2021년 국가직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

문 1. 겉으로는 유용한 프로그램으로 보이지만 사용자가 의도하지 않은 악성 루틴이 숨어 있어서 사용자가 실행시키면 동작하는 악성 소프트웨어는?

① 키로거 ② 트로이목마
③ 애드웨어 ④ 랜섬웨어

② **트로이목마**(Trojan Horse)
정상적인 프로그램으로 가장한 악성 프로그램으로, 다른 시스템으로 전파되지는 않는다. 트로이목마는 보통 해커들이 대상 컴퓨터의 인증이나 백신을 우회하여 시스템 내부에 침투하기 위해 사용한다.

<오답 체크> ① **키로거**(key logger)
사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록하는 소프트웨어를 말한다.

③ **애드웨어**(Adware)
광고를 포함한 소프트웨어를 말한다.
사용자에게 광고를 보여줌으로써 프로그래머는 소프트웨어 개발 비용을 충당할 수 있고, 사용자는 무료 또는 저렴한 가격으로 프로그램을 이용할 수 있게 만들어준다. 따라서 모든 애드웨어가 악성코드는 아니다.
하지만 이러한 애드웨어가 무분별하게 사용자의 동의 없이 컴퓨터에 설치되어 광고 화면을 무분별하게 띄워 불편을 초래하는 악성코드가 될 수 있다.

④ **랜섬웨어**(Ransomware)
인질의 몸값을 뜻하는 ransom과 제품을 뜻하는 ware의 합성어로, 컴퓨터에 감염시켜 사용자의 파일을 암호화한 뒤 인질로 잡아 금전을 요구하는 악성 프로그램이다.

답 ②

문 2. 능동적 공격에 해당하는 것만을 모두 고르면?

ㄱ. 도청	ㄴ. 서비스 거부
ㄷ. 트래픽 분석	ㄹ. 메시지 변조

① ㄱ, ㄷ ② ㄴ, ㄷ
③ ㄴ, ㄹ ④ ㄷ, ㄹ

ㄴ. ㄹ. 서비스 거부, 메시지 변조 공격은 능동적 공격
<오답 체크> ㄱ. ㄷ. 도청, 트래픽 분석은 소극적 공격에 해당한다.

✠ **소극적 공격**(수동적 공격)
도청(가로채기, interception)
트래픽 분석(traffic analysis)
메시지 내용 공개(release of message contents) 등

◈ **적극적 공격**(능동적 공격)
차단(interruption)
변조(modification)
위조(fabrication)
신분 위장(masquerade)
서비스 거부 공격(Dos)
재전송 공격(replay attack) 등

답 ③

문 3. 분산 서비스 거부(DDoS) 공격에 대한 설명으로 옳지 않은 것은?

① 하나의 공격 지점에서 대규모 공격 패킷을 발생시켜서 여러 사이트를 동시에 공격하는 방법이다.
② 가용성에 대한 공격이다.
③ 봇넷이 주로 활용된다.
④ 네트워크 대역폭이나 컴퓨터 시스템 자원을 공격 대상으로 한다.

✠ **DDoS 공격**에서 공격자는 악성코드를 통해 다수의 시스템을 감염시켜 좀비PC로 만든 뒤, 그 다수의 좀비PC를 이용해 공격 대상 시스템에 많은 양의 트래픽을 보내 시스템 자원을 고갈시키는 공격을 감행한다. 공격 대상 시스템은 여러 곳으로부터 공격을 받기 때문에, 공격의 근원지를 찾기 매우 어려워진다.

① DDOS는 다수의 공격 지점에서 대규모 공격 패킷을 발생시켜 하나의 사이트를 동시에 공격하는 방법이다.

<오답 체크> ②④ DDoS 공격은 네트워크 트래픽과 시스템 자원을 고갈시켜 서비스를 제공하지 못하게 만드는 공격으로, 이는 시스템의 가용성을 떨어뜨린다.

③ **봇넷**(botnet)
악성코드 등에 감염되어 소유자 모르게 해커의 명령을 받아 사이버 범죄에 동원되는 좀비PC들로 구성된 네트워크

답 ①

문 4. 부인방지 서비스를 제공하기 위한 전자서명에 대한 설명으로 옳지 않은 것은?

① 서명할 문서에 의존하는 비트 패턴이어야 한다.
② 다른 문서에 사용된 서명을 재사용하는 것이 불가능해야 한다.
③ 전송자(서명자)와 수신자(검증자)가 공유한 비밀 정보를 이용하여 서명하여야 한다.
④ 서명한 문서의 내용을 임의로 변조하는 것이 불가능해야 한다.

③ 전송자와 수신자가 공유한 비밀 정보란 비밀키를 의미하는데, 전자서명은 **공개키 방식**을 이용한다.
전자서명 생성/검증 과정에서 송신자는 자신의 개인키로 서명을 하고, 수신자는 송신자의 공개키를 사용하여 서명을 검증한다.

<오답 체크> ① 전자서명은 서명한 문서와 별개의 파일 형태가 아닌, 문서에 결합된 형태라는 의미이다.
② 재사용 불가 특성
④ 위조 불가 특성

♣ **전자서명의 특성**
- **위조 불가**(unforgeable)
- **서명자 인증**(authentic)
- **부인 방지**(non-repudiation)
- **변경 불가**(unalterable)
- **재사용 불가**(not reusable)

답 ③

문 5. 다음은 IT 보안 관리를 위한 국제 표준(ISO/IEC 13335)의 위험분석 방법에 대한 설명이다. ㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은?

> (㉠)은 가능한 빠른 시간 내에 적정 수준의 보호를 제공한 후 시간을 두고 중요 시스템에 대한 보호 수단을 조사하고 조정하는 것을 목표로 한다. 이 방법은 모든 시스템에 대하여 (㉡)에서 제시하는 권고 사항을 구현하는 것으로 시작한다. 중요 시스템을 대상으로 위험에 즉각적으로 대응하기 위하여 비정형 접근법이 적용될 수 있다. 그리고 (㉢)에 의한 단계별 프로세스를 적절하게 수행한다. 결과적으로 시간이 흐름에 따라 비용 대비 효과적인 보안 통제가 선택되도록 할 수 있다.

	㉠	㉡	㉢
①	상세 위험 분석	기준선 접근법	복합 접근법
②	상세 위험 분석	복합 접근법	기준선 접근법
③	복합 접근법	기준선 접근법	상세 위험 분석
④	복합 접근법	상세 위험 분석	기준선 접근법

㉠ **통합 접근법**(복합 접근방법)은 고위험 영역은 상세 위험분석을 수행하고, 그 외 영역은 기준선 접근법을 사용한다.

기본적으로 모든 시스템에 대해 비용이 적게 드는 기준선 접근법을 적용하고, 고위험 영역에서는 비용보다 보안에 집중하여 상세 위험분석을 수행하여 비용과 효율성을 동시에 만족시킬 수 있는 분석법이다.

하지만 고위험 영역에 대한 설정이 잘못 되었을 경우 위험분석 비용이 낭비되고 효과가 떨어지는 단점이 생기게 된다.

㉡ **기준선 접근법**(베이스라인 접근법)은 보호 대책에 대한 항목별로 체크리스트를 작성해 평가하는 방법으로, 국제정보보호관리체계, 정보보호관리체계(ISMS), 개인정보보호관리체계(PIMS) 등과 같은 인증 심사 때 많이 사용한다.

㉢ **상세 위험 분석 접근법**은 자산 식별, 위협 분석, 취약점 분석을 단계별로 수행하여 위험을 분석하는 방법이다.

답 ③

문 6. 다음에서 설명하는 크로스사이트 스크립팅(XSS) 공격의 유형은?

> 공격자는 XSS 코드를 포함한 URL을 사용자에게 보낸다. 사용자가 그 URL을 요청하고 해당 웹 서버가 사용자 요청에 응답한다. 이때 XSS 코드를 포함한 스크립트가 웹 서버로부터 사용자에게 전달되고 사용자 측에서 스크립트가 실행된다.

① 세컨드 오더 XSS
② DOM 기반 XSS
③ 저장 XSS
④ 반사 XSS

④ **반사 XSS 공격**(Reflected XSS)

사용자에게 악성 URL을 배포하여 사용자가 클릭하도록 유도하여 바로 사용자를 공격하는 방법이다. 공격자는 공격용 악성 URL을 생성한 뒤, 이 URL을 이메일 메세지나 거짓 정보 등 다양한 경로로 사용자들에게 배포한다. 사용자는 이 URL 링크를 클릭하는 순간 바로 악성 스크립트가 사용자의 브라우저에서 실행된다.

<오답 체크> ①③ **저장 XSS 공격**(Stroed XSS) = **세컨드 오더 XSS 공격**(Second Order XSS)

웹 서버에 악성 스크립트를 영구적으로 저장해 놓는 공격 방법으로, 웹 사이트의 게시판, 사용자 프로필 및 댓글난 등에 악성 스크립트를 삽입해 놓는다. 사용자가 사이트를 방문하여 저장되어 있는 페이지에 접근하면, 서버에 있던 악성 스크립트를 사용자에게 전달되어 사용자 브라우저에서 실행되어 공격한다.

② **DOM 기반 XSS 공격**(DOM-based XSS)

반사 XSS 공격과 유사하게, 사용자에게 악성 URL을 배포한 후 사용자가 클릭하도록 유도하여 공격하는 방법이다.(DOM 객체의 HTML 문서 이용)

반사 XSS 공격이 악성 스크립트가 담긴 URL 주소가 일단 서버에 전달되어야 하는 반면, DOM 기반 XSS 공격은 서버에 정상적인 HTML 문서가 전달된다.(서버에 악성 스크립트가 저장되지 않음)

이후 사용자가 서버로부터 해당 HTML 문서를 읽을 때, 사용자의 웹 브라우저에서 URL에 담긴 자바스크립트가 실행되고 이를 통해 악성 스크립트를 실행되어 공격한다.

◈ **XSS**(Cross-site Scripting, **크로스 사이트 스크립팅**)**는 웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.**

답 ④

문 7. SHA 알고리즘에서 사용하는 블록 크기와 출력되는 해시의 길이를 바르게 연결한 것은?

알고리즘	블록 크기	해시 길이
① SHA-1	256비트	160비트
② SHA-256	512비트	256비트
③ SHA-384	1024비트	256비트
④ SHA-512	512비트	512비트

· 해시 길이 : SHA 뒤의 숫자가 해시 길이를 의미한다.
(단, 0과 1은 160비트의 길이)
· 블록 크기 : SHA-256까지는 512비트 블록 크기,
SHA-384부터 1024비트의 블록 크기를 가진다.

② SHA-256은 512비트 블록 크기, 256비트 해시 길이
<오답 체크> ① SHA-1은 512비트 블록 크기, 160비트 해시 길이
③ SHA-384는 1024비트 블록 크기, 384비트 해시 길이
④ SHA-512는 1024비트 블록 크기, 512비트 해시 길이

✠ **해시 함수**

알고리즘	해시 길이	블록 크기
SHA-0, SHA-1	160비트	512비트
SHA-224	224비트	512비트
SHA-256	256비트	512비트
SHA-384	384비트	1024비트
SHA-512	512비트	1024비트
MD4, MD5	128비트	512비트
RIPEMD-128	128비트	512비트
RIPEMD-160	160비트	512비트
RIPEMD-256	256비트	512비트
RIPEMD-320	320비트	512비트
HAVAL	128~256 비트의 가변 길이를 출력 1024비트의 블록크기	
HAS160(한국)	160비트	512비트

답 ②

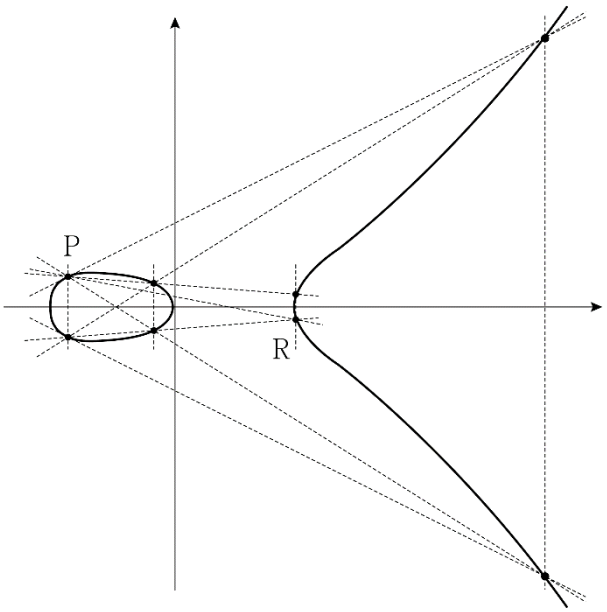
문 8. 데이터베이스 접근 권한 관리를 위한 DCL(Data Control Language)에 속하는 명령으로 그 설명이 옳은 것은?

① GRANT: 사용자가 테이블이나 뷰의 내용을 읽고 선택한다.
② REVOKE: 이미 부여된 데이터베이스 객체의 권한을 취소한다.
③ DROP: 데이터베이스 객체를 삭제한다.
④ DENY: 기존 데이터베이스 객체를 다시 정의한다.

② **REVOKE**: 사용자에게 부여했던 권한을 취소하는 명령어
<오답 체크> ① **GRANT**: 사용자에게 허용 권한을 부여하는 명령어.
③ **DROP**: 테이블이나 뷰, 계정 등을 삭제하는 명령어.
데이터베이스 객체를 삭제하는 명령어는 DELETE 명령어이다.
④ **DENY**: 사용자에게 접근 금지를 설정.
기존 데이터베이스 객체를 다시 정의하는 명령어는 ALTER 명령어이다.

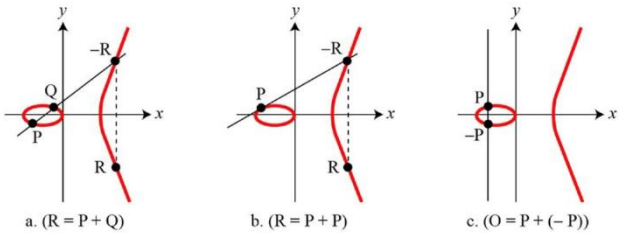
답 ②

문 9. 타원곡선 암호시스템(ECC)은 타원곡선 이산대수의 어려움을 이용한다. 그림과 같이 실수 위에 정의된 타원곡선과 타원곡선상의 두 점 P와 R이 주어진 경우, R = kP를 만족하는 정수 k의값은? (단, 점선은 타원곡선의 접선, 점을 연결하는 직선 또는 수직선을 나타낸다)



① 2 ② 3
③ 4 ④ 5

◖ 타원 곡선의 정의 ◗



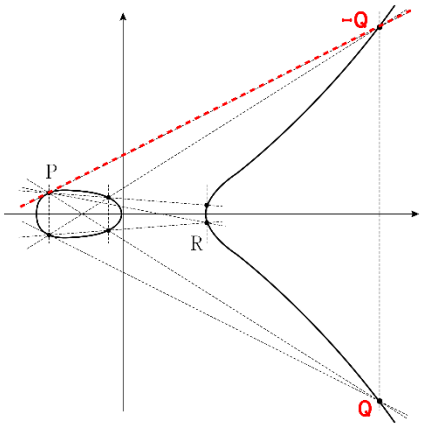
타원곡선은 직선과 만나는 세 점 또는 두 점을 더한 값들의 합은 0이며, 위와 같은 방정식이 성립한다.

예를 들어 a 그래프를 보면, 직선과 만나는 세 점은 P, Q, -R이며, P + Q - R = 0이 성립한다.

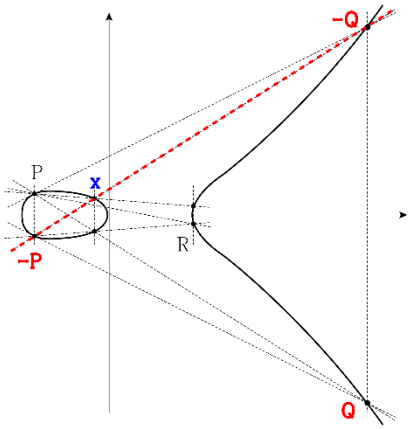
(여기서 R을 이항하여, R = P + Q의 식이 도출)

단, 가운데 b 그래프처럼 P 점에서 접하는 경우, P점과 2번 만나는 것으로 계산하여, P + P - R = 0 식이 성립한다.

(R을 이항하여, R = P + P ⇢ R = 2P)

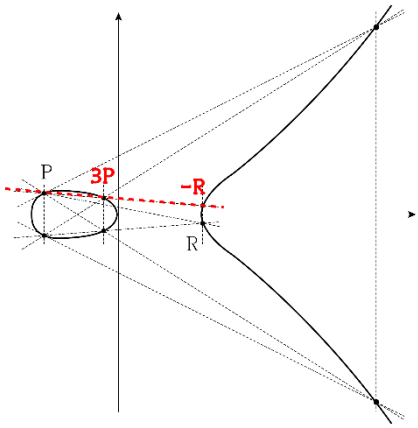


1. 먼저 점 P와 접하는 직선과 만나는 교점을 -Q로 가정한다.
⇒ P + P - Q = 0 ⇒ **2P = Q** …… ㉠



2. 점 P를 x축으로 대칭 이동하는 점 -P를 지정하고,
점 -P에서 점 -Q으로 그은 직선과 만나는 교점을 X로 가정한다.
⇒ - P + X - Q = 0 ⇒ **- P + X = Q** …… ㉡

3. ㉠과 ㉡식을 연립하여 X를 구한다.
⇒ 2P = - P + X ⇒ **3P = X**



4. 마지막으로 P와 3P와 -R을 지나는 직선을 그으면,
⇒ P + 3P - R = 0 ⇒ **4P = R**, 즉 **k = 4**

답 ③

문 10. 「개인정보 보호법」상 가명정보의 처리에 관한 특례에 대한 사항으로 옳지 않은 것은?

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 내부적으로 해당 정보를 처리 보관하되, 제3자에게 제공해서는 아니 된다.

③ 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

④ 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

② **「개인정보 보호법」 제28조의5**(가명정보 처리 시 금지의무 등)
② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 **즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기**하여야 한다.

<오답 체크> ①「개인정보 보호법」 제28조의2 ①항
③「개인정보 보호법」 제28조의4 ②항
④「개인정보 보호법」 제28조의3 ①항

「개인정보 보호법」

제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 **정보주체의 동의 없이** 가명정보를 처리할 수 있다.
② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 **보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관**이 수행한다.
② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.

③ 제1항에 따른 결합 절차와 방법, 전문기관의 지정과 지정 취소 기준·절차, 관리·감독, 제2항에 따른 반출 및 승인 기준·절차 등 필요한 사항은 대통령령으로 정한다.

제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 **가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등** 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

제28조의5(가명정보 처리 시 금지의무 등) ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.
② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 **즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기**하여야 한다.

제28조의6(가명정보 처리에 대한 과징금 부과 등) ① 보호위원회는 개인정보처리자가 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우 **전체 매출액의 100분의 3 이하에 해당하는 금액**을 과징금으로 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 **4억원 또는 자본금의 100분의 3 중 큰 금액 이하**로 과징금을 부과할 수 있다.

답 ②

문 11. 시스템 내 하드웨어의 구동, 서비스의 동작, 에러 등의 다양한 이벤트를 선택·수집하여 로그로 저장하고 이를 다른 시스템에 전송할 수 있도록 해 주는 유닉스의 범용 로깅 메커니즘은?

① utmp ② syslog
③ history ④ pacct

② **syslog** 로그는 사용자 인증과 관련된 로그 및 커널, 데몬들에서 생성된 모든 로그를 기록한다.
시스템 내 수많은 커널 경고, 디버깅 정보, 각종 메시지 출력 등에 대한 로그 정보를 저장한다.

<오답 체크> ① **utmp** 로그는 현재 로그인하여 접속중인 사용자에 대한 정보를 기록한다.(로그아웃을 하면 기록은 삭제된다)

③ **history** 로그는 각 사용자별로 수행한 명령들을 기록한 로그이다.

④ **pacct** 로그는 사용자가 시간대별로 수행한 명령어와 프로그램에 대한 정보를 기록한 로그이다.

답 ②

문 12. 공개키 암호시스템에 대한 설명으로 옳은 것만을 모두 고르면?

> ㄱ. 한 쌍의 공개키와 개인키 중에서 개인키만 비밀로 보관하면 된다.
> ㄴ. 동일한 안전성을 가정할 때 ECC는 RSA보다 더 짧은 길이의 키를 필요로 한다.
> ㄷ. 키의 분배와 관리가 대칭키 암호시스템에 비하여 어렵다.
> ㄹ. 일반적으로 암호화 및 복호화 처리 속도가 대칭키 암호시스템에 비하여 빠르다.

① ㄱ, ㄴ ② ㄱ, ㄹ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

ㄱ. 공개키는 상대방이 사용할 수 있도록 공개해야 하며, 개인키는 암호문을 복호화할 때 쓰이므로 비밀로 보관해야 한다.

ㄴ. **ECC 알고리즘**
타원곡선 상의 이산대수(이산로그) 계산의 어려움을 이용한 공개키 암호 알고리즘. RSA 알고리즘에 비해 키 길이가 매우 짧은 것이 특징이며, 그 덕에 메모리가 처리능력이 제한된 무선통신 환경에서는 ECC가 매우 효과적이다.
RSA 512비트와 비슷한 안전성을 제공하는 ECC 키 길이는 106 비트면 충분하다. 이러한 차이는 키 길이가 길수록 더 두드러지게 나타나며, ECC 512비트는 RSA 15,000비트와 동일한 안전성을 가진다.

<오답 체크> ㄷ. 대칭키 방식은 송수신자가 같은 키를 사용하기 때문에 키를 안전하게 주고 받는 과정이 필요한 반면, 공개키 방식은 암호화용 키(공개키)와 복호화용 키(개인키)가 다르기 때문에 암호화용 키를 마음껏 배포해도 문제가 없다.
또한 대칭키 방식은 각 통신 상대방마다 다른 키를 사용하기 때문에 사용자 수가 늘어날 경우 관리해야 할 키가 기하급수적으로 증가하지만, 공개키 방식은 상대방이 몇 명이든 상관없이 개인별로 공개키-개인키의 한 쌍만 가지고 있으면 된다.

ㄹ. 공개키 방식은 대칭키 방식보다 키의 길이도 길며, 암호화·복호화 속도도 느리다.

답 ①

문 13. 이메일의 보안을 강화하기 위한 기술이 아닌 것은?

① IMAP
② S/MIME
③ PEM
④ PGP

① **IMAP**(Internet Message Access Protocol, 인터넷 메시지 접속 프로토콜)
전자메일 수신 프로토콜, 읽어도 삭제되지 않음, 다운 여부 본인이 결정
IMAP는 단순 메일 수신 프로토콜로, 보안 기능은 탑재되어 있지 않다.

<오답 체크> ② **S/MIME**(Secure/Multipurpose Internet Mail Extension)
MIME를 보호하기 위해 암호화 및 인증을 지원하는 기술로, RSA를 이용하고 인증기관 필요로 한다.

③ **PEM**(Privacy Enhanced Mail)은 IETF에서 만든 전자우편 암호화 시스템으로, 자동 암호화로 전송 중 데이터가 유출되더라도 내용을 볼 수 없어, PGP에 비해 보안성이 뛰어나다.
다만, 중앙 집중식 키 인증 방식을 사용하기 때문에 대중적으로 널리 사용되기 어렵다는 단점이 있다.

④ **PGP**(Pretty Good Privacy)
전자우편 서비스에 대한 보안 기술로, 인증기관을 사용하지 않고 개개인의 신뢰 관계를 이용하여 인증하는 방식이다.

답 ①

문 14. 국제 정보보호 표준(ISO 27001:2013 Annex)은 14개 통제 영역에 대하여 114개 통제 항목을 정의하고 있다. 통제 영역의 하나인 물리적 및 환경적 보안에 속하는 통제 항목에 대한 설명에 해당하지 않는 것은?

① 보안 구역은 인가된 인력만의 접근을 보장하기 위하여 적절한 출입 통제로 보호한다.
② 자연 재해, 악의적인 공격 또는 사고에 대비한 물리적 보호를 설계하고 적용한다.
③ 데이터를 전송하거나 정보 서비스를 지원하는 전력 및 통신 배선을 도청, 간섭, 파손으로부터 보호한다.
④ 정보보호에 영향을 주는 조직, 업무 프로세스, 정보처리 시설, 시스템의 변경을 통제한다.

④ 운영 보안 영역의 **'변경 관리'** 항목에 대한 설명이다.
물리적 및 환경적 보안 영역은 정보처리 시설, 자산, 장비 등에 대한 보안과 관련된 항목들과 관련된 영역이며, 조직, 업무 프로세스, 시스템 변경 등은 운영과 관련된 영역으로 볼 수 있다.

<오답 체크> ① 물리적 및 환경적 보안 영역 '물리적 출입 통제'
② 물리적 및 환경적 보안 영역 '외부 및 환경 위협에 대비한 보호'
③ 물리적 및 환경적 보안 영역 '배선 보안'

답 ④

문 15. 대칭키 암호시스템에 대한 암호 분석 방법과 암호 분석가에게 필수적으로 제공되는 모든 정보를 연결한 것으로 옳지 않은 것은?

① 암호문 단독(ciphertext only) 공격 - 암호 알고리즘, 해독할 암호문
② 기지 평문(known plaintext) 공격 - 암호 알고리즘, 해독할 암호문, 임의의 평문
③ 선택 평문(chosen plaintext) 공격 - 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문
④ 선택 암호문(chosen ciphertext) 공격 - 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 암호문과 해독할 암호문에 사용된 키로 복호화한 해당 평문

② **알려진(기지) 평문 공격**(known-plaintext attack)
공격자가 약간의 평문과 암호문 쌍을 획득한 상태로, 패턴을 찾아내어 다른 암호문을 해독하려는 공격이다.
암호 알고리즘, 해독할 암호문, 임의의 평문과 해당 암호문의 정보를 알고 있는 상태이다.
참고로, **암호 알고리즘은 누구에게나 공개**되어도 키만 잘 보관하면 안전하다.(커크호프의 법칙, Kerckhoffs`s principle)

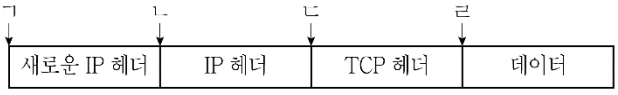
<오답 체크> ① **암호문 단독 공격**(chiphertext-only attack)
공격자가 획득한 것은 암호문 하나뿐이다.
다른 정보 없이 암호문만 가지고 평문을 추정하기 때문에 가장 어려운 방법이다.

③ **선택 평문 공격**(chosen ciphertext attack)
공격자가 **암호기에 접근**하여 원하는 평문을 선택하여 그 평문으로부터 암호문을 획득할 수 있는 상황으로, 자신의 임의대로 평문을 선택할 수 있기 때문에 패턴을 찾기가 더 수월하다.
기지 평문 공격은 무작위의 평문과 암호문 쌍을 획득한 상태인데 반해, 선택 평문 공격은 원하는 평문과 암호문 쌍을 획득한 상태이다.

④ **선택 암호문 공격**(chosen ciphertext attack)
공격자가 **복호기에 접근**하여 임의로 암호문으로부터 평문을 얻을 수 있는 상황으로, 공격자는 원하는 암호문을 선택하고 그로부터 평문을 획득할 수 있다.

답 ②

문 16. IPv4 패킷에 대하여 터널 모드의 IPSec AH(Authentication Header)프로토콜을 적용하여 산출된 인증 헤더가 들어갈 위치로 옳은 것은?



① ㄱ ② ㄴ
③ ㄷ ④ ㄹ

▶ 전송 모드에서는 IP 페이로드와 IP 헤더 일부를 인증·암호화하며, 기존의 IP 헤더를 그대로 유지한다.
▶ 터널 모드에서 기존의 프로토콜들은 그대로 유지되며, 기존 IP 헤더 앞에 AH 헤더가 붙고, 가장 앞에 새로운 IP 헤더가 추가된다. 따라서, AH 프로토콜의 인증 헤더는 새로운 IP 헤더와 (기존)IP 헤더 사이인, 'ㄴ'에 들어간다.

● AH 기본모드

IP Header	TCP Header	Data

● AH 전송모드

IP Header	AH Header	TCP Header	Data

● AH 터널모드

New IP Header	AH Header	IP Header	TCP Header	Data

● ESP 기본모드

IP Header	TCP Header	Data

● ESP 전송모드

IP Header	ESP Header	TCP Header	Data	ESP Trailer	ESP Auth

● ESP 터널모드

New IP Header	ESP Header	IP Header	TCP Header	Data	ESP Trailer	ESP Auth

답 ②

문 17. 정보보호 관련 법률과 소관 행정기관을 잘못 짝 지은 것은?

① 「전자정부법」 - 행정안전부
② 「신용정보의 이용 및 보호에 관한 법률」 - 금융위원회
③ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 - 개인정보보호위원회
④ 「정보통신기반 보호법」 - 과학기술정보통신부

③ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 -> 방송통신위원회와 과학기술정보통신부 소관이다.

답 ③

문 18. 침입탐지시스템의 비정상(anomaly) 탐지 기법에 대한 설명으로 옳지 않은 것은?

① 상대적으로 급격한 변화나 발생 확률이 낮은 행위를 탐지한다.
② 정상 행위를 예측하기 어렵고 오탐률이 높지만 알려지지 않은 공격에도 대응할 수 있다.
③ 수집된 다양한 정보로부터 생성한 프로파일이나 통계적 임계치를 이용한다.
④ 상태전이 분석과 패턴 매칭 방식이 주로 사용된다.

④ 상태전이 분석과 패턴 매칭 방식은 오용(misuse) 탐지 기법에 해당한다.

◈ **오용 탐지**(Misuse Detection)
= 시그니처 기반(Signature Base)
= 지식 기반(Knowledge Base)
이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지
오탐율이 낮고 비교적 효율적이나 알려진 공격 이외는 탐지 불가능
전문가 시스템(Expert System)의 지식 DB를 이용한 IDS
Zero Day attack(제로 데이 공격)에 취약
상태전이 분석과 패턴 매칭 방식

◈ **이상 탐지**(Anomaly Detection IDS) = 비정상 탐지
= 행위 기반(Behavior)
= 통계적 탐지(Statistical Detection)
정상 패턴을 DB에 등록해두고, 정상에서 벗어나는 행위를 탐지(임계치 설정)
알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능
오탐율 높고, 임계치 설정이 어려움

답 ④

문 19. 「전자서명법」상 과학기술정보통신부장관이 정하여 고시하는 전자서명인증업무 운영기준에 포함되어 있는 사항이 아닌 것은?

① 전자서명 관련 기술의 연구·개발·활용 및 표준화
② 전자서명 및 전자문서의 위조·변조 방지대책
③ 전자서명인증서비스의 가입·이용 절차 및 가입자 확인방법
④ 전자서명인증업무의 휴지·폐지 절차

「전자서명법」 제7조(전자서명인증업무 운영기준 등)
① 과학기술정보통신부장관은 전자서명의 신뢰성을 높이고 가입자 및 이용자가 합리적으로 전자서명인증서비스를 선택할 수 있도록 정보를 제공하기 위하여 필요한 조치를 마련하여야 한다.
② 과학기술정보통신부장관은 다음 각 호의 사항이 포함된 전자서명인증업무 운영기준(이하 "운영기준"이라 한다)을 정하여 고시한다. 이 경우 운영기준은 국제적으로 인정되는 기준 등을 고려하여 정하여야 한다.
1. 전자서명 및 전자문서의 위조 · 변조 방지대책
2. 전자서명인증서비스의 가입 · 이용 절차 및 가입자 확인방법
3. 전자서명인증업무의 휴지 · 폐지 절차
4. 전자서명인증업무 관련 시설기준 및 자료의 보호방법
5. 가입자 및 이용자의 권익 보호대책
6. 장애인 · 고령자 등의 전자서명 이용 보장
7. 그 밖에 전자서명인증업무의 운영 · 관리에 관한 사항

① 기술개발 및 표준화는 전자서명인증업무 운영기준이 아니라, 한국인터넷진흥원이 전자서명인증 정책을 지원하기 위해 수행하는 업무 중 하나에 해당한다.

「전자서명법」 제21조(전자서명인증 정책의 지원 등) 한국인터넷진흥원은 전자서명을 안전하고 신뢰성 있게 이용할 수 있는 환경을 조성하고 전자서명인증 정책을 지원하기 위하여 다음 각 호의 업무를 수행한다.
1. 전자서명인증 관련 기술개발 · 보급 및 표준화 연구
2. 전자서명인증 관련 제도 연구 및 상호인정 등 국제협력 지원
3. 제16조제1항에 따른 전자서명인증사업자에 대한 검사 지원
4. 그 밖에 전자서명인증 정책의 지원에 필요한 사항

답 ①

문 20. 안드로이드 보안 체계에 대한 설명으로 옳지 않은 것은?

① 모든 응용 프로그램은 일반 사용자 권한으로 실행된다.
② 기본적으로 안드로이드는 일반 계정으로 동작하는데 이를 루트로 바꾸면 일반 계정의 제한을 벗어나 기기에 대한 완전한 통제권을 가질 수 있다.
③ 응용 프로그램은 샌드박스 프로세스 내부에서 실행되며,기본적으로 시스템과 다른 응용 프로그램으로의 접근이 통제된다.
④ 설치되는 응용 프로그램은 구글의 인증 기관에 의해 서명·배포된다.

④ 기본적으로 안드로이드는 인증서를 사용해 디지털 방식으로 서명한 앱만 기기에 설치하거나 업데이트할 수 있도록 설정되어 있다.
앱 개발자가 구글 플레이 스토어(Google Play)를 통해 앱을 배포하기 위해서는 먼저 자신의 앱 서명 키로 앱에 서명한 다음, 서명 키를 암호화한다.
그 다음 구글 플레이에 앱 서명 키를 업로드하고, 업로드 인증서를 생성하고 등록한다.
그리고 구글 플레이에 앱을 업로드하여 배포한다.

<오답 체크> ② 안드로이드 기기의 최상위 권한(루트 권한)을 획득해 기기의 제한을 해제하는 행위를 루팅(rooting)이라고 한다.
단말기 생산자 또는 판매자들이 깔아놓은 불필요한 앱을 지우거나 권한을 해제하기 위한 목적으로 루팅을 하는 사용자들이 적지 않다.

답 ④