2018년 국회직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
①	②	④	③	⑤	②	④	②	④	①
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
⑤	②	③	①	⑤	②	⑤	⑤	②	④

1. 정보보호의 침해 유형을 소극적 공격과 적극적 공격으로 구분했을 때 적극적 공격에 해당하는 것은?

① 특정 서버에 대한 접속을 마비시킨다.
② 문서들을 분석하여 개인 정보를 추출한다.
③ 패스워드 파일로부터 패스워드를 추측한다.
④ 특정 사용자의 전자우편 메시지를 분석한다.
⑤ 특정 서버와의 트래픽을 선택적으로 감시한다.

답 ①

① 특정 서버에 대한 접속을 마비
-> 서비스 거부 공격(DoS)에 대한 설명

<오답 체크> 나머지 선택지들의 분석, 추측, 감시 등은, 직접적으로 피해를 일으키는 공격 행위가 아닌 소극적 공격 행위이다.

✠ **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

2. 대칭키 암호에 대한 설명으로 옳지 않은 것은?

① DES, AES는 대칭키 암호 알고리즘에 속한다.
② 대칭키 암호는 두 개의 키 값(비밀키, 공개키)이 서로 대칭적으로 존재해야 한다.
③ AES는 SPN(Substitution-Permutation Network) 기반 대칭키 암호이다.
④ AES는 128비트 라운드 키를 사용한다.
⑤ ARIA, SEED는 우리나라 대칭키 암호이다.

답 ②

② 비밀키와 공개키가 존재하는 것은 공개키 암호 방식이다.
대칭키 암호 방식에서는 동일한 비밀키 하나를 송신자와 수신자와 대칭적으로 가지고 있는다.

<오답 체크>

④ AES에서 키 길이는 128, 192, 256비트이지만, 암·복호화 과정에서 쓰이는 라운드 키는 128비트로 동일하다.

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

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

3. 메시지 인증 코드(MAC: Message Authentication Code)가 제공하는 기능들로 짝지어진 것은?

ㄱ. 부인 방지
ㄴ. 상호 인증
ㄷ. 접근 제어
ㄹ. 무결성 보장

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ
⑤ ㄷ, ㄹ

답 ④

ㄴ, ㄹ. 메시지 인증 코드(MAC: Message Authentication Code)는 대칭키를 이용하여 해시값을 생성하는 인증 코드로, 무결성과 출처 인증(송신자에 대한 인증)이 가능하다.

<오답 체크>

ㄱ. MAC는 대칭키를 사용하기 때문에 부인 방지 기능은 제공할 수 없다. 부인 방지 기능을 제공하기 위해서는 공개키 암호화 방식을 사용해야 한다.

ㄷ. 접근 제어 기능은 데이터 암호화를 통해 제공할 수 있다.
MAC는 해시값을 구하는 데 대칭키를 이용할 뿐, 대칭키를 이용하여 직접 데이터를 암호화하지는 않고, 데이터는 평문의 상태로 해시값을 붙여 전송한다. 따라서 접근 제어 기능은 제공하기 위해서는 별도의 암호화 알고리즘을 이용하여 데이터를 암호화하여야 한다.

4. CC(Common Criteria) 인증 제도에 대한 설명으로 옳지 않은 것은?

① CC에서 TOE는 Target of Evaluation의 약자로서 평가 대상을 의미한다.
② CC에서 정보보호시스템은 EAL(Evaluation Assurance Level)로 보안수준을 평가받는다.
③ CC는 미국 NIST FIPS PUB 197 자료를 참고해서 만들어진 제도이다.
④ CC에서 PP는 Protection Profile을 의미하는 것으로 보안 요구 사항을 정의한다.
⑤ CC는 CCRA(Common Criteria Recognition Arrangement)라는 국제상호인정협정을 가지며, CCRA 수준으로 평가를 수행한다.

답 ③

③ 미국 연방 정보 처리 표준 FIPS PUB 197에서는 AES 암호화 알고리즘에 대해 규정하고 있다.
CC는 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준으로, AES 암호화에 대한 표준 규정과는 관련이 없다.

◈ CC의 구성요소
○ 평가보증등급(**EAL**)
국제 공통평가기준(CC)에서 정의한 제품의 보증등급으로, EAL1에서 EAL7까지 7단계
○ 보호프로파일(**PP**, Protection Profile)
사용자나 개발자의 보안 요구사항을 표현하기 위해 CC를 준용하여 작성된 것으로, 보안기능을 포함한 IT 제품이 갖추어야 할 보안요구사항 집합.
제품군에 대한 보안 요구사항을 정의한 것으로, 특정 제품의 기술적인 구현에 독립적이며, 여러 제품이나 시스템이 동일한 PP를 적용할 수 있다.
○ 보안목표명세서(**ST**, Security Target)
개발자가 특정 IT 제품의 보안기능을 표현하기 위해 CC를 준용하여 작성한 것으로, 제품 평가를 위한 기초자료로 사용됨
특정 제품에 대한 보안 명세를 정의한 것이기 때문에 기술적인 구현에 종속적이며, 각 제품이나 시스템은 각각의 ST를 적용한다.
ST는 PP를 포함한다.
○ 평가대상(**TOE**(Target of Evaluation)
평가의 대상인 IT 제품이나 시스템과 이와 관련된 관리자 설명서 및 사용자 설명서

5. OTP(One Time Password)에 대한 설명으로 옳지 않은 것은?

① OTP는 비밀번호 예측 공격을 막기 위한 방법으로 사용 가능하다.
② 패킷 스니핑을 통한 비밀번호 재사용 공격의 대응책으로 활용 가능하다.
③ 동기화 방식 OTP에서는 시간과 인증 횟수를 기반으로 비밀번호를 동기화 한다.
④ 비동기화 방식 OTP는 인증서버에서 전송된 난수를 기반으로 비밀번호를 생성한다.
⑤ 시간 동기화 방식 OTP는 인증서버와 OTP 생성기의 시간오차범위를 허용하지 않는다.

답 ⑤

▷ **OTP**(One-Time Password, **일회용 비밀번호**)
한 번 생성되면 그 인증값이 임시적으로 한 번만 유효한 비밀번호 인증 방식으로, 재사용이 불가능하다.

⑤ OTP 서버와 OTP 생성기는 시간 오차가 발생할 수밖에 없으므로 일정 범위의 시간 오차를 허용해야 한다.

6. ARP Spoofing이 악용하는 매핑(mapping) 정보로 짝지어진 것은?

① IP 주소 - 도메인 주소
② IP 주소 - MAC 주소
③ MAC 주소 - TCP port 번호
④ MAC 주소 - 도메인 주소
⑤ IP 주소 - TCP port 번호

답 ②

▷ **ARP Spoofing**(ARP 스푸핑)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격이다.
공격자는 클라이언트와 서버 사이의 패킷을 읽고 확인한 후 정상적인 목적지로 향하도록 다시 돌려보내 연결이 유지되도록 한다.

② ARP 스푸핑에서 공격자가 악용하는 매핑 정보는 ARP 테이블에 담긴 IP-MAC 매핑 정보이다. 공격자는 특정 IP 주소에 대한 MAC 주소를 공격자 자신의 MAC 주소로 수정한다. 그렇게 되면 송신자가 해당 IP 주소로 데이터를 전송하려 할 때 IP-MAC 변환 과정에서 공격자의 MAC 주소로 변환이 되고, 따라서 해당 데이터는 공격자에게 전송이 된다.

<오답 체크>

① IP 주소와 도메인 주소의 매핑 정보를 조작하여 행하는 공격은 DNS 스푸핑, 파밍 등이 있다.

7. BLP(Bell-La Padula) 모델이 가지고 있는 특성과 규칙에 대한 설명으로 옳지 않은 것은?

① 비밀정보가 허가되지 않은 방식으로 접근되는 것을 방지하고자 하는 것을 목표로 함
② 강제적 접근통제를 하고자 하는 경우 본 모델을 기반으로 통제 규칙을 정의함
③ 단순 보안 규칙은 주체가 객체를 읽기 위해서는 주체의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 함
④ 스타 보안 규칙은 주체가 객체에 쓰기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 함
⑤ 강한 스타 보안 규칙은 주체의 읽기/쓰기는 하위 혹은 상위가 아닌 동일한 보안 분류 수준의 객체에 대해서만 가능함

답 ④

▷ **BLP**(Bell-Lapadula, 벨 라파듈라) 모델
기밀성을 중시한 모델, 높은 수준의 데이터가 낮은 수준으로 이동하여 유출되는 것을 방지하기 위한 모델이다.
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.

④ Star(*) 속성 – NWD(No Write Down)
스타 보안 속성은 쓰기에 관한 보안 속성으로, 자신보다 낮은 수준의 객체에 쓸 수 없다는 것이다. 따라서 주체가 객체에 쓰기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 낮거나 같아야 한다.

<오답 체크>

② BLP 모델은 주체와 객체의 보안 레벨에 기반한 강제적 접근 제어(MAC) 방식에 해당한다.

③ 단순 보안 속성 – NRU(No Read Up)
자신보다 높은 등급의 객체를 읽을 수 없으며, 낮거나 같은 등급의 객체만 읽을 수 있다.

8. 웹 공격의 유형에 대한 설명으로 옳지 않은 것은?

① XSS(Cross-Site Scripting) : 저장 XSS 공격, 반사 XSS 공격, DOM 기반 XSS 공격으로 분류되며, 이에 대응하기 위해서는 웹 어플리케이션의 개발단계에서 XSS에 대비한 입출력값을 검증하고 적절하게 인코딩하는 방법을 선택하는 것이 중요하다.

② SQL injection : 웹에서 사용자가 입력하는 값이 DB 질의어와 연동이 되는 경우에는 클라이언트 측에서만 자바스크립트 등을 통해 사용자의 입력값을 검증하는 것으로 해결된다.

③ CSRF(Cross-Site Request Forgery) : 사용자가 자신의 의도와는 무관하게 공격자가 의도한 웹사이트 사용 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 만드는 공격이다.

④ 쿠키획득 공격 : 로그인된 사용자의 쿠키값을 XSS 등의 공격으로 획득하여 로그인을 할 수 있다.

⑤ 인증우회 공격 : 인증되지 않은 사용자가 접근할 수 없는 페이지를 접근할 수 있는 URL을 획득하여 인증 없이 접근하는 공격방법이다.

답 ②

② 클라이언트 측뿐만 아니라 서버 측에서도 입력값을 검증해야 한다. 공격자 클라이언트 측 프로그램을 수정하거나 우회하여 서버로 SQL 질의어를 보내는 방법은 많이 있기 때문에, 서버 측에서 다시 한번 질의어를 필터링한다.

<오답 체크>

① **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.

▷ **저장 XSS 공격**(Stroed 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.

▷ **반사 XSS 공격**(Reflected XSS)

사용자에게 악성 URL을 배포하여 사용자가 클릭하도록 유도하여 바로 사용자를 공격하는 방법이다.

취약한 서버는 에러 메시지나 검색 결과값 등의 응답 페이지에 클라이언트가 입력한 값들을 그대로 다시 되돌려 보여주는데, 공격자는 악성 스크립트가 담긴 오류 메시지를 서버 측으로 보내 서버 측의 응답 페이지에 악성 스크립트가 담기도록 하여 악성 URL을 생성한다. 이 URL을 이메일이나 거짓 유인 정보 등 다양한 경로로 인터넷 사용자들에게 배포하고, 사용자가 URL 링크를 클릭하면 악성 스크립트가 사용자의 브라우저에서 실행된다.

▷ **DOM 기반 XSS 공격**(DOM based XSS)

DOM(Document Object Model, 문서 객체 모델)이란 W3C 표준으로 HTML 및 XML 문서의 표준 접근방법을 정의한 모델이다. DOM 기반 XSS 공격은 이러한 DOM 환경에서 사용자의 웹 브라우저가 HTML 페이지를 구문 분석할 때마다, 공격 스크립트가 DOM 생성의 일부로 실행되도록 하는 공격이다.

저장 XSS 공격이나 반사 XSS 공격이 서버 측 취약점으로 인해 발생하는 공격법인 반면, DOM 기반 XSS는 서버와 관계없이 브라우저의 취약점으로 인해 발생하는 공격법이다.

9. Diffie-Hellman 알고리즘은 $(G^a \bmod P)^b \bmod P$와 $(G^b \bmod P)^a \bmod P$를 계산한 값이 같다는 대수적인 성질을 활용한다. 다음 설명 중 옳지 않은 것은?

① a와 b는 비밀값이다.
② P는 소수이다.
③ 두 개의 키를 합성하면 새로운 키가 생성된다.
④ 중간자 공격을 방지한다.
⑤ 암호화와 복호화에 필요한 키를 분배하거나 교환하기 위한 것이다.

답 ④

④ 디피-헬만 키 교환방식은 통신 상대방을 인증하지 않기 때문에 중간자 공격에 취약하다.

<오답 체크> ① 송·수신자 사이에 전송되는 값은 p, g, $G^a \bmod P$, $G^b \bmod P$ 값이다. a와 b는 상대방에게 전송하지 않고 본인만 알고 있는 비밀값이다.

✠ 디피 헬만 키 교환 순서

1. 앨리스가 충분히 큰 소수 p와 g를 선택하여 밥에게 전송한다. g는 1부터 p-1 사이의 수(p의 원시근)이다.
2. 앨리스가 정수 a를 선택한다. 이 정수는 외부에 공개되지 않으며, 밥 또한 알 수 없다.
3. 앨리스가 $A = g^a \bmod p$, 즉 g^a를 p로 나눈 나머지를 계산한다.
4. 밥이 마찬가지로 정수 b를 선택하여 $B = g^b \bmod p$ 를 계산한다.
5. 앨리스와 밥이 서로에게 A와 B를 전송한다.
6. 앨리스가 $B^a \bmod p$를, 밥이 $A^b \bmod p$를 계산한다.

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$$
$$A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

이로써 앨리스와 밥은 공통의 비밀키 $g^{ab} \bmod p$ 를 갖게 된다.

10. 「개인정보 보호법」의 개인정보 영향평가에 대한 설명으로 옳지 않은 것은?

① 공공기관의 장은 개인정보 영향평가를 하고 그 결과를 한국인터넷진흥원장에게 제출하여야 한다.
② 개인정보 영향평가는 대통령령으로 정하는 기준에 해당하는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우, 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
③ 개인정보 영향평가를 하는 경우에는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험 정도 등에 대하여 고려하여야 한다.
④ 평가기관의 지정기준 및 지정취소, 평가기준, 평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
⑤ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 개인정보 영향평가를 하기 위하여 적극 노력하여야 한다.

답 ①

① 한국인터넷진흥원장(X) -> 행정안전부장관(○)

「개인정보 보호법」 제33조(개인정보 영향평가)

① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 **행정안전부장관**에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.

② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.

1. 처리하는 **개인정보의 수**
2. 개인정보의 **제3자 제공 여부**
3. 정보주체의 권리를 **해할 가능성 및 그 위험 정도**
4. 그 밖에 대통령령으로 정한 사항

③ 행정안전부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.

④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.

⑤ 행정안전부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.

⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 **대통령령**으로 정한다.

⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.

⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

11. 전자문서에 대한 인증 및 부인 방지에 활용하는 암호화 방식은?

① SEED
② HIGHT
③ AES
④ RC6
⑤ RSA

답 ⑤

⑤ 인증과 부인 방지 기능을 모두 제공하는 것은 공개키 암호화 방식이다. 선택지 중 공개키 암호화에 해당하는 것은 RSA 하나뿐이다.

<오답 체크>

①②③④ SEED, HIGHT, AES, RC6는 대칭키 암호화 방식이다. 대칭키 방식은 메시지를 보내는 상대방, 송신자 인증(출처 인증)은 가능하지만, 부인 방지 기능은 제공할 수 없다.

✠ **대칭키** 암호 알고리즘
DES, 3-DES, IDEA, AES, RC5, RC6, Skipjack, Blowfish
(국산) SEED, HIGHT, ARIA, LEA, LSH

✠ **비대칭키** 암호(공개키 암호) 알고리즘
RSA : 소인수분해
Rabin : 소인수분해
ElGamal : 이산대수
ECC : 타원곡선 상의 이산대수
Schnorr : 이산대수, ElGamal에 기반, 짧은 키 길이
DSA : 이산대수, Schnorr의 응용
DSS : 이산대수, 전자서명 전용
ECDSA : 내부적으로 타원곡선
Knapsack : 부분집합의 합을 구하는 문제
(NP-complete 문제)
KCDSA : 국산, 국내표준
ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

12. 정보통신망의 안전성 확보를 위해 수립하는 기술적, 물리적, 관리적 보호 조치 등 종합적인 정보보호 관리 체계 인증 제도는?

① PIMS(Personal Information Management System)
② ISMS(Information Security Management System)
③ ITSEC(Information Technology Security Evaluation Criteria)
④ CMVP(Cryptographic Module Validation Program)
⑤ KCMVP(Korea Cryptographic Module Validation Program)

답 ②

② **ISMS**(정보보호관리체계인증))
기업이 주요 정보자산을 보호하기 위해 수립 · 관리 · 운영하는 정보보호 관리체계가 인증기준에 적합한지를 심사하여 인증을 부여하는 제도
- ISMS 법적근거
· 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47조
정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제47조~54조
정보보호 관리체계 인증 등에 관한 고시
=> 이를 통해 정보통신망을 운영하는 데 있어 보호 조치 등을 수행하는 정보보호관리체계 인증제도는 ISMS임을 알 수 있다.

<오답 체크>

① **PIMS**(개인정보보호 관리체계인증)는 개인정보를 보호하는 것에 중점을 둔 관리체계 인증제도이다.
기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적 · 지속적으로 보호 업무를 수행하는지에 대해 객관적으로 심사하여 기준 만족 시 인증을 부여하는 제도
- PIMS 법적근거
· 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의 3
· 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제54조의 2
· 개인정보 보호법 제32조의 2
· 개인정보 보호법 시행령 제 34조의 2~제 34조의 8
· 개인정보보호 관리체계 인증 등에 관한 고시
③ **ITSEC**(Information Technology Security Evaluation Criteria) 유럽의 정보보호 시스템 평가 제도
④ **CMVP**(Cryptographic Module Validation Program) 미국과 캐나다에서 공동으로 개발한 암호화 모듈 검증 제도이다.
⑤ **KCMVP**(Korea Cryptographic Module Validation Program, 한국 암호화 모듈 검증 제도)

13. 블록체인(Blockchain) 관련 보안 기술에 대한 설명으로 옳지 않은 것은?

① 블록체인은 해시 함수를 사용하여 데이터에 대한 무결성을 보장한다.
② 블록체인 기술은 데이터의 신뢰성 및 투명성을 제공한다.
③ 공개형 블록체인 기술은 공개키 암호를 사용하기 때문에 권한이 있는 피어(peer)만 참여할 수 있다.
④ 블록체인 기술의 한 예인 하이퍼레저 패브릭(Hyperledger Fabric)에서는 공개키 인증서를 이용하여 피어에 대한 신원(identity) 정보를 제공한다.
⑤ 블록체인 기술에서는 작업 증명이나 지분 증명 등과 같은 합의 알고리즘을 사용한다.

답 ③

③ 블록체인의 형태
- 공개형 블록체인(Public Blockchain): 누구나 노드 참여가 가능한 블록체인 구조
- 폐쇄형 블록체인(Private Blockchain); 검증된 사람만이 참여가 가능한 블록체인 구조
- 컨소시엄 블록체인(Consortium Blockchain): 폐쇄형 블록체인 중 하나로, 여러 기관들이 컨소시엄을 이루어 블록체인 네트워크를 같이 운영하는 구조
- 허가형 블록체인(Permissioned Blockchain): 폐쇄형 블록체인 중 하나로, 각 참여자들은 서로 다른 권한을 가지며 특정 행위를 수행하기 위해서는 권한을 부여받아야 한다.

④ 하이퍼레저 패브릭(Hyperledger Fabric)
· 허가형(permissioned) 또는 폐쇄형 블록체인
· 일반 프로그래밍 언어(general-purpose programming language) 사용
· 내부 가상통화 부재(no internal cryptocurrency)
· 높은 성능(high performance)
· 교체 가능한 모듈 구조(pluggable modular architecture)
· 멀티 블록체인(multi-blockchain) 지원
하이퍼레저 패브릭에서는 PKI 환경의 인증기관을 통해 공개키 인증서와 대응되는 개인키를 자격증명으로 발급한다.

⑤ ▷ 작업증명(PoW, Proof of Work)
블록체인 채굴자(miner)가 가진 시스템의 해시 연산 능력에 비례하여 데이터를 기록할 수 있는 권한을 획득하는 방식
▷ 지분증명(PoS, Proof of Stake)
채굴자가 가진 현재의 자산에 비례하여 데이터 기록 권한을 획득하는 방식

14. 파밍(Pharming) 공격에 활용하기 위해 공격자의 웹서버 IP 주소와 매핑해주는 특정 정보로 옳은 것은?

① 정상 사이트의 도메인 주소
② 정상 사이트 서버의 MAC 주소
③ 정상 사이트가 연결되어 있는 스위치의 port 번호
④ 사용자 컴퓨터의 공인 IP주소
⑤ 정상 사이트 서버의 TCP port 번호

답 ①

① **파밍**(pharming)
사용자가 자신의 웹 브라우저에서 올바른 도메인을 입력해도 가짜 웹 페이지에 접속하게 하여 개인정보를 훔치는 것이다.
공격자는 가짜 웹서버를 생성한 뒤, **정상 사이트의 도메인 주소를 가짜 웹서버의 IP 주소와 매핑해**준다. 그러면 사용자들이 정상적인 도메인 주소를 입력해도 조작된 매핑 정보로 인해 가짜 웹서버로 접속이 되어 개인정보 유출 등의 피해를 입게 된다.

15. 해시 함수에 대한 설명으로 옳지 않은 것은?

① 해시 함수를 사용하면 임의 길이의 메시지에 대해 특정 길이를 갖는 출력값을 얻을 수 있다.
② 해시 함수는 일방향 함수에 해당한다.
③ 동일한 출력값을 갖는 임의의 두 입력 메시지를 찾기 어렵다는 것을 강한 충돌 저항성(strong collision resistance)이라고 한다.
④ 해시 함수는 블록체인에서 체인 형태로 사용되어 데이터의 신뢰성을 보장한다.
⑤ 해시 함수는 대칭키 암호와 달리 키 값을 적용할 수 없기 때문에 MAC(Message Authentication Code)로 사용할 수 없다.

답 ⑤

⑤ 메시지 인증 코드(MAC, Message Authentication Code)는 대칭키를 사용하여 구한 해시값으로, 무결성과 출처 인증(발신지에 대한 인증) 기능을 제공한다.

▶ 일방향성(onewayness)
(= 역상 저항성(preimage resistance))
(= 약 일방향성(weak onewayness)
역산할 수 없어야 한다.
해시값으로부터 원본 메시지를 찾을 수 없어야 한다.
▶ 약한 충돌 내성(weak collision resistance)
(= 제2 역상 저항성(second preimage resistance))
(= 강 일방향성(strong onewayness))
주어진 해시값과 같은 해시값을 갖는 다른 메시지를 찾을 수 없어야 한다.
▶ 강한 충돌 내성(strong collision resistance)
(= 충돌 저항성(collision Resistance))
(= 충돌 회피성(collision freeness))
출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없어야 한다.

16. 공개키 기반 구조(PKI: Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?

① 공개키 인증서는 특정 사용자의 신원과 그 사용자의 공개키를 바인딩시키는 기술이다.
② 공개키 인증서를 생성할 때는 인증기관(CA: Certificate Authority)의 공개키를 사용하여 서명할 수 있다.
③ CA간에는 인증 체인을 형성할 수 있기 때문에 특정 CA에 의해 서명된 인증서는 인증 체인상의 다른 CA에 의해서도 보장될 수 있다.
④ 공개키 인증서 서명에는 RSA나 ECDSA를 사용할 수 있다.
⑤ PKI에서 RA(Registration Authority)는 인증서 발급을 요청한 사용자의 신원을 검증하는 역할을 한다.

답 ②

② 공개키 인증서는 인증기관의 개인키를 사용하여 서명을 하여 생성을 하고, 사용자가 인증기관의 공개키를 사용하여 서명을 검증하여 올바른 공개키 인증서임을 확인한다.

<오답 체크>

④ RSA와 ECDSA는 모두 공개키 암호화 알고리즘으로 전자서명에 이용될 수 있다.

✠ **비대칭키** 암호(공개키 암호) 알고리즘
RSA : 소인수분해
Rabin : 소인수분해
ElGamal : 이산대수
ECC : 타원곡선 상의 이산대수
Schnorr : 이산대수, ElGamal에 기반, 짧은 키 길이
DSA : 이산대수, Schnorr의 응용
DSS : 이산대수, 전자서명 전용
ECDSA : 내부적으로 타원곡선
Knapsack : 부분집합의 합을 구하는 문제
(NP-complete 문제)
KCDSA : 국산, 국내표준
ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

17. 다음 중 <보기>에서 설명하는 것은?

> IETF의 작업 그룹에서 RSADSI(RSA Data Security Incorporation) 의 기술을 기반으로 개발한 전자우편 보안 기술이며, RFC3850, 3851 등에서 정의되어 있다. 전자우편에 대한 암호화 및 전자서명을 통하여 메시지 기밀성, 메시지 무결성, 사용자 인증, 송신 사실 부인 방지, 프라이버시 보호 등의 보안 기능을 제공한다.

① MIME(Multipurpose Internet Mail Extensions)
② SMTP(Simple Mail Transfer Protocol)
③ PGP(Pretty Good Privacy)
④ PEM(Privacy Enhanced Mail)
⑤ S/MIME(Secure/Multipurpose Internet Mail Extensions)

답 ⑤

⑤ **S/MIME**(Secure/Multipurpose Internet Mail Extension)
MIME를 보호하기 위해 암호화 및 인증을 지원하는 기술로, RSA를 이용하고 인증기관 필요로 한다.
PGP 의 낮은 보안성과 기존 시스템과의 통합이 용이하지 않다는 점을 보완하기 위해 IETF 의 작업 그룹에서 RSADSI(RSA Data Security Incorporation)의 기술을 기반으로 개발된 전자우편 보안 시스템이다.

<오답 체크> ① **MIME**(Multipurpose Internet Mail Extension)
기본적으로 7비트 아스키 문자만 지원하는 SMTP의 문제를 해결하고자 SMTP를 확장하여 오디오, 비디오, 응용 프로그램, 기타 여러 종류의 데이터 파일을 주고받을 수 있도록 만든 프로토콜이다.

② **SMTP**(Simple Mail Transfer Protocol, 간이 전자 우편 전송 프로토콜)
클라이언트와 서버, 서버와 서버 사이에서 전자메일 송신을 담당하는 프로토콜

③ **PGP**(Pretty Good Privacy)
전자우편 서비스에 대한 보안 기술로, 인증기관을 사용하지 않고 개개인의 신뢰 관계를 이용하여 인증하는 방식이다.
1991년에 Philip R. Zimmermann에 의해 개발되었으며, 전자우편 보안에 있어 사실상의 표준이 되었다.

④ **PEM**(Privacy Enhanced Mail)
IETF에서 만든 암호화 방식으로, 데이터를 6비트씩 분할하여 아스키 문자로 변환하는 Base64 변환 방식을 사용한다.
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.

18. 무선 네트워크 보안 기술에 대한 설명으로 옳지 않은 것은?

① WEP는 보안 취약성이 있다고 알려져 있다.
② WPA2 기술은 AES-CCMP를 사용한다.
③ 무선네트워크 환경에서 인증/인가를 위해 RADIUS 프로토콜을 사용하여 연결한다.
④ Diameter 프로토콜은 RADIUS보다 세션관리, 보안 측면에서 개선 및 확장된 프로토콜이다.
⑤ WPA-PSK 방식은 공개키 인증서 공유 방식으로 확장성이 좋다.

답 ⑤

⑤ WPA-PSK 방식은 WPA 개인모드에서 사용하는 인증 방식으로, 별도의 인증 서버 없이 사전에 미리 공유한 키를 통해 인증하는 방식이며, 확장성이 없다.

<오답 체크>
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 인증서버로 전송하여 인증 서버가 단말 인증을 한다.

④ Diameter 프로토콜은 RADIUS보다 세션관리, 신뢰성, 보안 측면에서 업그레이드 된 프로토콜이다. RADIUS가 UDP를 사용하는 반면, Diameter 프로토콜은 TCP와 SCTP를 사용한다.

○ **WEP 방식**
암호화를 위해 RC4 사용하며(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

19. 전송 계층 보안(TLS: Transport Layer Security) 프로토콜에 대한 설명으로 옳지 않은 것은?

① TLS는 TCP 프로토콜상에서 사용되며, DTLS는 UDP 프로토콜상에서 사용된다.
② TLS 프로토콜에서는 레코드 프로토콜 단계에서 공개키 인증서를 사용한다.
③ TLS는 SSL을 기초로 개발되었다.
④ FTPS에서는 FTP 파일 전송 프로토콜에서 안전한 전송을 위해 TLS를 사용한다.
⑤ TLS 프로토콜에서 대칭키 암호인 ARIA를 사용할 수 있다.

답 ②

② TLS에서 공개키 인증서를 사용하는 단계는 상호 인증을 하는 핸드셰이크 프로토콜 단계이다.
레코드 프로토콜 단계에서는 실제 데이터를 단편화 및 압축, 암호화를 하고 MAC을 적용하여 전송하는 단계이다.

<오답 체크>

① DTLS(Datagram TLS)는 UDP에 TLS를 적용하기 위한 경량 프로토콜이다. UDT 기반 애플리케이션들, 특히 사물인터넷(IoT)에 보안성을 추가해줄 수 있는 프로토콜로 주목받고 있다.
③ SSL 3.0을 기초로 TLS 1.0이 탄생하였다.
④ FTP에 SSL/TLS 추가 --> FTPS
FTP에 SSH 추가 --> SFTP
SSH 기반의 새로운 파일 전송 프로토콜 --> Secure FTP
⑤ SSL/TLS는 기본적으로 기밀성을 위해서 대칭키를, 인증을 위해서 공개키를, 무결성을 위해서 MAC(메시지 인증 코드)를 사용한다. 따라서 ARIA 또한 사용할 수 있다.

20. 「개인정보 보호법 시행령」에서 정한 고유식별정보의 범위에 포함되지 않는 것은?

① 주민등록법 제7조의2 제1항에 따른 주민등록번호
② 여권법 제7조 제1항 제1호에 따른 여권번호
③ 도로교통법 제80조에 따른 운전면허의 면허번호
④ 국가연구개발사업의 관리 등에 관한 규정 제25조 제11항에 따른 과학기술인 등록번호
⑤ 출입국관리법 제31조 제4항에 따른 외국인등록번호

답 ④

④ 과학기술인 등록번호는 규정되어 있지 않다. 고유식별정보는 일반적으로 시험장에서 신분증으로 사용할 수 있는 신분증인 주민등록증, 여권, 운전면허증, 그리고 외국인을 위한 외국인등록번호를 생각하면 된다.

「개인정보 보호법 시행령」 제19조(고유식별정보의 범위)
법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.
1. 「주민등록법」 제7조의2제1항에 따른 **주민등록번호**
2. 「여권법」 제7조제1항제1호에 따른 **여권번호**
3. 「도로교통법」 제80조에 따른 운전면허의 **면허번호**
4. 「출입국관리법」 제31조제4항에 따른 **외국인등록번호**