2018-국회직-정보보호론-가형-해설

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

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.
정답 체크 :
(1) 가용성(DoS) 공격에 해당하므로 적극적 공격이다.
오답 체크 :
(2) 추출은 무결성(변조/위조)과 가용성(DoS)에 대한 공격이 아니므로 소극적 공격이다.
(3) 추측은 무결성(변조/위조)과 가용성(DoS)에 대한 공격이 아니므로 소극적 공격이다.
(4) 분석(analysis)은 기밀성 공격에 해당하므로 소극적 공격이다.
(5) 감시(sniffing, snooping)는 기밀성 공격에 해당하므로 소극적 공격이다.

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.
정답 체크 :
(2) 대칭키는 비밀키가 서로 대칭적으로 존재하고, 비대칭키(공개키)는 개인키, 공개키가 비대칭적으로 존재한다.
오답 체크 :
(1) DES, 3-DES, AES, IDEA, Blowfish 등은 대칭키 암호에 속한다.
(3) AES는 SPN 구조를 가진다. (DES는 Feistel 구조를 가진다.)
(4) AES는 128/192/256비트 라운트 키를 사용한다.
(5) ARIA, SEED는 우리나라 대칭키 암호이다.

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

정답 체크 :
(4)
(ㄴ) : MAC과 디지털 서명(전자 서명)에서 제공한다.
(ㄹ) : MAC, 해시, 디지털 서명에서 제공한다.

오답 체크 :
(1), (2), (3), (5)
(ㄱ) : 디지털 서명에서 제공한다.
(ㄷ) : 접근 제어는 암호화(MAC, 해시, 디지털 서명 등)를 통해 수행할 수 없다. 접근 제어는 MAC, DAC, RBAC 등을 통해서 수행한다.
Tip! : 보안 위협과 암호 기술에 의한 방지를 그림으로 나타내면 다음과 같다.

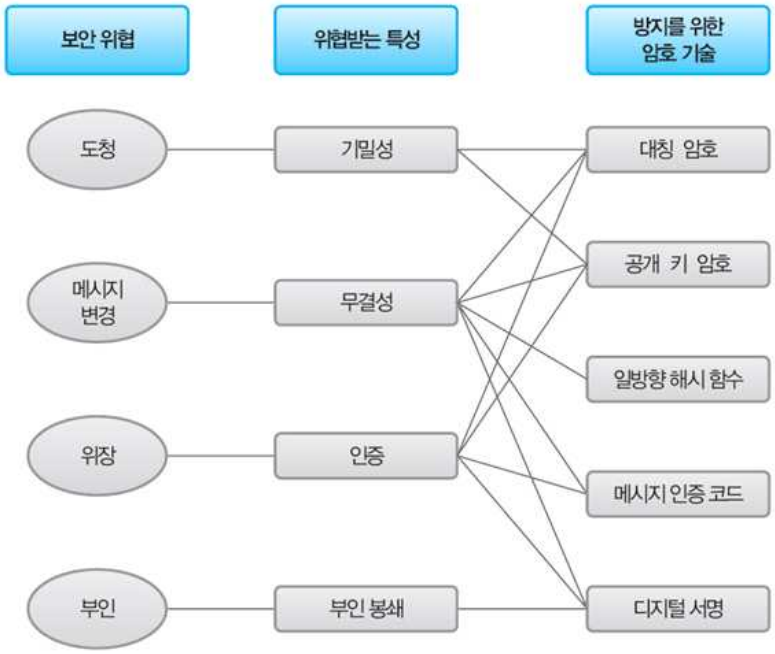


그림 2-10 • 보안 위협과 암호 기술에 의한 방지

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.

정답 체크 :
(3) NIST FIPS PUB 197 : AES를 나타내고, CC는 ISO/IEC 15408이다.
오답 체크 :
(1) TOE : 획득하고자 하는 보안 수준 또는 평가 대상을 의미한다.
(2) EAL : 7개의 보증 등급을 가진다. 보증 등급은 기능 시험(EAL-1), 구조 시험(EAL-2), 방법론적 시험과 점검(EAL-3), 방법론적 설계, 시험, 검토(EAL-4), 준정형적 설계 및 시험(EAL-5), 준정형적 검증된 설계 및 시험(EAL-6), 정형적 검증(EAL-7)로 나눠진다.
(4) PP : 사용자 또는 개발자의 요구사항을 정의한다. 기술적인 구현 가능성을 고려하지 않는다.
(5) CCRA : 회원국의 공통평가기준(CC: Common Criteria) 인증서를 획득한 정보 보호 제품은 타회원국에서도 인정하는 CC 기반의 국제 상호 인정 협정이다.

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.
정답 체크 :
(5) 시간 동기화 방식은 인증 서버와 OTP 생성기의 시간오차범위(1~2분 정도)를 허용한다.
오답 체크 :
(1) OTP는 비밀번호 예측 공격을 막기 위한 1회용 패스워드를 의미한다.
(2) 1회용 패스워드이므로 스니핑을 통한 비밀번호 재사용 공격을 막을 수 있다.
(3) 동기화 방식은 시간(시간 동기화)과 인증 횟수(이벤트 동기화)를 기반으로 비밀번호를 동기화한다.
(4) 비동기화 방식은 클라이언트에서 보낸 난수(S/KEY) 또는 인증 서버에서 전송된 난수(challenge-response)를 기반으로 비밀번호를 생성한다.

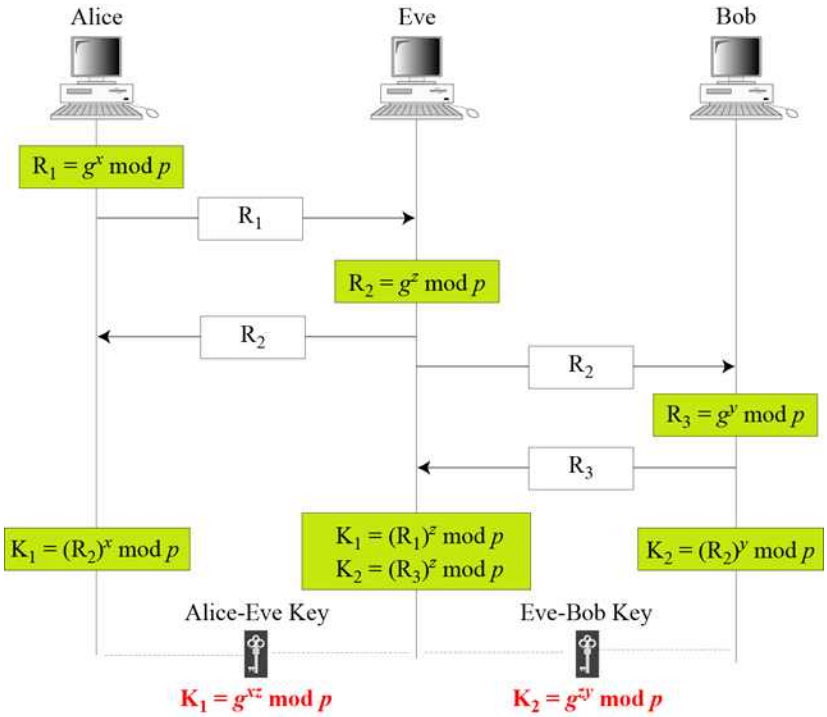
6. ARP Spoofing이 악용하는 매핑(mapping) 정보로 짝지어진 것은?
① IP 주소 - 도메인 주소
② IP 주소 - MAC 주소
③ MAC 주소 - TCP port 번호
④ MAC 주소 - 도메인 주소
⑤ IP 주소 - TCP port 번호
정답 체크 :
(2)
ARP Spoofing은 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다. 그러므로 악용되는 매핑 정보는 IP 주소와 MAC 주소이다.

7. BLP(Bell-La Padula) 모델이 가지고 있는 특성과 규칙에 대한 설명으로 옳지 않은 것은?
① 비밀정보가 허가되지 않은 방식으로 접근되는 것을 방지하고자하는 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 취 급 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
정답 체크 :
(4) 스타 보안 규칙(star property) : No Write Down으로 주체가 객체에 쓰기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 낮거나 같아야 한다.
오답 체크 :
(1) BLP를 기밀성을 목적으로 한다.
(2) MAC은 BLP를 기반으로 한다.
(3) 단순 보안 규칙(simple security property) : No Read Up으로 주체가 객체를 읽기 위해서는 주체의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 한다.
(5) 강한 스타 보안 규칙(strong start property) : 주체는 자신과 등급이 다른 객체에 대해 읽거나 쓸 수 없다.

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 연 동이 되는 경우에는 클라이언트 측에서만 자바스크립트 등을 통 해 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 공격방 법이다.
정답 체크 :
(2) SQL Injection : 클라이언트에서 입력값 검증을 한다고 하더라도 얼마든지 우회가 가능하므로 서버쪽에서도 입력값 검증을 해야 한다.
오답 체크 :
(1) XSS : 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.
(3) CSRF : 유명 경매 사이트인 옥션에서 발생한 개인정보 유출 사건에서 사용된 공격 방식 중 하나다.
(4) 쿠키획득 : XSS 스크립트가 포함된 이메일을 읽으면 클라이언트의 쿠키가 공격자에게 전

송된다.
(5) 인증우회 : 해당 공격의 예는 관리자가 숨겨놓은 관리자 페이지를 들 수 있다.

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.
정답 체크 :
(4) 아래 그림과 같은 중간자 공격이 가능하다.



오답 체크 :
(1) a와 b는 난수로써 비밀값이다.
(2) P는 소수이고, G는 원시근이다.
(3) 두 개의 키를 합성하면 새로운 키(공유되는 비밀키)가 생성된다.
(5) 키를 분배하거나 교환하기 위한 것으로 공개키의 시초가 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 개인 정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우, 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말 한다.

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 개인정보 처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 개인정보 영향 평가를 하기위하여 적극 노력하여야 한다.
정답 체크 :
(1) “개인정보 보호법” 제33조(개인정보 영향평가) 상 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 행정안전부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.
오답 체크 :
(2) “개인정보 보호법” 제33조(개인정보 영향평가) 상 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 행정안전부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.
(3) “개인정보 보호법” 제33조(개인정보 영향평가) 상 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
(4) “개인정보 보호법” 제33조(개인정보 영향평가) 상 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법ㆍ절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
(5) “개인정보 보호법” 제33조(개인정보 영향평가) 상 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
정답 체크 :
(5) RSA : 공개키로 암호화 또는 전자서명을 제공한다. 전자서명은 전자문서에 대한 인증 및 부인 방지에 활용할 수 있다.
오답 체크 :
(1) SEED : 대칭키로 암호화를 수행한다.
(2) HIGHT : 대칭키로 암호화를 수행한다.
(3) AES : 대칭키로 암호화를 수행한다.
(4) RC6 : 대칭키로 암호화를 수행한다.

12. 정보통신망의 안전성 확보를 위해 수립하는 기술적, 물리적, 관리적 보호조치 등 종합적인 정보보호 관리체계 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)
정답 체크 :
(2) ISMS : 정보통신망의 안전성 및 정보의 신뢰성을 확보하고, 조직의 정보보호 수준 제고를 위하여 관리적·기술적·물리적 보호조치를 종합한 것으로, 조직의 관리체계를 효과적으로 수립하도록 2001년 모델을 개발하여 국내 표준으로 제정되었으며 관리체계의 기본 틀이자 공통 프레임워크로 활용되고 있다.
오답 체크 :
(1) PIMS : 국민들에게는 개인정보를 안전하게 관리하는 조직에게 객관적으로 식별할 수 있는 기준을 제시하여 조직 스스로 개인정보 유·노출 및 개인정보의 수집·보관·이용 등 취급 절차상에서 발생할 수 있는 침해 요인을 파악하고 이를 미연에 방지하도록 하는 체계적이고 종합적인 관리체계이다.
(3) ITSEC : 1991년 5월 유럽 국가들이 발표한 공동 보안 지침서이다. TCSEC이 기밀성만을 강조한 것과 달리 무결성과 가용성을 포괄하는 표준안을 제시하였다.
(4) CMVP : 미국(NIST)와 캐나다(CSE)에 의해 만들어진 암호 모듈(암호화 알고리즘, 키의 길이 등) 검증 프로그램이다.
(5) KCMVP : 국산 알고리즘을 탑재한 암호모듈에 대한 구현의 적합성, 안전성 등을 검증하는 제도이다. 여기서 암호모듈이란 암호(대칭/비대칭), 난수 생성, 소수 판정, 해시, 전자서명, 인증 등 암호기능을 소프트웨어, 하드웨어, 펌웨어 또는 이를 조합하는 형태를 의미한다.

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.
정답 체크 :
(3) 비공개형 블록체인은 권한이 있는 피어만 참여할 수 있지만, 공개형 블록체인은 권한이 없는 피어도 참여할 수 있다.
오답 체크 :
(1) 예를 들어 블록체인을 활용하는 비트코인에서는 해시 함수로 SHA-256과 RIPEMD-160을 사용한다.
(2) 신뢰성(누구도 정보를 임의로 변경할 수 없음)과 투명성(모든 사람에게 공개되어 있음)을

제공한다.
(4) 하이퍼레저 패브릭은 리눅스 재단에서 주관하는 블록체인 오픈소스 프로젝트이다. 비공개형 블록체인 플랫폼으로서 기업 비즈니스를 구현하기에 적합한 환경이고, 특정 비즈니스 모델에 특화된 타 플랫폼과 달리 여러 산업에 범용적으로 도입 가능한 기술 표준을 제시한다. ECA(Enrollment Certification Authority)가 공개키 인증서를 발행하여 피어에 대한 신원 정보를 제공한다.
(5) 작업 증명(proof-of-work)와 지분 증명(proof-of-stake) 등과 같은 합의 알고리즘을 사용한다. 이것은 누구나 쉽게 이중지불되는 돈의 문제를 회피할 수 있게 한다.

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
정답 체크 :
(1)
파밍은 Phishing(개인 정보)과 farming(대규모 피해)의 합성어이다. DNS Spoofing과 같이 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시키는 공격 기법이다. 해당 공격 기법을 이용하여 공격자의 웹서버 IP 주소와 정상 사이트의 도메인 주소를 매핑해 준다.

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.
정답 체크 :
(5) 해시 함수는 키 값을 적용할 수 있기 때문에 MAC으로 사용될 수 있다. 이를 HMAC이라고 한다.
오답 체크 :
(1) 입력이 1bit 혹은 1Tbit라도 고정된 길이의 출력을 가진다.
(2) 일방향성을 가진다. 즉, 해시값으로부터 메시지를 얻어낼 수 없다.
(3) 강한 충돌 저항성 : 해시 값이 일치할 것 같은, 다른 2개의 메시지를 발견해 내는 것이 매우 곤란한 성질을 의미한다.
(4) 예를 들어 블록체인을 활용하는 비트코인에서는 해시 함수로 SHA-256과 RIPEMD-160을

사용한다.

16. 공개키 기반 구조(PKI: Public Key Infrastructure) 에 대한 설명으로 옳지 않은 것은?
① 공개키 인증서는 특정 사용자의 신원과 그 사용자의 공개키를 바인딩 시키는 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.
정답 체크 :
(2) 공개키 인증서를 생성할 때는 인증기관의 개인키를 사용하여 서명할 수 있다. 인증기관의 공개키는 서명을 검증할 때 사용한다.
오답 체크 :
(1) 공개키 인증서(공인 인증서)는 "특정 사용자의 공개키가 신뢰할만하다"라는 것을 알려준다.
(3) CA가 계층적 구조 또는 체인 구조를 가질 수 있다. 특정 CA에 의해 서명된 인증서는 상위 계층 혹은 체인 상의 다른 CA에 의해서 보장된다.
(4) 공개키 인증서 서명에는 RSA, ECDSA, DSA를 사용할 수 있다.
(5) RA는 인증기관의 일 중 「공개 키의 등록과 본인에 대한 인증」을 대행하는 기관이다.

17. 다음 중 <보기>에서 설명하는 것은?

<보 기> IETF의 작업 그룹에서 RSADSI(RSA Data Security Incorporation) 의 기술을 기반으로 개발한 전자우편 보안 기술이며, RFC 3850, 3851 등에서 정의되어 있다. 전자우편에 대한 암호화 및 전자서명을 통하여 메시지 기밀성, 메시지 무결성, 사용자 인 증, 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)
정답 체크 :
(5) S/MIME : RFC 3369, 3370, 3850, 3851에 정의되어 있다.
오답 체크 :
(1) MIME : RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289, RFC 2049에 정의된다.
(2) SMTP : RFC 821, RFC 5321에 정의되어 있다.
(3) PGP : RFC 4880에 정의되어 있다.
(4) PEM : RFC 7468에 정의되어 있다.

Tip! : 구체적인 숫자를 외우지 말고 앞자리를 외운다. 예를 들면, S/MIME은 3이고, PGP는 4이고, PEM은 7이다. 그리고 모든 이론에서 숫자와 관련된 것은 주의를 기울여야 한다. 숫자 문제의 경우 이의 제기의 소지가 없기 때문에 출제자의 입장에서 보면 문제 내기가 아주 좋다.

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.
정답 체크 :
(5) WPA-PSK는 미리 키를 공유하는 방식이다. 즉, 공개키 인증서를 사용하지 않는다.
오답 체크 :
(1) WEP의 경우 비밀키의 비트 길이가 작고(64비트) 고정 암호키를 사용하기 때문에 보안에 취약하다.
(2) WPA2는 CCMP(암호키 동적 변경)과 AES 등 강력한 블록 암호 알고리즘을 사용한다.
(3) 기업 환경에서 RADIUS 프로토콜(별도의 인증 서버)을 사용한다.
(4) Diameter 프로토콜은 앞서 사용된 RADIUS 프로토콜에서 훨씬 더 유용하게 진화되었고 RADIUS 프로토콜을 대체하고 있다. Diameter는 새로운 명령어나 EAP와 함께 사용하기 위한 속성 등을 추가하여 확장할 수 있다.

19. 전송 계층 보안(TLS: Transport Layer Security) 프로토콜에 대한 설명으로 옳지 않은 것은?
① TLS는 TCP 프로토콜상에서 사용되며, DTLS는 UDP 프로토콜 상에서 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.
정답 체크 :
(2) 인증서는 핸드쉐이크 프로토콜 단계에서 사용한다.
오답 체크 :
(1) TLS는 TCP에 기반하며, DTLS는 UDP에 기반한다.
(3) TLS는 SSL 3.0을 기초로 해서 만들어졌다.
(4) FTPS는 SSL/TLS에 기반하며, SFTP는 SSH에 기반한다.
(5) TLS에서 대칭키 암호인 ARIA, AES, SEED, 3DES, IDEA, DES, RC2 등을 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
정답 체크 :
(4) 고유식별정보는 모든 사람들 식별할 수 있어야 하는데 과학기술인 등록번호는 특정 집단에 대한 번호이므로 고유식별정보가 될 수 없다.
오답 체크 :
(1), (2), (3), (5)
“개인정보 보호법 시행령” 제19조(고유식별정보의 범위) 상 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