x 실행
1 : 링크 수, 일반 파일은 대개 1이다.
ⓑ hello : 소유자
world : 그룹
4096 : 용량
Nov 21 15:12 : 마지막 수정한 날짜
abc.txt : 파일명

ㄱ. rwxr-xr-x은 앞에서부터 세 자리씩 소유자, 그룹, 기타 사용자의 권한이다. 소유자는 rwx 읽기, 쓰기, 실행이 모두 가능하고, 그룹과 기타 사용자는 w 권한이 빠져있다. 파일을 수정하는 것이 쓰기 권한이다.
ㄴ. **chmod**(change mode)는 파일이나 디렉터리에 대한 권한을 변경하는 명령어이다.
chmod 777은 앞에서부터 소유자, 그룹, 기타 사용자에게 각각 7, 7, 7의 권한을 부여한다는 의미이다.
7은 이진수로 111이 되는데, 이것은 rwx에 각각 1, 1, 1의 권한(허용)을 부여하겠다는 것이다.
예를 들어, 5의 권한은 101이므로, r과 x에는 허용을, w에는 금지를 하겠다는 것이다.

▶ 옵션 -R: 하위 디렉터리의 모든 권한 변경
▶ SetUid 설정: 권한에 4000을 붙인다. ex) chmod 4777
SetGid 설정: 권한에 2000을 붙인다.
Sticky bit(스티키 비트) 설정: 1000을 붙인다.

<오답 체크> ㄷ. **chown**(change owner)는 파일 또는 폴더의 소유권을 바꾸는 명령어이다.
그런데 chown은 소유자뿐 아니라 그룹도 변경할 수 있다. 앞으로 정보보호론 시험이 어려워질 경우 좀 더 심층적으로 나올 수 있으므로 알아두자.
우선 명령어 형식은 **chown [옵션] [소유자 : 그룹명] [파일]** 이다.
▶ 옵션 -R: 하위 디렉터리의 모든 권한 변경
▶ [소유자:그룹] 부분을 통해 소유자와 그룹을 한 번에 변경할 수 있다.
소유자 – 소유자만 변경한다.
: 그룹명 – 그룹만 변경한다.
소유자 : – 소유자와 그룹 모두 동일한 것으로 변경한다.
소유자 : 그룹명 – 소유자와 그룹을 각각 다른 것으로 변경한다. (같은 것으로 해도 상관없다.)

그런데 파일의 소유권을 변경할 때는 루트 계정의 권한이 필요하다. 일반 사용자로 로그인한 경우에는 앞에 **sudo**(substitute user do)를 붙여야 한다.
sudo는 뒤에 입력한 명령어를 루트 권한으로 실행할 수 있게 해주는 명령어이다.
따라서 일반사용자인 hello가 파일의 소유자를 root로 변경하려면, **'sudo chown root abc.txt'**의 명령을 입력해야 한다.

문 8. 다음은 CC(Common Criteria)의 7가지 보증 등급 중 하나에 대한 설명이다. 시스템이 체계적으로 설계되고, 테스트되고, 재검토되도록(methodically designed, tested and reviewed) 요구하는 것은?

> 낮은 수준과 높은 수준의 설계 명세를 요구한다. 인터페이스 명세가 완벽할 것을 요구한다. 제품의 보안을 명시적으로 정의한 추상화 모델을 요구한다. 독립적인 취약점 분석을 요구한다. 개발자 또는 사용자가 일반적인 TOE의 중간 수준부터 높은 수준까지의 독립적으로 보증된 보안을 요구하는 곳에 적용 가능하다. 또한 추가적인 보안 관련 비용을 감수할 수 있는 곳에 적용 가능하다.

① EAL 2 ② EAL 3
③ EAL 4 ④ EAL 5

답 ③

CC(Common Criteria, 국제공통평가기준)
국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준이다.

EAL(평가보증등급)
국제공통평가기준인 **CC**에서 정의한 제품의 보증등급으로, EAL1에서 EAL7까지 7단계로 구분

TCSEC	CC
D: Minimal protection (최소한의 보호)	EAL1: Functionally Tested (기능시험)
C1: Discretionary Security Protection (임의적 보호)	EAL2: Structurally Tested (구조시험)
C2: Controlled Access Protection (통제된 보호)	EAL3: Methodically Tested and Checked (방법론적 시험과 점검)
B1: Labeled Security Protection (레이블된 보호)	EAL4: Methodically Designed, Tested and Reviewed (방법론적 설계, 시험 및 검토)
B2: Structured Protection (구조적 보호)	EAL5: Semiformally Designed and Tested (준정형적 설계 및 시험)
B3: Security Domains (보안영역)	EAL6: Semiformally Verified Design and Tested (준정형적 검증된 설계 및 시험)
A: Verified protection (검증된 설계)	EAL7: Formally Verified Design and Tested (정형적 검증)

문 9. 다음에 설명한 Diffie-Hellman 키 교환 프로토콜의 동작 과정에서 공격자가 알지 못하도록 반드시 비밀로 유지해야 할 정보만을 모두 고른 것은?

> 소수 p와 p의 원시근 g에 대하여, 사용자 A는 p보다 작은 양수 a를 선택하고, $x = g^a \bmod p$를 계산하여 x를 B에게 전달한다. 마찬가지로 사용자 B는 p보다 작은 양수 b를 선택하고, $y = g^b \bmod p$를 계산하여 y를 A에게 전달한다. 그러면 A와 B는 $g^{ab} \bmod p$를 공유하게 된다.

① a, b
② p, g, a, b
③ a, b, $g^{ab} \bmod p$
④ p, g, a, b, $g^{ab} \bmod p$

답 ③

디피 헬만에서 반드시 비밀로 유지해야 하는 정보는 각 사용자가 선택한 임의의 정수 **a와 b**뿐이다. 처음 선택한 소수들 p와 g, 그리고 양쪽이 주고 받은 계산값 $x = g^a \bmod p$, $y = g^b \bmod p$는 누가 알아도 상관 없다.
또한 마지막 계산한 값 $g^{ab} \bmod p$가 양쪽이 공유하는 비밀키(대칭키)가 된다. 따라서 당연히 이 키 값은 비밀을 유지해야 한다.

◈ 디피 헬만 키 교환 순서
1. 앨리스가 충분히 큰 소수 p와 g를 선택하여 밥에게 전송한다.
   g는 1부터 p-1 사이의 수이다. p와 g는 누구의 손에 들어가도 상관 없다.
2. 앨리스가 정수 a를 선택한다. **a는 외부에 공개되지 않으며**, 밥 또한 알 수 없다.
3. 앨리스가 $A = g^a \bmod p$, 즉 g^a를 p로 나눈 나머지를 계산한다. A는 공개해도 상관 없다.
4. 밥도 마찬가지로 정수 b를 선택하여 $B = g^b \bmod p$ 를 계산한다. 역시 **b는 외부에 공개되지 않으며**, B는 누구의 손에 들어가도 상관 없다.
5. 앨리스와 밥이 서로에게 A와 B를 전송한다.
6. 앨리스가 $B^a \bmod p$를, 밥이 $A^b \bmod p$를 계산한다.
   $B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$
   $A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$ 으로 같다.
   이로써 앨리스와 밥은 공통의 비밀키($g^{ab} \bmod p$)를 갖게 된다.

문 10. IEEE 802.11i에 대한 설명으로 옳지 않은 것은?

① 단말과 AP(Access Point) 간의 쌍별(pairwise) 키와 멀티캐스팅을 위한 그룹 키가 정의되어 있다.
② 전송되는 데이터를 보호하기 위해 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol) 방식을 지원한다.
③ 서로 다른 유무선랜 영역에 속한 단말들의 종단간(end-to-end) 보안 기법에 해당한다.
④ 802.1X 표준에서 정의된 방법을 이용하여 무선 단말과 인증 서버 간의 상호 인증을 할 수 있다.

답 ③

▷ **802.11i**는 802.11 무선랜 보안 표준 기술에 보안성을 강화한 기술로, WPA/WPA2 방식을 사용한다.
WPA는 RC4-TKIP
WPA2는 AES-CCMP알고리즘을 사용한다.

③ 801.11i에서는 WiFi 단말기(Station, STA)들을 인증하기 위한 별도의 인증 서버가 존재한다. 인증을 위해 단말과 AP(Access Point) 사이는 802.1x/EAP 프로토콜을 사용하고, AP와 인증서버 사이는 RADIUS 프로토콜을 사용한다.
단말이 AP를 인증 요청을 신호를 보내면, AP는 그 요청을 인증 서버로 전송하여 인증 서버가 단말 인증을 한다.
종단간(end-to-end) 보안 방식이란, 중간에 서버를 두지 않고 단말기에서 단말기로 직접 암호화/인증을 수행하는 방식을 말한다.

문 11. SSL(Secure Socket Layer)에서 메시지에 대한 기밀성을 제공하기 위해 사용되는 것은?

① MAC(Message Authentication Code)
② 대칭키 암호 알고리즘
③ 해시 함수
④ 전자서명

답 ②

② SSL/TLS는 기본적으로 기밀성을 위해서 대칭키를, 무결성을 위해서 메시지 인증 코드(MAC)를 사용한다.
하지만 대칭키 방식의 키 관리 어려움으로 인해 공개키 방식 또한 사용한다.

▷ **SSL**(Secure Sockets Layer, **보안 소켓 레이어**) **또는**
TLS(Transport Layer Security, **전송 계층 보안**)
응용 계층과 전송 계층 사이에서 통신 과정에서 종단간 보안과 데이터 무결성을 제공하는 보안 프로토콜
클라이언트와 서버 간 상호 인증과 기밀성과 무결성 서비스를 제공
인터넷 전자상거래를 위해 넷스케이프사가 개발한 것으로, 웹 브라우저와 웹 서버 간의 전자상거래 정보를 안전하게 전송하기 위한 프로토콜이다.

문 12. 메시지 인증에 사용되는 해시 함수의 요건으로 옳지 않은 것은?

① 임의 크기의 메시지에 적용될 수 있어야 한다.
② 해시를 생성하는 계산이 비교적 쉬워야 한다.
③ 다양한 길이의 출력을 생성할 수 있어야 한다.
④ 하드웨어 및 소프트웨어에 모두 실용적이어야 한다.

답 ③

③ 대부분의 해시 함수는 입력 메시지의 길이에 상관없이 출력되는 해시값의 길이는 동일하다.

◈ **출력 해시값 길이**
SHA-0, SHA-1 : 160비트
SHA-224 : 224비트
SHA-256 : 256 비트
SHA-384 : 384비트
SHA-512 : 512 비트
MD4, MD5 : 128비트
RIPEMD-128 : 128비트
RIPEMD-160 : 160비트
HAVAL : 128~256비트의 가변 길이를 출력

문 13. 사용자 A가 사용자 B에게 보낼 메시지 M을 공개키 기반의 전자 서명을 적용하여 메시지의 무결성을 검증하도록 하였다. A가 보낸 서명이 포함된 전송 메시지를 다음 표기법에 따라 바르게 표현한 것은?

PU_X: X의 공개키
PR_X: X의 개인키
E(K, M): 메시지 M을 키 K로 암호화
H(M): 메시지 M의 해시
||: 두 메시지의 연결

① $E(PU_B, M)$ ② $E(PR_A, M)$
③ $M \,||\, E(PU_B, H(M))$ ④ $M \,||\, E(PR_A, H(M))$

답 ④

전자 서명은 공개키 방식을 이용하는데 공개키 방식은 대칭키 방식보다 암호화/복호화에 걸리는 시간이 길기 때문에, 메시지가 아닌 메시지의 해시값에 서명을 한다.
또한 전자 서명은 송신자는 자신의 개인키를 사용하여 서명을 하고, 수신자는 송신자의 공개키를 사용하여 서명을 검증한다.

1. 먼저 메시지(M)의 해시값 H(M)을 구한다.
2. 1에서 구한 해시값을 송신자 자신의 개인키로 암호화를 한다.
   $E(PR_A, H(M))$
3. 여기에 원문 메시지(M)를 첨부하여 압축한 뒤 전송한다.
   $M \,||\, E(PR_A, H(M))$
4. 수신자는 전송받은 데이터의 압축을 푼다.
5. 송신자의 공개키(PU_A)를 이용하여 복호화를 하여 데이터 안의 H(M)값을 얻는다.
   $D(PU_A, E(PR_A, H(M))) = H(M)$
6. 수신자는 본인이 직접 원문 메시지(M)로부터 해시값 H'(M)을 구한다.
7. 전송받은 해시값 H(M)과 자신이 구한 해시값 H'(M)의 일치 여부를 확인하여 서명이 옳은지 확인한다.

문 14. 대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(error propagation)가 발생하지 않는 모드만을 묶은 것은? (단, ECB: Electronic Code Book, CBC: Cipher Block Chaining, CFB: Cipher Feedback, OFB: Output Feedback)

① CFB, OFB ② ECB, OFB
③ CBC, CFB ④ ECB, CBC

답 ②

② ECB는 모든 블록이 개별적으로 작동하기 때문에 오류 전파가 없다.
OFB는 평문이나 암호문과는 무관한 별도의 스트림 암호를 생성하여 암호화에 이용하기 때문에 평문 블록의 오류가 다른 블록으로 전파되지 않는다.
또한 CTR 방식 역시 별도의 카운터 값을 이용하기 때문에 오류 전파가 없다.

<오답 체크> ③ CBC와 CFB는 암호문 블록을 다음 단계의 암호화에 이용하는데, 평문 블록이 오류가 있으면 그 단계의 암호문 블록에 오류가 발생하여 다음 단계의 암호문 블록에도 영향을 미치기 때문에 오류가 전파된다.

○ **ECB**(electronic codebook, 전자 코드북) 모드
가장 간단한 구조로, 암호화하려는 메시지를 여러 블록으로 나누어 각각 암호화하는 방식이다.

○ **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.
초기화 벡터가 같은 경우 출력 결과가 같기 때문에, 매 암호화마다 다른 초기화 벡터를 사용해야 한다.

○ **CFB**(cipher feedback, 암호 피드백) 모드
CBC의 변형으로, 이전 단계의 암호문 블록을 암호화한 후 현재의 평문 블록과 XOR 한다.
첫 번째 평문 블록의 경우에는 초기화 벡터(IV)를 암호화한 것과 XOR 한다.

○ **OFB**(output feedback, 출력 피드백) 모드
초기화 벡터(IV)를 매 단계마다 암호화해가며 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

○ **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

문 15. 유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 옳지 않은 것은?

① utmp - 로그인, 로그아웃 등 현재 시스템 사용자의 계정 정보
② loginlog - 성공한 로그인에 대한 내용
③ pacct - 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보
④ btmp - 실패한 로그인 시도

답 ②

② loginlog: 로그인할 때 5번 이상 실패할 경우의 기록

<오답 체크> ① utmp: 현재 로그인하여 접속중인 사용자에 대한 정보
그런데 이 문제는 오류가 있다. utmp는 현재 시스템 사용자의 정보가 기록 중인데, 로그아웃에 대한 기록이 있다는 건 말이 안 된다. 로그아웃을 했으면 현재 사용자에 해당하지 않기 때문이다. 또한 utmp로그는 사용자가 로그인해서 들어오면 정보를 기록하다가, 로그아웃을 할 때 기록해둔 정보를 삭제한다.
다만, ②번이 확실히 틀린 설명이기 때문에 그냥 그렇게 냈나보다하고 넘어가야 한다.

③ pacct: 사용자가 시간대별로 수행한 명령어와 프로그램에 대한 정보를 기록

④ btmp: 로그인 실패 기록에 대한 정보가 포함

문 16. 「개인정보 보호법」상 개인정보처리자가 개인정보가 유출되었음을 알게 되었을 때에 지체 없이 해당 정보주체에게 알려야 할 사항에 해당하지 않는 것은?

① 유출된 개인정보의 항목
② 유출된 시점과 그 경위
③ 조치 결과를 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고한 사실
④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

답 ③

③ 유출 규모가 대통령령으로 정한 규모 이상일 경우 전문기관에 신고하여야 한다는 규정은 있지만, 그 신고 사실을 정보주체에게 알려야 한다는 규정은 없다.
참고로 대통령령으로 정한 규모란 '**1천 명 이상**의 정보주체에 관한 개인정보'이며, 전문기관은 '**한국인터넷진흥원**'으로 규정되어 있다.

「개인정보 보호법」
제34조(개인정보 유출 통지 등)
① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.
1. **유출된 개인정보의 항목**
2. **유출된 시점과 그 경위**
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. **정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처**

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 **통지 및 제2항에 따른 조치 결과를 지체 없이 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다.** 이 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

「개인정보 보호법 시행령」
제39조(개인정보 유출 신고의 범위 및 기관)
① 법 제34조제3항 전단에서 "대통령령으로 정한 규모 이상의 개인정보"란 **1천명 이상**의 정보주체에 관한 개인정보를 말한다.
② 법 제34조제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 **한국인터넷진흥원**을 말한다.

문 17. 인증서를 발행하는 인증기관, 인증서를 보관하고 있는 저장소, 공개키를 등록하거나 등록된 키를 다운받는 사용자로 구성되는 PKI(Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?

① 인증기관이 사용자의 키 쌍을 생성할 경우, 인증기관은 사용자의 개인키를 사용자에게 안전하게 보내는 일을 할 필요가 있다.
② 사용자의 공개키에 대해 인증기관이 전자서명을 해서 인증서를 생성한다.
③ 사용자의 인증서 폐기 요청에 대하여 인증기관은 해당 인증서를 저장소에서 삭제함으로써 인증서의 폐기 처리를 완료한다.
④ 한 인증기관의 공개키를 다른 인증기관이 검증하는 일이 발생할 수 있다.

답 ③

③ 인증서를 삭제하는 것으로 끝이 아니고, 그 삭제 내용을 CRL(Certificate Revocation Rist, 인증서 폐기 목록)에 등록해야 서버가 그 인증서가 유효하지 않다는 것을 확인할 수 있다.

◈ 인증서 취소 사유
▷ 사용자 개인키가 노출되었거나 훼손된 경우
▷ CA가 사용자를 더 이상 인증해줄 수 없는 경우
▷ CA의 인증서가 노출되었거나 훼손된 경우
<오답 체크> ② 인증서에는 인증기관의 서명이 첨부되어 있다. 인증서 이용자는 인증기관의 공개키로 이 서명을 검증하여, 인증서가 위·변조되지 않았다는 것을 확인할 수 있다.

문 18. 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 옳은 것은?

① 생성된 수열의 비트는 정규분포를 따라야 한다.
② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 없어야 한다.
③ 시드(seed)라고 불리는 입력 값은 외부에 알려져도 무방하다.
④ 비결정적(non-deterministic) 알고리즘을 사용하여 재현 불가능한 수열을 생성해야 한다.

답 ②

▷ 의사 난수(psudeo random number)는 진정한 의미에서의 난수는 아니지만 그 결과값을 추측하는 건 매우 어렵기 때문에 어느 정도 난수로 취급할 수 있는 문자열을 말한다.
② 의사 난수는 추론이 불가능해야 한다.
<오답 체크> ① 의사 난수의 특성 중 하나는 무작위성이다. 통계적으로 분포가 편중되지 않아야 한다는 특성인데, 정규분포는 가운데 평균값을 중심으로 모여있는 분포이기 때문에 무작위성에 어긋난다.
③ 의사 난수는 컴퓨터 계산을 통해 생성하며 계산에 사용할 초기값을 시드(seed)라고 한다. 이 시드값이 어떻게 되느냐에 따라 뒤에 난수열이 달라지는데, 시드값이 동일하다면 뒤에 생성되는 난수열도 같아진다. 따라서 시드값은 외부에 알리지 않아야 하며, 시드값 역시 예측하기 어려워야 한다.
보통 시드값으로는 현재의 시간(1/1000초), 마우스의 움직임이나 키보드 입력 시간 간격 등을 사용한다.
④ 의사 난수는 결정론적 알고리즘(deterministic algorithm)을 사용한다. 결정론적 알고리즘이란 주어진 동일한 입력에 대해서 항상 동일한 출력이 생성되는 특성을 가진 알고리즘을 말하는데, 의사 난수는 컴퓨터의 일정한 계산에 의해 생성되기 때문에 계산에 쓰이는 입력값이 같을 경우 출력값 역시 같기 때문에 재현 불가능성을 가질 수 없다.

◈ 난수의 성질
▷ 무작위성: 통계적인 편중이 없이 엉터리 수열로 되어 있는 성질
▷ 예측 불가능성: 과거의 수열로부터 다음 수를 예측할 수 없다는 성질
▷ 재현 불가능성: 같은 수열을 재현할 수 없다는 성질. 재현하기 위해서는 수열 그 자체를 보존해 두는 수밖에 없다.
▶ 무작위성만 만족하는 난수를 '약한 의사 난수'라고 한다.
▶ 무작위성과 예측 불가능성을 만족하는 난수를 '강한 의사 난수'라고 한다.
'암호학적으로 안전한 난수'는 무작위성과 예측 불가능성까지만 만족하면 된다.
▶ 재현 불가능성까지 모두 만족하는 난수를 '진정한 난수'라고 한다. 진정한 난수는 소프트웨어만으로는 생성할 수 없으며, 자연 물리적 현상으로부터 얻은 정보를 기초로 생성하여야 가능하다.

문 19. 사용자 워크스테이션의 클라이언트, 인증서버(AS), 티켓발행서버(TGS), 응용서버로 구성되는 Kerberos에 대한 설명으로 옳은 것은? (단, Kerberos 버전 4를 기준으로 한다)

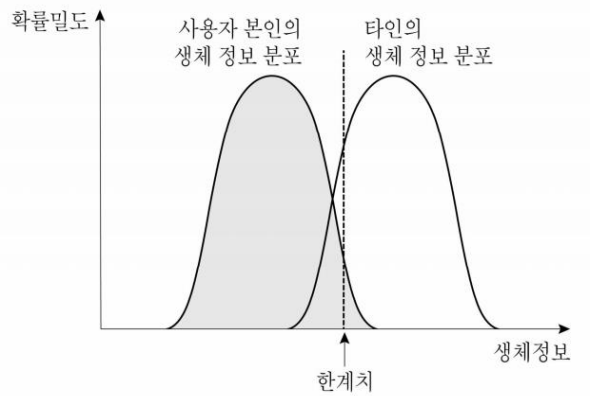
① 클라이언트는 AS에게 사용자의 ID와 패스워드를 평문으로 보내어 인증을 요청한다.
② AS는 클라이언트가 TGS에 접속하는 데 필요한 세션키와 TGS에 제시할 티켓을 암호화하여 반송한다.
③ 클라이언트가 응용서버에 접속하기 전에 TGS를 통해 발급받은 티켓은 재사용될 수 없다.
④ 클라이언트가 응용서버에게 제시할 티켓은 AS와 응용서버의 공유 비밀키로 암호화되어 있다.

답 ②

<오답 체크> ① 커버로스 인증 방식에서는 클라이언트는 패스워드를 인증 서버로 보낼 필요가 없다.
③ 티켓의 유효기간 만료 전이라면 티켓을 재사용할 수 있다.
④ 클라이언트가 응용서버에 제시하는 티켓은 서비스 승인 티켓이며, 이 티켓은 TGS로부터 받은 티켓이다.
이 말은 TGS가 생성하고 응용서버가 검증하는 티켓이라는 의미이며, 따라서 TGS와 응용서버가 공유하는 비밀키로 암호화되어 있을 것이다.

◈ 커버로스 작동 순서
1. 클라이언트는 사용자의 ID와 원하는 TGS ID를 인증서버(AS)에 전송
2. AS는, TGS에 보내기 위한 티켓 승인 티켓을($Ticket_{TGS}$)를 사용자의 패스워드로부터 얻은 키로 암호화한 후 클라이언트로 보낸다.
(티켓에는 재사용 방지를 위해 유효기간(lifetime)이 포함되어 있다. 티켓 승인 티켓은 클라이언트가 볼 수 없도록 인증서버와 TGS의 대칭키로 암호화되어 있다.)
3. 클라이언트는 사용자의 패스워드를 이용해 복호화를 하여 티켓 승인 티켓을 획득한다.
4. 사용자 ID, 요구하는 서비스 ID, 티켓 승인 티켓을 TGS에 전송한다.
5. TGS는 전송받은 메시지를 복호화하여 ID, 유효기간, IP와 네트워크 점검 등을 확인한 후 서비스 승인 티켓($Ticket_V$)를 클라이언트로 전송한다.
6. 클라이언트는 사용자 ID와 서비스 승인 티켓을 서비스 서버(응용서버)로 보낸다.
(서비스 승인 티켓은 클라이언트가 볼 수 없도록 TGS와 서비스 서버의 대칭키로 암호화되어 있다.)
7. 서비스 서버는 ID와 티켓의 내용을 확인한 후 인증을 완료한다.

문 20. 생체 인식 시스템은 저장되어 있는 개인의 물리적 특성을 나타내는 생체 정보 집합과 입력된 생체 정보를 비교하여 일치 정도를 판단한다. 다음 그림은 사용자 본인의 생체 정보 분포와 공격자를 포함한 타인의 생체 정보 분포, 그리고 본인 여부를 판정하기 위한 한계치를 나타낸 것이다. 그림 및 생체 인식 응용에 대한 설명으로 옳은 것만을 고른 것은?



ㄱ. 타인을 본인으로 오인하는 허위 일치의 비율(false match rate, false acceptance rate)이 본인을 인식하지 못하고 거부하는 허위 불일치의 비율(false non-match rate, false rejection rate)보다 크다.
ㄴ. 한계치를 우측으로 이동시키면 보안성은 강화되지만 사용자 편리성은 저하된다.
ㄷ. 보안성이 높은 응용프로그램은 낮은 허위 일치 비율을 요구한다.
ㄹ. 가능한 용의자를 찾는 범죄학 응용프로그램의 경우 낮은 허위 일치 비율이 요구된다.

① ㄱ, ㄷ ② ㄱ, ㄹ
③ ㄴ, ㄷ ④ ㄴ, ㄹ

답 ①

사용자 본인의 그래프에서 한계치를 벗어난 오른쪽 부분은 정당한 권한이 있는 본인을 거부하는 **오거부률(FRR,** 허위 불일치의 비율)이다.
타인의 그래프에서 한계치 왼쪽으로 넘어온 부분은 권한이 없는 타인을 본인으로 인식하는 **오인식률(FAR**, 허위 일치의 비율)이다.

ㄱ. 오인식률(FAR)이 오거부율(FRR)보다 크다.
ㄷ. 보안성이 높은 응용 프로그램은 권한이 없는 사용자가 들어올 확률이 매우 낮아야 한다. 따라서 오인식률이 매우 낮아야 한다.
<오답 체크> ㄴ. 한계치를 오른쪽으로 이동시키면 오거부율은 매우 낮아져 쉽게 인증이 가능해 사용자 편리성이 증대된다. 하지만 그와 동시에 오인식률이 높아져 보안성이 약해진다.
ㄹ. 가능한 용의자를 찾아야 상황에서는 조금이라도 용의자라 의심가는 경우는 모두 조사를 해야 한다. 따라서 범인이 아닌데 범인이라고 의심하는 오인식률(허위 일치 비율)이 높아야 한다.
물론 최종 재판에서 유무죄 판단을 할 때는 명백한 범인이라는 확증이 있어야 하는 것이지만, 용의자를 확보하고 수사를 진행할 때는 조금이라도 가능성이 있는 경우의 수를 모두 확인해야 한다. 예를 들어 목격자 진술이 신장 180cm 가량의 검은 옷을 입은 남성이라고 한다면, 신장 170cm~190cm 사이의 검정색뿐 아니라 남색, 짙은 파란색 등 어두운 계열의 의상 착용자까지 모두 확인해봐야 할 것이다.

▷ **본인의 그래프와 타인의 그래프가 만나는 부분은 FAR와 FRR이 값이 같은데, 이 때의 값을 CER**(Crossover Error Rate)**이라고 한다.**