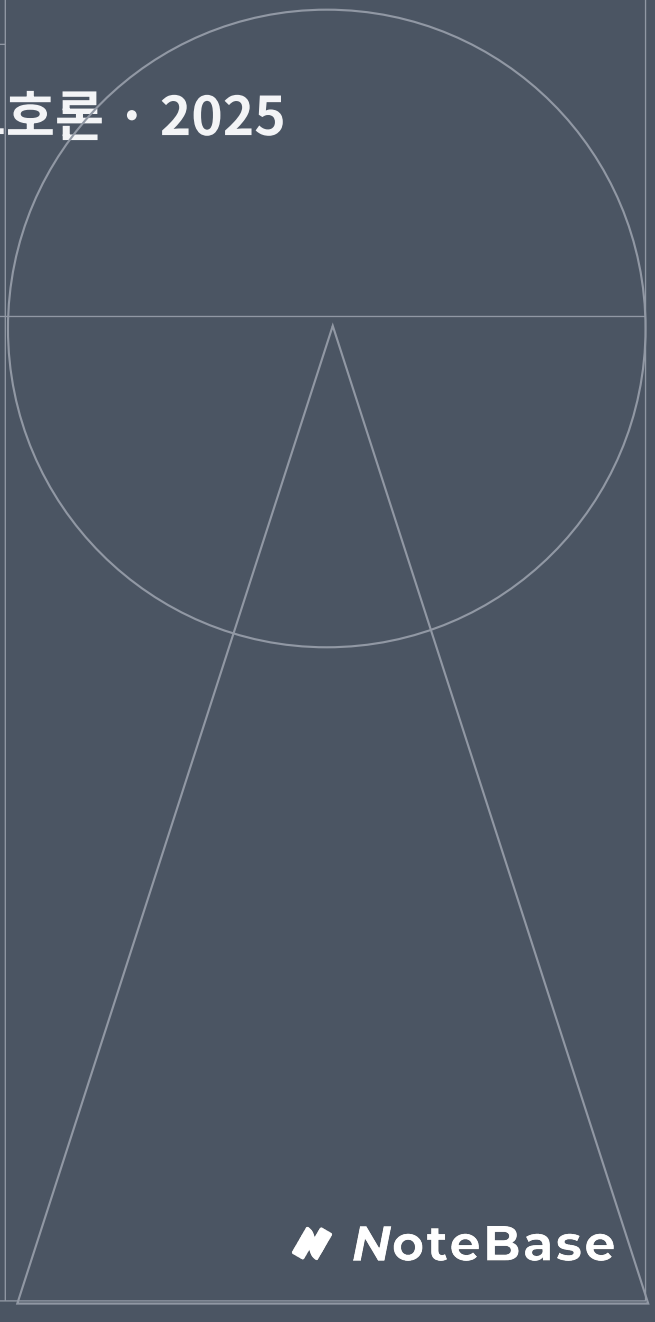
기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2025



NoteBase

기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2025

공무원/국회직/9급 · 정보보호론 · 2025

1. 보안 공격의 특성이 나머지 넷과 거리가 가장 먼 것은?

① Sniffing
② Snooping
③ Masquerade
④ Eavesdropping
⑤ Traffic Analysis

정답 3번

출제 포인트

보안 공격을 수동 공격과 능동 공격으로 구분하고, 성격이 다른 하나를 찾는 문제이다.

핵심 개념

수동 공격은 통신 내용을 몰래 관찰하거나 통신량·패턴을 분석하여 정보를 얻는 공격으로, 정보의 흐름 자체를 바꾸지 않는다. Sniffing, Snooping, Eavesdropping, Traffic Analysis가 이에 해당한다.
능동 공격은 신분을 사칭하거나 메시지를 변조·재전송하는 등 통신이나 시스템 상태에 직접 영향을 주는 공격이다. Masquerade는 정당한 사용자인 것처럼 가장하는 능동 공격이다.

선지별 해설

① X — Sniffing은 네트워크를 흐르는 패킷을 몰래 수집·관찰하는 수동 공격이다. 틀린 판단은 Sniffing이 나머지 넷과 가장 거리가 멀다는 것이며, 올바르게는 Masquerade가 성격이 다른 공격이다.
② X — Snooping은 타인의 데이터나 통신을 몰래 엿보아 정보를 얻는 수동 공격이다. 틀린 판단은 Snooping이 나머지 넷과 가장 거리가 멀다는 것이며, 올바르게는 Masquerade가 성격이 다른 공격이다.
③ O — Masquerade는 공격자가 정당한 사용자나 시스템인 것처럼 신분을 가장하는 능동 공격이다. 나머지 네 공격은 정보를 몰래 관찰·분석하는 수동 공격이므로 Masquerade가 가장 성격이 다르다.
④ X — Eavesdropping은 통신 내용을 몰래 도청하는 수동 공격이다. 틀린 판단은 Eavesdropping이 나머지 넷과 가장 거리가 멀다는 것이며, 올바르게는 Masquerade가 성격이 다른 공격이다.
⑤ X — Traffic Analysis는 통신 내용을 직접 해독하지 못하더라도 송수신 주체, 빈도, 시간, 데이터량 등의 통신 패턴을 분석하는 수동 공격이다. 틀린 판단은 Traffic Analysis가 나머지 넷과 가장 거리가 멀다는 것이며, 올바르게는 Masquerade가 성격이 다른 공격이다.

NoteBase

오답 포인트

Sniffing, Snooping, Eavesdropping은 표현이 서로 달라 별개의 성격처럼 보이고, Traffic Analysis는 통신 내용을 직접 훔치지 않을 수 있어 능동 공격처럼 착각하기 쉽다. 그러나 네 공격은 모두 정보를 관찰·수집할 뿐 통신에 직접 개입하지 않는 수동 공격이다.

다시 나오면 이렇게 판단

공격이 관찰·도청·패턴 분석에 그치면 수동 공격으로, 사칭·변조·재전송처럼 통신이나 시스템 상태에 직접 개입하면 능동 공격으로 판단한다.

암기 포인트

Sniffing·Snooping·Eavesdropping·Traffic Analysis는 수동, Masquerade는 사칭하는 능동 공격이다.

NoteBase

2. SQL 인젝션 공격이 발생할 가능성이 가장 높은 코드 구조는?

① 사용자 입력을 서버에서 세션으로 저장

② 사용자 입력을 파일로 저장한 후 비동기 처리

③ 사용자 입력을 인코딩 후 정적 HTML로 출력

④ 쿼리문 실행 전 입력값을 모두 소문자로 변환

⑤ 사용자 입력값을 문자열로 직접 연결해 SQL 쿼리를 구성

정답 5번

출제 포인트

SQL 인젝션은 사용자 입력이 SQL문의 데이터가 아니라 쿼리 구문의 일부로 해석될 때 발생하며, 입력값을 문자열로 직접 이어 붙이는 구조가 가장 위험하다는 점을 묻는 문제이다.

핵심 개념

SQL 인젝션: 공격자가 입력한 따옴표, 연산자, SQL 구문 등이 애플리케이션의 쿼리 구조를 바꾸도록 만드는 공격이다.

직접 문자열 연결은 입력과 SQL 명령의 경계를 없애므로 위험하다. 반면 준비된 문장과 매개변수 바인딩은 입력을 SQL 코드가 아닌 데이터로 처리한다.

인코딩, 소문자 변환, 세션·파일 저장은 SQL 인젝션의 근본 대책이 아니다. 핵심 대책은 문자열 연결을 피하고 매개변수화된 쿼리를 사용하는 것이다.

NoteBase

선지별 해설

① X
사용자 입력을 서버의 세션에 저장하는 것만으로는 입력값이 SQL 쿼리 구문에 직접 포함되지 않는다. 틀린 표현은 '세션으로 저장'이 SQL 인젝션 가능성이 가장 높은 구조라는 부분이다. 올바르게는 세션에 저장한 값을 이후 SQL문에 문자열로 직접 연결할 때 SQL 인젝션 위험이 생긴다.

② X
사용자 입력을 파일에 저장한 뒤 비동기 처리한다는 사실만으로 SQL 구문이 만들어지지는 않는다. 틀린 표현은 '파일로 저장 후 비동기 처리' 자체가 가장 위험하다는 부분이다. 올바르게는 비동기 처리 단계에서도 입력값을 SQL문에 직접 연결하면 위험하므로 매개변수 바인딩을 사용해야 한다.

③ X
입력값을 인코딩하여 정적 HTML로 출력하는 구조는 SQL 쿼리 구성과 직접 관련되지 않는다. 틀린 표현은 '인코딩 후 정적 HTML 출력'이 SQL 인젝션 가능성이 가장 높다는 부분이다. 올바르게는 HTML 출력 인코딩은 주로 스크립트 삽입을 막는 출력 대책이며, SQL 인젝션은 별도로 매개변수화된 쿼리로 방지한다.

④ X
입력값을 소문자로 바꾸어도 따옴표, 연산자와 SQL 키워드의 의미가 사라지지 않으므로 안전한 방어가 아니다. 다만 선지는 입력값을 SQL문에 직접 연결한다고 명시하지 않아 ⑤보다 위험 구조가 분명하지 않다. 틀린 표현은 '소문자 변환'만으로 SQL 인젝션 위험이 가장 높다고 보는 부분이다. 올바르게는 대소문자 변환에 의존하지 않고 매개변수화된 쿼리를 사용해야 한다.

⑤ O
사용자 입력값을 문자열로 직접 연결하여 SQL 쿼리를 만들면 공격 입력이 쿼리의 조건이나 구문으로 해석될 수 있다. 입력과 SQL 코드의 경계가 무너지므로 다섯 구조 중 SQL 인젝션 가능성이 가장 높다.

오답 포인트

④의 '모두 소문자로 변환'은 보안 처리처럼 보이지만 SQL 인젝션 방어가 아니다. 그러나 이 문항은 단순히 방어가 약한 처리를 찾는 것이 아니라 공격 가능성이 가장 높은 코드 구조를 묻는다. ⑤의 '문자열로 직접 연결해 SQL 쿼리를 구성'이 취약점의 발생 원인을 정확히 드러낸다.

다시 나오면 이렇게 판단

사용자 입력이 저장·출력되는 위치보다 SQL문이 만들어지는 방식을 먼저 확인한다. 입력값을 쿼리 문자열에 연결하면 위험하고, SQL문과 입력값을 분리하여 매개변수로 전달하면 안전성이 높아진다.

NoteBase

암기 포인트

SQL 인젝션의 핵심 위험 신호는 '사용자 입력 + SQL 문자열 직접 연결'이다.

NoteBase

3. TCP/IP 프로토콜 계층의 응용 계층 보안 서비스로 옳지 않은 것은?

① PGP(Pretty Good Privacy)
② SET(Secure Electronic Transaction)
③ VPN(Virtual Private Network)
④ S/MIME(Secure Multi-Purpose Internet Mail Extensions)
⑤ Kerberos

정답 3번

출제 포인트

TCP/IP 계층별 보안 기술 가운데 전자우편·전자상거래·사용자 인증처럼 응용 서비스 자체를 보호하는 기술과 네트워크 계층을 보호하는 VPN을 구별하는 문제이다.

핵심 개념

응용 계층 보안은 전자우편, 전자상거래, 사용자 인증 등 특정 응용 서비스의 데이터와 기능을 보호한다. PGP와 S/MIME은 전자우편 보안, SET은 전자상거래 결제 보안, Kerberos는 네트워크 환경의 사용자·서비스 인증을 제공한다. 반면 이 문항의 계층별 대표 분류에서 VPN은 IP 계층의 통신 경로를 보호하는 네트워크 계층 보안 기술로 본다.

선지별 해설

① O — PGP는 전자우편 메시지의 암호화와 전자서명을 제공하는 응용 계층 보안 기술이다.
② O — SET은 인터넷상의 신용카드 전자상거래를 안전하게 처리하기 위해 기밀성, 무결성, 인증을 제공하는 응용 계층 보안 규격이다.
③ X — VPN을 응용 계층 보안 서비스로 분류한 점이 틀렸다. 이 문항의 대표적 계층 분류에서는 VPN이 IPsec 등을 이용해 IP 패킷과 네트워크 간 통신 경로를 보호하는 네트워크 계층 보안 서비스이다. 따라서 올바른 표현은 'VPN은 네트워크 계층 보안 서비스이다'이다.
④ O — S/MIME은 전자우편에 암호화와 전자서명을 적용하여 기밀성, 무결성, 인증을 제공하는 응용 계층 보안 기술이다.
⑤ O — Kerberos는 티켓을 이용해 사용자와 네트워크 서비스의 신원을 인증하는 응용 계층 인증 프로토콜이다.

오답 포인트

VPN도 사용자가 실행하는 보안 서비스처럼 보이므로 응용 계층으로 착각하기 쉽다. 그러나 이 문항은 사용 화면이 아니라 보호 대상과 동작 계층을 묻는다. PGP·SET·S/MIME·Kerberos는 특정 응용의 메시지·거래·인증을 보호하고, ③의 VPN은 대표적으로 IP 패킷과 네트워크 통신 경로를 보호한다.

NoteBase

다시 나오면 이렇게 판단

전자우편·전자상거래·사용자 인증처럼 특정 응용 기능을 직접 보호하면 응용 계층으로 판단한다. IP 패킷을 암호화하고 원격지나 네트워크 사이에 안전한 터널을 만들면 네트워크 계층의 VPN으로 판단한다.

암기 포인트

응용 계층은 PGP·SET·S/MIME·Kerberos, 네트워크 계층은 대표적으로 IPsec 기반 VPN이다.

NoteBase

4. SSL/TLS 서비스에 대한 설명으로 옳은 것은?

① 송신자와 수신자 간의 접근제어를 관리한다.
② 송신자의 인증 및 데이터 암호화를 지원한다.
③ 인증 헤더를 통하여 송신자를 인증할 수 있다.
④ 메시지를 여러 개의 단편으로 분할하고, 압축을 수행한다.
⑤ 전달되는 데이터가 전송 도중에 변경되지 않았음을 확인할 수 있다.

정답 4번

출제 포인트

SSL/TLS가 제공하는 통신 보안 기능과 레코드 프로토콜의 처리 기능을 구별하는 문제이다.

핵심 개념

SSL/TLS: 응용 계층과 전송 계층 사이에서 통신 상대 인증, 데이터 기밀성, 무결성을 제공하는 보안 프로토콜이다.
접근제어: 인증된 사용자가 어떤 자원에 어떤 행위를 할 수 있는지를 권한에 따라 제한하는 기능으로, SSL/TLS의 통신 채널 보호와는 구별된다.
인증 헤더(AH): IPsec에서 무결성과 출처 인증을 제공하는 프로토콜 요소이며, SSL/TLS의 인증 방식이 아니다.
SSL/TLS 레코드 프로토콜은 상위 계층 데이터를 단편화하고, 전통적 SSL/TLS 처리에서는 선택적 압축을 거쳐 무결성 보호와 암호화를 적용한다.

선지별 해설

① X — 틀린 표현은 '송신자와 수신자 간의 접근제어를 관리한다'이다. SSL/TLS는 두 통신 주체 사이의 보안 채널을 형성하지만 자원 이용 권한을 결정하지 않는다. 올바르게는 접근제어는 응용 프로그램이나 운영체제 등의 권한 관리 기능이 담당한다.
② O — SSL/TLS 핸드셰이크는 인증서와 서명 등을 이용해 통신 상대를 인증할 수 있고, 협상된 대칭키 암호를 이용해 전송 데이터를 암호화한다. 서버 인증이 일반적이며 클라이언트 인증도 선택적으로 지원하므로 기술적으로 옳은 설명이다.
③ X — 틀린 표현은 '인증 헤더를 통하여'이다. 인증 헤더(AH)는 IPsec의 구성 요소이다. 올바르게는 SSL/TLS는 핸드셰이크 과정의 인증서와 전자서명 등을 통해 통신 상대를 인증한다.
④ O — SSL/TLS 레코드 프로토콜은 상위 계층의 메시지를 여러 레코드 단위로 단편화하며, 전통적 SSL/TLS 처리 절차에는 선택적 압축 단계가 포함된다. 공식 채점에서는 이 선지를 정답으로 제시한다.
⑤ O — SSL/TLS는 MAC 또는 AEAD 인증 태그를 이용해 전송 데이터의 무결성을 검증하므로, 전송 중 데이터가 변경되었는지를 탐지할 수 있다. 따라서 이 선지도 기술적으로 옳은 설명이다.
공식 정답은 4번이지만, 문언대로 판단하면 ②와 ⑤도 일반적인 SSL/TLS 기능에 해당하므로 이 문항에는 복수 정답의 소지가 있다.

NoteBase

오답 포인트

①은 안전한 연결을 만든다는 사실을 접근권한까지 관리한다는 뜻으로 넓힌 함정이다. ③은 SSL/TLS의 인증 기능과 IPsec의 인증 헤더(AH)를 섞은 함정이다. ④의 '단편화'는 IP 계층의 단편화가 아니라 SSL/TLS 레코드 단위로 나누는 처리라는 점을 구별해야 한다.

다시 나오면 이렇게 판단

SSL/TLS 기능은 '상대 인증·기밀성·무결성'으로 판단하고, 권한 관리인 접근제어와 IPsec 용어인 AH·ESP가 나오면 다른 보안 기능과 혼동한 선지인지 확인한다. 레코드 프로토콜의 처리 순서는 단편화, 선택적 압축, 무결성 보호, 암호화의 흐름으로 판단한다.

암기 포인트

SSL/TLS는 인증·암호화·무결성, AH는 IPsec, 접근제어는 권한 관리이다.

NoteBase

5. 「개인정보 보호법」에 따른 정보주체의 권리로 옳지 않은 것은?

① 개인정보 열람 청구권
② 개인정보 이전 요청권
③ 개인정보 삭제 요구권
④ 개인정보 처리 정지 요구권
⑤ 개인정보 처리에 관한 동의 철회권

정답 2번

쟁점

이 문제는 「개인정보 보호법」이 정보주체에게 보장하는 권리의 종류에 관한 문제이다. 핵심은 법이 사용하는 정확한 권리 명칭과 개인정보처리자의 처리행위를 구별하는 것이다.

용어 풀이

정보주체 = 처리되는 개인정보로 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람이다.
전송 요구권 = 정보주체가 일정한 요건 아래 자신의 개인정보를 본인이나 다른 적격한 자에게 보내도록 요구하는 권리이다.

핵심 구분

「개인정보 보호법」은 정보주체에게 개인정보의 열람, 정정·삭제, 처리정지, 동의 철회 등을 요구할 권리를 보장한다. 현행법은 개인정보의 전송을 요구할 권리도 규정하지만, 그 법정 용어는 '개인정보 이전 요청권'이 아니라 '개인정보 전송 요구권'이다. 특히 개인정보의 국외 이전은 개인정보처리자가 개인정보를 국외의 제3자에게 제공하거나 처리하게 하는 행위를 가리키므로, 정보주체의 전송 요구권과 구별된다.

NoteBase

선지별 해설

① O
- 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 요구할 수 있다.

② X
- '개인정보 이전 요청권'은 「개인정보 보호법」이 사용하는 정확한 권리 명칭이 아니다. 현행법이 인정하는 것은 일정한 요건에 따른 개인정보 전송 요구권이다.
- 틀린 표현: 개인정보 이전 요청권
- 올바른 표현: 개인정보 전송 요구권

③ O
- 정보주체는 자신의 개인정보를 열람한 뒤 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만 다른 법령에서 수집 대상으로 명시한 개인정보에는 삭제 요구가 제한될 수 있다.

④ O
- 정보주체는 개인정보처리자에게 자신의 개인정보 처리의 전부 또는 일부를 정지하도록 요구할 수 있다. 법률상 특별한 사유가 있으면 개인정보처리자가 그 요구를 거절할 수 있다.

⑤ O
- 정보주체는 개인정보 처리에 관한 동의를 철회할 수 있다. 동의가 철회되면 개인정보처리자는 원칙적으로 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다.

오답 포인트

②의 '이전'을 현행법상 '전송'과 같은 표현으로 보아 넘기는 것이 함정이다. 법령형 문항에서는 비슷한 일상어보다 조문이 사용하는 정확한 용어를 기준으로 판단한다. 또한 국외 이전은 개인정보처리자의 처리행위이고, 전송 요구는 정보주체의 권리라는 차이가 있다.

다시 나오면 이렇게 판단

정보주체의 권리를 묻는 문항에서는 열람, 정정·삭제, 처리정지, 동의 철회, 전송 요구처럼 조문상의 권리 명칭을 먼저 확인한다. 이어 '요구권'인지 개인정보처리자가 수행하는 '처리행위'인지 구별하면 된다.

암기 포인트

정보주체는 열람·정정·삭제·처리정지·동의 철회·전송을 요구하고, 법정 용어는 '이전 요청'이 아니라 '전송 요구'이다.

NoteBase

6. 다음과 같은 해시값을 생성하는 알고리즘은? (단, 해시값은 16진수임)

f287a3e6d95e1616724ed8c2bc853903375990c4

① AES
② SHA-1
③ MD-5
④ SHA-2
⑤ SEED

정답 2번

출제 포인트

해시값의 16진수 자릿수로 출력 비트 수를 계산하고, 이를 각 암호 알고리즘의 기능 및 출력 길이와 대응시키는 문제이다.

핵심 개념

16진수 한 자리는 4비트를 나타내므로 제시된 40자리 해시값은 160비트이다. SHA-1은 임의 길이의 입력을 160비트 해시값으로 변환하는 해시 함수이다. MD5는 128비트 해시값을 생성하며, AES와 SEED는 해시 함수가 아니라 대칭키 블록 암호이다. SHA-2 계열은 SHA-224, SHA-256, SHA-384, SHA-512처럼 SHA-1과 다른 출력 길이를 사용한다.

NoteBase

선지별 해설

① X
AES라는 판단이 틀리다. AES는 평문을 암호문으로 변환하는 대칭키 블록 암호이며, 올바른 알고리즘은 160비트 해시값을 생성하는 SHA-1이다.

② O
SHA-1은 160비트, 즉 16진수 40자리의 해시값을 생성하므로 제시된 값의 길이와 일치한다.

③ X
MD-5라는 판단이 틀리다. MD5는 128비트, 즉 16진수 32자리의 해시값을 생성하며, 제시된 40자리 값에 해당하는 알고리즘은 SHA-1이다.

④ X
SHA-2라는 판단이 틀리다. SHA-2 계열의 대표 출력 길이는 224비트, 256비트, 384비트, 512비트이며, 제시된 160비트 해시값은 SHA-1에 해당한다.

⑤ X
SEED라는 판단이 틀리다. SEED는 해시 함수가 아니라 대칭키 블록 암호이며, 올바른 알고리즘은 SHA-1이다.

오답 포인트

AES와 SEED를 해시 함수로 혼동하거나, SHA라는 공통 이름만 보고 SHA-1과 SHA-2를 구분하지 않는 것이 함정이다. 이 문항에서는 해시값의 내용이 아니라 16진수 40자리라는 길이가 결정적 단서이다.

다시 나오면 이렇게 판단

먼저 16진수 자릿수에 4를 곱해 비트 수를 구한다. 그다음 128비트는 MD5, 160비트는 SHA-1, 224·256·384·512비트는 SHA-2 계열로 대응시키고, AES와 SEED는 블록 암호이므로 제외한다.

암기 포인트

MD5는 32자리·128비트, SHA-1은 40자리·160비트이다. AES와 SEED는 해시가 아니라 블록 암호이다.

NoteBase

7. 디지털 증거에 대한 무결성을 확보하기 위한 조치로 옳은 것은?

① 파일 압축
② 파일 암호화
③ 파일 변환
④ 해시값 계산 및 대조
⑤ 파일 분할

정답 4번

출제 포인트

디지털 증거의 무결성을 확인하는 방법과 압축·암호화·변환·분할의 기능을 구별하는 문제이다.

핵심 개념

디지털 증거의 무결성이란 증거를 수집한 뒤 그 내용이 변경되지 않았음을 입증할 수 있는 상태를 말한다. 수집 시점과 검증 시점에 각각 해시값을 계산하여 대조하고, 두 값이 같으면 파일 내용이 동일하다고 판단한다.
해시값은 입력 데이터가 달라지면 다른 값이 나오도록 설계된 고정 길이의 요약값이다.

선지별 해설

① X — '파일 압축'은 파일의 저장 용량을 줄이거나 전송 효율을 높이는 처리일 뿐, 원본과 사본의 동일성을 검증하지 않는다. 올바르게는 무결성 확인을 위해 압축 여부가 아니라 해시값을 계산하여 대조해야 한다.
② X — '파일 암호화'는 허가받지 않은 사람이 내용을 읽지 못하게 하여 기밀성을 확보하는 조치이다. 올바르게는 무결성 확보에는 해시값 계산·대조나 전자서명과 같은 변경 탐지 수단을 사용해야 한다.
③ X — '파일 변환'은 파일의 형식이나 표현 방식을 바꾸는 처리이며, 변환 과정에서 데이터 구조가 달라질 수도 있다. 올바르게는 원본 파일의 해시값을 먼저 계산·보존하고 이후 해시값과 대조하여 변경 여부를 확인해야 한다.
④ O — 디지털 증거를 수집할 때 계산한 해시값과 이후 검증 시 계산한 해시값을 대조하면 파일의 변경 여부를 확인할 수 있으므로 무결성 확보에 적절하다.
⑤ X — '파일 분할'은 하나의 파일을 여러 조각으로 나누는 처리로, 그 자체로 내용이 변하지 않았음을 입증하지 않는다. 올바르게는 분할 전 원본이나 각 분할 파일의 해시값을 기록하고 나중에 대조해야 한다.

오답 포인트

압축·암호화·변환·분할도 파일에 가하는 기술적 처리이므로 무결성 조치처럼 보일 수 있다. 그러나 이 처리들은 각각 용량 축소, 기밀성 확보, 형식 변경, 파일 조각화를 위한 것이며, 변경 여부를 직접 검증하는 핵심 수단은 해시값의 계산과 대조이다.

NoteBase

다시 나오면 이렇게 판단

문제에서 ‘원본과 동일한가’, ‘변조되지 않았는가’, ‘무결성’이 제시되면 수집 당시의 해시값과 현재 해시값을 비교하는지를 확인한다. ‘내용을 숨긴다’는 암호화·기밀성, ‘용량을 줄인다’는 압축, ‘형식을 바꾼다’는 변환으로 구별한다.

암기 포인트

무결성은 해시값 대조, 기밀성은 암호화이다.

NoteBase

8. 다음에서 설명하는 공격 방법은?

> ○ 암호 설계 단계에서 고려하지 않은 전력 소모량, 전자파 누설, 열 등을 이용한 공격 방법으로 폴 코처(Paul Kocher)에 의하여 처음 제안되었다.
>
> ○ 타이밍 공격(timing attack), 전력분석 공격(power attack), 전자파 공격(electromagnetic emission attack) 등이 이 공격의 유형에 해당된다.

① 부채널 공격(side-channel attack)
② 선택 암호문 공격(chosen-ciphertext attack)
③ 전수조사 공격(brute-force attack)
④ 통계적 공격(statistical attack)
⑤ 암호문 단독 공격(ciphertext-only attack)

정답 1번

출제 포인트

암호 알고리즘의 수학적 구조가 아니라 구현 과정에서 새어 나오는 시간·전력·전자파 등의 물리 정보를 이용하는 공격을 구별하는 문제이다.

핵심 개념

부채널 공격은 암호 장치가 연산할 때 발생하는 실행 시간, 전력 소비, 전자파 방사 등의 부가 정보를 관찰하여 비밀정보를 추정하는 공격이다. 타이밍 공격·전력분석 공격·전자파 공격이 대표적인 유형이다.
선택 암호문 공격과 암호문 단독 공격은 공격자가 확보하거나 선택할 수 있는 암호문과 복호 결과의 범위로 구분하는 암호분석 모델이고, 전수조사 공격은 가능한 키를 차례로 시험하는 공격이다.

NoteBase

선지별 해설

① O — 지문의 전력 소모량, 전자파 누설, 열, 실행 시간은 암호 구현에서 의도하지 않게 노출되는 부가 정보이므로 부채널 공격에 해당한다. Paul Kocher가 제안한 타이밍 공격과 전력분석 공격도 대표적인 부채널 공격이다.
② X — 틀린 표현은 '선택 암호문 공격'이다. 선택 암호문 공격은 공격자가 선택한 암호문에 대응하는 평문 또는 복호 결과를 얻어 암호체계를 분석하는 공격이다. 올바르게는 지문의 공격 방법을 '부채널 공격'이라고 해야 한다.
③ X — 틀린 표현은 '전수조사 공격'이다. 전수조사 공격은 가능한 키 후보를 하나씩 시험하여 올바른 키를 찾는 공격이다. 올바르게는 물리적 누설 정보를 이용하는 지문의 방법을 '부채널 공격'이라고 해야 한다.
④ X — 틀린 표현은 '통계적 공격'이다. 통계적 공격은 평문·암호문 또는 측정값에서 나타나는 통계적 특성이나 상관관계를 분석하는 방식이다. 지문은 시간·전력·전자파 같은 구현상의 누설 경로를 기준으로 공격을 분류하므로, 올바르게는 '부채널 공격'이다.
⑤ X — 틀린 표현은 '암호문 단독 공격'이다. 암호문 단독 공격은 공격자가 암호문만 확보한 상태에서 평문이나 키를 추정하는 공격 모델이다. 올바르게는 장치의 물리적 누설 정보를 이용하는 지문의 방법을 '부채널 공격'이라고 해야 한다.

오답 포인트

②와 ⑤는 공격자가 이용할 수 있는 암호문·복호 정보의 조건을 나타내고, ③은 키 공간을 탐색하는 방법이다. 반면 지문은 시간·전력·전자파처럼 암호 장치의 구현 과정에서 새어 나오는 정보를 반복해서 제시하므로 공격의 입력 조건이 아니라 누설 경로에 주목해야 한다.

다시 나오면 이렇게 판단

실행 시간, 소비 전력, 전자파, 열, 소리처럼 암호 연산 과정의 물리적 현상이 단서로 제시되면 부채널 공격으로 판단한다. 가능한 키를 모두 시험하면 전수조사 공격이고, 선택한 암호문의 복호 결과를 이용하면 선택 암호문 공격이며, 암호문만 이용하면 암호문 단독 공격이다.

암기 포인트

시간·전력·전자파·열은 구현 옆길로 새는 정보이므로 부채널 공격이다.

NoteBase

9. 다음에서 설명하는 프라이버시 강화 기술은?

> ○ 대규모 데이터에서 개별 주체들의 개인정보 노출을 최소화하는 동시에 개인정보를 활용할 수 있는 방법
>
> ○ 인공지능(AI) 학습에서 개인정보를 보호하기 위해 데이터를 계산하거나 결과를 산정하기 전에 데이터에 통계적 '노이즈'를 삽입하여 개인정보가 제3자에게 노출되지 않도록 익명성을 제공

① 동형 암호
② 연합 학습
③ 신뢰 실행 환경
④ 제로 지식 증명
⑤ 차분 프라이버시

정답 5번

출제 포인트

이 문제는 데이터나 분석 결과에 통계적 노이즈를 더해 개인의 포함 여부나 개인정보를 추론하기 어렵게 만드는 차분 프라이버시의 특징을 다른 프라이버시 강화 기술과 구별하는 문제이다.

핵심 개념

차분 프라이버시: 데이터의 계산 과정이나 결과에 통계적 노이즈를 추가하여 특정 개인의 데이터가 포함되었는지에 따른 결과 차이를 제한하는 프라이버시 보호 기법이다. 키워드는 '통계적 노이즈', '개인 단위 노출 최소화', '데이터 활용 가능'이다.
동형 암호는 암호문을 복호화하지 않고 계산하는 기술이고, 연합 학습은 원본 데이터를 각 참여자에게 둔 채 학습 결과를 모으는 방식이다. 신뢰 실행 환경은 격리된 하드웨어 영역에서 처리하며, 제로 지식 증명은 비밀 자체를 공개하지 않고 어떤 명제가 참임을 증명한다.

NoteBase

선지별 해설

① X
틀린 표현은 '동형 암호'이다. 동형 암호는 암호화된 데이터를 복호화하지 않은 상태로 연산할 수 있게 하는 기술이다. 통계적 노이즈를 추가해 개인별 노출을 제한하는 설명은 차분 프라이버시에 해당한다.

② X
틀린 표현은 '연합 학습'이다. 연합 학습은 원본 데이터를 중앙으로 모으지 않고 각 참여자의 장치나 기관에서 모델을 학습한 뒤 모델 갱신값 등을 집계하는 방식이다. 데이터나 결과에 통계적 노이즈를 넣어 익명성을 제공하는 설명은 차분 프라이버시에 해당한다.

③ X
틀린 표현은 '신뢰 실행 환경'이다. 신뢰 실행 환경은 프로세서의 보호·격리된 영역에서 코드와 데이터를 안전하게 처리하는 기술이다. 노이즈를 이용하여 개인의 정보 노출 가능성을 줄이는 기술은 차분 프라이버시이다.

④ X
틀린 표현은 '제로 지식 증명'이다. 제로 지식 증명은 비밀 정보 자체를 공개하지 않고도 어떤 명제가 참이라는 사실을 상대방에게 증명하는 기술이다. 통계적 노이즈로 개별 정보의 영향을 감추는 기술은 차분 프라이버시이다.

⑤ O
차분 프라이버시는 데이터 분석이나 인공지능 학습 과정에서 통계적 노이즈를 추가하여 특정 개인의 데이터가 결과에 미치는 영향을 제한한다. 따라서 대규모 데이터의 활용 가능성을 유지하면서 개인 단위의 정보 노출을 최소화한다.

오답 포인트

프라이버시 강화 기술은 모두 개인정보 보호를 목적으로 하므로 목적만 보고 고르면 혼동하기 쉽다. 이 문항의 결정적 표현은 '통계적 노이즈를 삽입'이다. 암호문 상태의 연산은 동형 암호, 분산된 원본 데이터로 공동 학습하는 것은 연합 학습, 격리 영역에서의 처리는 신뢰 실행 환경, 비밀 공개 없는 증명은 제로 지식 증명에 해당한다.

다시 나오면 이렇게 판단

기술의 공통 목적보다 작동 방식을 확인한다. '노이즈 추가'가 보이면 차분 프라이버시, '암호문 연산'은 동형 암호, '로컬 학습 후 갱신값 집계'는 연합 학습, '격리된 보호 영역'은 신뢰 실행 환경, '비밀을 밝히지 않는 증명'은 제로 지식 증명으로 판단한다.

NoteBase

암기 포인트

노이즈는 차분 프라이버시, 암호문 연산은 동형 암호, 분산 학습은 연합 학습, 격리 실행은 신뢰 실행 환경, 비밀 없는 증명은 제로 지식 증명이다.

NoteBase

10. 다크웹(Dark Web)에 대한 설명으로 옳지 않은 것은?

① 사용자와 서버의 익명성을 유지할 가능성이 높고, IP 주소 추적이 어렵다.

② 종단 간 암호화를 통해 통신 내용을 보호하여 보안성이 뛰어나다.

③ 중앙 서버 없이 분산된 노드들로 운영되는 구조이다.

④ 도메인은 일반적으로 .onion 확장자를 가지며, Tor 네트워크 전용으로 운영된다.

⑤ 고립된 폐쇄형 네트워크로 구성되어 있어, 물리적 인터넷 인프라를 사용하지 않고 자체적인 독립 인프라에서 운영된다.

정답 5번

출제 포인트

다크웹의 익명성·암호화·분산성·접속 방식과 실제 기반 인프라를 구분하는 문제이다.

핵심 개념

다크웹은 일반 검색 엔진에 공개되지 않고 Tor 같은 익명화 네트워크와 전용 소프트웨어를 통해 접근하는 웹 영역이다.

다크웹은 익명성과 추적 회피를 강화하지만, 물리적으로 별도의 통신망을 새로 만드는 것은 아니다. Tor의 중계 노드와 다크웹 서비스도 인터넷 회선, 라우터, 서버 등 기존 인터넷 인프라 위에서 작동한다.

NoteBase

선지별 해설

① O — Tor는 여러 중계 노드를 거치게 하여 사용자와 서비스 서버의 실제 IP 주소 및 위치를 직접 연결하기 어렵게 하므로 익명성을 높이고 추적을 어렵게 한다. 다만 익명성이 절대적으로 보장된다는 뜻은 아니다.

② O — Tor는 통신 데이터를 여러 겹으로 암호화하여 각 중계 노드가 전체 경로와 통신 내용을 한꺼번에 알기 어렵게 한다. 특히 .onion 서비스와의 통신은 Tor 네트워크 내부에서 보호되므로 일반적인 직접 통신보다 기밀성과 익명성이 강화된다.

③ O — Tor는 다수의 분산된 중계 노드를 거쳐 트래픽을 전달하는 구조로 운용되므로 하나의 중앙 통신 서버가 모든 트래픽을 직접 중계하는 방식이 아니다.

④ O — 다크웹의 대표적인 Tor 은닉 서비스는 일반적으로 .onion 주소를 사용하며, Tor Browser와 같은 Tor 네트워크 접속 수단이 필요하다.

⑤ X — 틀린 표현은 '물리적 인터넷 인프라를 사용하지 않고 자체적인 독립 인프라에서 운영된다'이다. 올바르게는 다크웹이 논리적으로 접근이 제한된 오버레이 네트워크이지만, 실제 통신은 기존 인터넷의 회선·라우터·서버 등 물리적 인프라를 이용한다고 해야 한다.

오답 포인트

'폐쇄형'이라는 말 때문에 다크웹을 인터넷과 물리적으로 분리된 독립망으로 오해하기 쉽다. 다크웹의 폐쇄성은 전용 접속 방식과 비공개 주소 체계에서 비롯되는 논리적 특성이며, 기반 통신 인프라까지 별개라는 뜻은 아니다.

다시 나오면 이렇게 판단

다크웹 관련 선지는 '논리적 접근 구조'와 '물리적 기반망'을 나누어 판단한다. Tor, .onion, 다중 중계, 익명화는 논리적 구조의 특징이고, 실제 데이터 전송은 기존 인터넷 인프라에 의존한다.

암기 포인트

다크웹은 인터넷과 분리된 별도 물리망이 아니라, 기존 인터넷 위에서 Tor 등으로 구현되는 익명화 오버레이 영역이다.

NoteBase

11. 한국의 CSAP(Cloud Security Assurance Program) 제도에 대한 설명으로 옳지 않은 것은?

① 국내 공공기관이 클라우드 서비스를 제공하기 전에 해당 서비스의 보안성을 사전에 평가받도록 하는 제도이다.

② CSAP 인증은 서비스 유형(IaaS, PaaS, SaaS)에 따라 구분되며, 각 유형별로 요구되는 보안 기준이 상이하다.

③ 최초 인증 이후에도 정기적인 사후 심사를 통해 서비스 보안 상태를 지속적으로 검증한다.

④ 민간 기업은 공공시장 진출을 위해 CSAP 인증을 받을 수 있으며, 이를 통해 공공기관 대상 클라우드 서비스 공급이 가능해진다.

⑤ 개인정보나 민감정보를 처리하는 클라우드 서비스가 CSAP 인증을 받으려면 데이터의 물리적 위치에 대한 평가도 필요하다.

정답 1번

출제 포인트

CSAP의 인증 대상이 공공기관인지 클라우드컴퓨팅서비스인지, 그리고 인증 유형·사후관리·물리적 보호조치가 어떻게 구성되는지를 묻는 문제이다.

핵심 개념

CSAP는 클라우드컴퓨팅서비스 제공자가 제공하는 서비스의 보안 관련 조치와 활동이 보안인증기준에 적합한지를 인증하는 제도이다. 인증 대상은 공공기관 자체가 아니라 클라우드컴퓨팅서비스이며, 인증평가에는 관리적·물리적·기술적 보호조치 등이 포함된다.

NoteBase

선지별 해설

① X
틀린 표현은 '국내 공공기관이 클라우드 서비스를 제공하기 전에'이다. CSAP는 공공기관이 제공할 서비스를 사전 평가받는 제도가 아니다. 올바르게는 클라우드컴퓨팅서비스 제공자가 공공기관 등에 공급하려는 서비스에 대해 보안인증기준 적합 여부를 평가받는 제도이다.

② O
보안인증은 IaaS, SaaS, PaaS 등 서비스 제공 형태에 따라 유형이 구분되며, 적용되는 보안인증기준도 유형과 등급에 따라 달라진다.

③ O
인증 취득 후에도 유효기간 동안 사후평가를 실시하여 보안인증기준을 계속 준수하는지 확인한다. 따라서 최초 인증만으로 관리가 끝나는 것이 아니다.

④ O
민간 클라우드컴퓨팅서비스 제공자도 자신의 서비스에 대해 CSAP 인증을 받을 수 있고, 인증된 서비스를 공공기관에 공급할 수 있다.

⑤ O
국가기관 등이 이용하는 클라우드서비스에는 시스템과 데이터의 물리적 위치 및 영역 분리와 같은 보호조치가 평가 대상에 포함된다. 따라서 개인정보나 민감정보를 처리하는 인증 대상 서비스도 데이터의 물리적 위치에 관한 평가를 받게 된다.

오답 포인트

①은 '공공기관이 클라우드 서비스를 이용하기 전에 안전성을 검토한다'는 절차와 '클라우드컴퓨팅서비스 제공자가 CSAP 인증을 받는다'는 절차의 주체를 바꾸어 놓았다. 이 문항의 핵심 함정은 평가 시점보다 인증의 대상과 신청 주체이다.

다시 나오면 이렇게 판단

CSAP 문항에서는 먼저 인증받는 주체와 대상을 확인한다. 클라우드컴퓨팅서비스 제공자가 자신의 서비스에 대해 인증을 받고, 인증 후에는 사후평가로 기준 준수 여부를 지속 확인한다고 판단한다.

암기 포인트

CSAP는 공공기관 인증이 아니라 클라우드서비스 인증이며, 최초평가 뒤에도 사후평가가 이어진다.

NoteBase

12. 방화벽의 유형과 그 특징에 대한 설명으로 옳지 않은 것은?

① 패킷 필터링 방화벽은 IP 주소, 포트 번호, 프로토콜 등의 정보를 기반으로 트래픽을 허용하거나 차단한다.

② 상태 기반 방화벽은 각 연결의 상태 정보를 추적하여, 비정상적인 연결 요청이나 응답을 감지할 수 있다.

③ 애플리케이션 계층 방화벽은 HTTP, FTP 프로토콜의 내용을 분석할 수 있으며, 콘텐츠 수준의 보안 통제를 수행한다.

④ 프록시 방화벽은 물리 계층에서 작동하며, 패킷의 헤더 정보를 확인하여 빠르게 트래픽을 처리한다.

⑤ 차세대 방화벽은 전통적인 방화벽 기능 외에도 애플리케이션 제어, 사용자 식별, 침입 방지 등의 기능이 있다.

정답 4번

출제 포인트

방화벽을 패킷 필터링, 상태 기반, 애플리케이션 계층, 프록시, 차세대 방식으로 나누고 각 방식의 동작 계층과 검사 대상을 구별하는 문제이다.

핵심 개념

패킷 필터링 방화벽은 패킷의 IP 주소, 포트 번호, 프로토콜 같은 헤더 정보를 규칙과 비교하여 통과 여부를 결정한다.
상태 기반 방화벽은 연결별 상태 정보를 기록하고 정상적인 세션에 속하는 패킷인지 판단한다.
애플리케이션 계층 방화벽은 HTTP, FTP 등 응용 프로토콜과 그 내용을 분석하여 세밀하게 통제한다.
프록시 방화벽은 응용 계층에서 클라이언트와 서버 사이의 중계자 역할을 하며, 양쪽의 연결을 분리하여 응용 데이터까지 검사한다.
차세대 방화벽은 전통적 방화벽 기능에 애플리케이션 식별·제어, 사용자 식별, 침입 방지 등의 기능을 결합한다.

NoteBase

선지별 해설

① O — 패킷 필터링 방화벽은 IP 주소, 포트 번호, 프로토콜 등의 패킷 헤더 정보를 규칙과 대조하여 트래픽을 허용하거나 차단한다.
② O — 상태 기반 방화벽은 연결의 생성·유지·종료 상태를 추적하므로, 정상 세션과 맞지 않는 비정상 연결 요청이나 응답을 탐지할 수 있다.
③ O — 애플리케이션 계층 방화벽은 HTTP, FTP와 같은 응용 프로토콜을 이해하고 요청이나 콘텐츠의 내용을 분석하여 콘텐츠 수준의 보안 통제를 수행할 수 있다.
④ X — 틀린 표현은 '물리 계층에서 작동하며, 패킷의 헤더 정보를 확인하여 빠르게 트래픽을 처리한다'이다. 프록시 방화벽은 물리 계층이 아니라 애플리케이션 계층에서 중계자로 동작하며 응용 데이터까지 검사한다. 헤더 중심의 빠른 처리는 패킷 필터링 방화벽의 특징에 가깝다.
⑤ O — 차세대 방화벽은 패킷 필터링과 상태 기반 검사 같은 전통적 기능에 애플리케이션 제어, 사용자 식별, 침입 방지 기능 등을 통합한다.

오답 포인트

④는 '프록시'라는 이름에 패킷 헤더 검사와 빠른 처리라는 패킷 필터링의 특징을 섞어 놓았다. 프록시는 연결을 대신 중계하면서 응용 계층의 내용을 깊게 검사하므로 단순 헤더 검사 방식보다 처리 부담이 큰 편이다.

다시 나오면 이렇게 판단

선지에서 검사 대상을 먼저 확인한다. IP·포트·프로토콜 헤더이면 패킷 필터링, 연결 상태이면 상태 기반, HTTP·FTP의 내용이면 애플리케이션 계층, 중계자 역할이면 프록시, 애플리케이션 제어·사용자 식별·침입 방지의 통합이면 차세대 방화벽으로 판단한다.

암기 포인트

패킷 필터링은 헤더, 상태 기반은 세션, 애플리케이션 방화벽은 내용, 프록시는 응용 계층 중계, 차세대 방화벽은 통합 보안이다.

NoteBase

13. SSH(Secure Shell)에 대한 설명으로 옳지 않은 것은?

① 네트워크상에서 원격 접속을 제공하기 위해 설계된 프로토콜로, 대칭키와 비대칭키 암호화가 모두 사용된다.

② 기본적으로 22번 포트를 사용하며, 세션 동안 전달되는 데이터는 도청 및 중간자 공격으로부터 안전하다.

③ 클라이언트가 서버에 접속하면, 서버가 먼저 클라이언트의 공개키를 인증하고 세션이 시작된다.

④ 원격 터미널 접속 외에도 파일 전송, 포트 포워딩, 터널링 등의 기능도 지원한다.

⑤ 공개키 기반 또는 Kerberos 기반의 인증을 사용하기도 한다.

정답 3번

출제 포인트

SSH의 암호화 방식, 기본 포트, 인증 순서와 지원 기능을 구별하는 문제이다.

핵심 개념

SSH는 안전하지 않은 네트워크에서 원격 로그인과 명령 실행을 암호화하여 제공하는 프로토콜이다. 공개키 방식은 서버 신원 확인·키 교환·사용자 인증 등에 활용되고, 대칭키 방식은 세션 중 실제 데이터를 빠르게 암호화하는 데 활용된다. 연결 과정에서는 클라이언트가 서버의 호스트 키를 먼저 검증한 뒤, 서버가 공개키·비밀번호·Kerberos 등의 방식으로 사용자를 인증한다.

선지별 해설

① O — SSH는 비대칭키 암호 기술을 서버 인증·키 교환·공개키 인증 등에 활용하고, 합의된 대칭키로 세션 데이터를 암호화한다.

② O — SSH의 기본 포트는 22번이며, 통신 내용을 암호화하고 서버의 호스트 키를 검증하므로 도청과 중간자 공격에 대응한다. 단, 중간자 공격 방지를 위해서는 호스트 키를 올바르게 검증해야 한다.

③ X — 틀린 표현은 '서버가 먼저 클라이언트의 공개키를 인증'한다는 부분이다. 올바르게는 클라이언트가 먼저 서버의 호스트 키를 검증하고, 그 뒤 서버가 공개키·비밀번호·Kerberos 등 허용된 방식으로 사용자를 인증한다. 클라이언트 인증이 반드시 공개키 방식으로 이루어지는 것도 아니다.

④ O — SSH는 원격 터미널뿐 아니라 SFTP·SCP를 통한 파일 전송, 포트 포워딩, 터널링도 지원한다.

⑤ O — SSH는 공개키 기반 사용자 인증을 지원하며, GSSAPI를 이용한 Kerberos 기반 인증도 사용할 수 있다.

NoteBase

오답 포인트

③은 서버도 공개키를 사용하고 클라이언트도 공개키 인증을 사용할 수 있다는 사실을 섞어 인증 주체와 순서를 뒤바꾼 선지이다. SSH 연결 초기에 우선 확인되는 것은 서버의 호스트 키이며, 사용자 인증 방식은 공개키로 한정되지 않는다.

다시 나오면 이렇게 판단

SSH 연결 문제에서는 '서버 호스트 키 검증 → 사용자 인증 → 원격 서비스 이용'의 흐름을 기준으로 판단한다. 공개키는 인증·키 교환에, 대칭키는 세션 데이터 암호화에 주로 쓰인다는 역할도 함께 구분한다.

암기 포인트

SSH는 22번 포트, 서버 호스트 키를 먼저 검증, 사용자 인증은 공개키·비밀번호·Kerberos 등으로 수행한다.

NoteBase

14. 은행 업무 환경에서의 접근 제어 방식(Access Control Model)에 대한 설명으로 옳은 것은?

① RBAC(Role-Based Access Control)는 조직 내 역할에 따라 접근 권한을 부여하므로, '여신 심사역' 역할을 가진 사용자는 자동으로 관련 시스템에 접근할 수 있다.

② DAC(Discretionary Access Control)는 자산 소유자가 권한을 자유롭게 부여할 수 있기 때문에, 보안 사고 발생 시 책임 소재가 명확해져 금융기관에서 자주 활용된다.

③ ABAC(Attribute-Based Access Control)는 특정 파일을 '중요 파일'로 분류하더라도 사용자 속성이 일치하지 않으면 누구든 접근이 가능하므로 보안성이 낮다.

④ RBAC는 개별 사용자마다 권한을 직접 지정하기 때문에, 사용자가 많을수록 관리가 어려워진다.

⑤ ABAC는 규칙이 아닌 사용자 개별 요청에 따라 접근이 결정되므로, 정책 자동화가 어렵다는 단점이 있다.

정답 1번

출제 포인트

이 문제는 RBAC, DAC, ABAC가 각각 무엇을 기준으로 접근 권한을 결정하는지 묻는 문제이다.

핵심 개념

RBAC: 직무나 역할에 권한을 묶고 사용자를 역할에 배정하는 방식이다. 키워드는 역할이다.
DAC: 자원의 소유자가 다른 사용자에게 접근 권한을 부여하거나 회수하는 방식이다. 키워드는 소유자의 재량이다.
ABAC: 사용자, 자원, 환경 등의 속성과 정책 규칙을 함께 평가하여 접근을 허용하거나 거부하는 방식이다. 키워드는 속성과 정책이다.
즉 RBAC는 역할, DAC는 소유자, ABAC는 속성·정책을 중심으로 구분한다.

NoteBase

선지별 해설

① O — RBAC는 조직의 역할에 권한을 연결하고 사용자를 해당 역할에 배정한다. 따라서 '여신 심사역' 역할에 관련 시스템 접근 권한이 부여되어 있다면 그 역할을 맡은 사용자는 그 권한을 사용할 수 있다.
② X — 틀린 부분은 '책임 소재가 명확해져 금융기관에서 자주 활용된다'이다. DAC는 자산 소유자가 재량으로 권한을 부여하므로 권한 관리의 일관성과 중앙 통제가 약해질 수 있고, 그 자체로 사고 책임이 명확해지는 방식도 아니다. 올바르게는 소유자가 자원 접근 권한을 자율적으로 부여하는 방식이라고 해야 한다.
③ X — 틀린 부분은 '사용자 속성이 일치하지 않으면 누구든 접근이 가능하다'이다. ABAC는 중요도 같은 자원 속성 하나만으로 허용하지 않고 사용자·자원·환경 속성이 정책 조건을 충족하는지를 평가한다. 올바르게는 정책에 정해진 속성 조건이 일치할 때만 접근을 허용한다고 해야 한다.
④ X — 틀린 부분은 '개별 사용자마다 권한을 직접 지정한다'이다. RBAC는 개별 사용자가 아니라 역할에 권한을 부여하고 사용자를 역할에 연결하므로 대규모 조직의 권한 관리가 쉬워진다. 올바르게는 역할 단위로 권한을 관리한다고 해야 한다.
⑤ X — 틀린 부분은 '규칙이 아닌 사용자 개별 요청에 따라 접근이 결정되어 정책 자동화가 어렵다'이다. ABAC는 속성과 정책 규칙을 동적으로 평가하므로 세밀한 접근 제어와 정책 자동화에 적합하다. 올바르게는 정책 규칙에 따라 접근이 결정된다고 해야 한다.

오답 포인트

②는 DAC의 소유자 재량이라는 특징을 책임 소재 명확화 및 금융기관의 빈번한 활용이라는 부당한 결론으로 연결했고, ④는 RBAC의 관리 단위를 역할이 아닌 개별 사용자로 바꾸어 놓았다. ③과 ⑤는 ABAC가 속성 기반 정책을 평가한다는 핵심을 반대로 서술했다. 특히 '자유롭게 부여'가 곧 책임 명확화나 높은 보안성을 뜻하지는 않는다.

다시 나오면 이렇게 판단

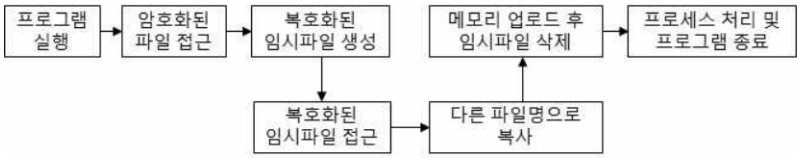
권한 결정의 중심이 역할이면 RBAC, 자원 소유자의 재량이면 DAC, 여러 속성과 정책 조건이면 ABAC로 판단한다. 이어서 선지의 장단점 설명이 그 관리 구조와 일치하는지 확인한다.

암기 포인트

RBAC는 역할, DAC는 소유자 재량, ABAC는 속성과 정책이다.

NoteBase

15. 다음 그림과 같이 수행하는 공격의 명칭은?



① 스니핑 공격
② 백도어 공격
③ 포맷 스트링 공격
④ 레이스 컨디션 공격
⑤ 버퍼 오버플로 공격

정답 4번

출제 포인트

이 문제는 복호화된 임시파일이 생성된 뒤 메모리에 올라가기 전까지의 시간차에 다른 파일을 끼워 넣는 흐름을 보고 레이스 컨디션 공격을 식별하는 문제이다. 레이스 컨디션은 여러 실행 주체가 공유 자원에 접근하는 순서나 시점에 따라 결과가 달라지는 취약점을 이용하는 공격이다.

선지별 해설

① X — 스니핑 공격은 네트워크를 흐르는 패킷이나 통신 내용을 몰래 엿듣는 공격이다. 이 도식에는 패킷 도청이 아니라 임시파일의 생성과 교체 시점이 나타나므로 해당하지 않는다. 틀린 표현인 '스니핑 공격'은 '레이스 컨디션 공격'으로 고쳐야 한다.
② X — 백도어 공격은 정상적인 인증·접근 절차를 우회할 수 있는 숨은 접근 경로를 설치하거나 이용하는 공격이다. 도식의 핵심은 숨은 접속 경로가 아니라 파일 처리 사이의 시간차를 악용하는 것이므로 해당하지 않는다. 틀린 표현인 '백도어 공격'은 '레이스 컨디션 공격'으로 고쳐야 한다.
③ X — 포맷 스트링 공격은 외부 입력이 출력 함수의 서식 문자열로 부적절하게 사용될 때 메모리를 읽거나 쓰는 취약점을 이용한다. 도식에는 서식 지정자나 출력 함수가 없으므로 해당하지 않는다. 틀린 표현인 '포맷 스트링 공격'은 '레이스 컨디션 공격'으로 고쳐야 한다.
④ O — 복호화된 임시파일이 생성·접근된 뒤 메모리에 업로드되기 전의 짧은 틈에 다른 파일을 복사하여 처리 대상을 바꾸는 흐름이다. 자원을 확인하거나 준비한 시점과 실제 사용하는 시점 사이의 경쟁 상태를 악용하므로 레이스 컨디션 공격이다.
⑤ X — 버퍼 오버플로 공격은 버퍼의 허용 크기를 넘는 데이터를 기록하여 인접 메모리나 제어 정보를 덮어쓰는 공격이다. 도식에는 버퍼 크기 초과나 메모리 덮어쓰기가 없으므로 해당하지 않는다. 틀린 표현인 '버퍼 오버플로 공격'은 '레이스 컨디션 공격'으로 고쳐야 한다.

NoteBase

오답 포인트

‘암호화된 파일’, ‘복호화’, ‘메모리 업로드’ 같은 보안 용어보다 처리 단계 사이에 다른 파일이 복사되는 시점에 주목해야 한다. 공격 대상을 확인한 때와 실제로 사용한 때가 분리되어 그 사이에 대상이 바뀌는 것이 레이스 컨디션의 핵심 함정이다.

다시 나오면 이렇게 판단

파일이나 권한을 확인한 뒤 실제 사용하기 전까지 틈이 있고, 그 사이 다른 프로세스가 대상 파일·링크·권한을 바꿀 수 있는지를 본다. ‘확인 시점’과 ‘사용 시점’의 불일치가 보이면 레이스 컨디션으로 판단한다.

암기 포인트

확인할 때와 사용할 때가 다르면 TOCTOU형 레이스 컨디션이다.

NoteBase

16. TCP/IP 응용계층의 보안 프로토콜에 해당하는 것만을 <보기>에서 모두 고르면?

< 보 기 >

ㄱ. S/MIME
ㄴ. L2TP
ㄷ. IPSec
ㄹ. SSH

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ
⑤ ㄷ, ㄹ

정답 2번

출제 포인트

TCP/IP 계층별 보안 프로토콜을 구분하고, 응용계층에서 동작하는 S/MIME과 SSH를 찾는 문제이다.

핵심 개념

S/MIME은 전자우편의 암호화와 전자서명을 제공하는 응용계층 보안 프로토콜이다.
SSH는 원격 로그인과 명령 실행 등을 암호화하여 보호하는 응용계층 보안 프로토콜이다.
L2TP는 데이터링크 계층의 터널링 프로토콜이고, IPsec은 IP 패킷을 보호하는 인터넷 계층(네트워크 계층) 보안 프로토콜이다.
따라서 응용계층에 해당하는 것은 ㄱ S/MIME과 ㄹ SSH이다.

NoteBase

선지별 해설

① X — ㄱ S/MIME은 응용계층이지만 ㄴ L2TP는 데이터링크 계층의 터널링 프로토콜이다. 틀린 부분은 'ㄱ, ㄴ'이며, 올바른 조합은 'ㄱ, ㄹ'이다.
② O — ㄱ S/MIME과 ㄹ SSH는 모두 응용계층에서 각각 전자우편 보안과 안전한 원격 접속을 제공한다.
③ X — ㄴ L2TP는 데이터링크 계층, ㄷ IPsec은 인터넷 계층에 해당하므로 둘 다 응용계층이 아니다. 틀린 부분은 'ㄴ, ㄷ'이며, 올바른 조합은 'ㄱ, ㄹ'이다.
④ X — ㄹ SSH는 응용계층이지만 ㄴ L2TP는 데이터링크 계층에 해당한다. 틀린 부분은 'ㄴ, ㄹ'이며, 올바른 조합은 'ㄱ, ㄹ'이다.
⑤ X — ㄹ SSH는 응용계층이지만 ㄷ IPsec은 인터넷 계층에서 IP 패킷을 보호한다. 틀린 부분은 'ㄷ, ㄹ'이며, 올바른 조합은 'ㄱ, ㄹ'이다.

오답 포인트

보안 기능이 있다는 이유만으로 모든 프로토콜을 응용계층으로 분류하면 안 된다. 특히 IPsec의 'IP'는 인터넷 계층을, L2TP의 'Layer 2'는 데이터링크 계층을 가리킨다는 점이 핵심 함정이다.

다시 나오면 이렇게 판단

프로토콜이 보호하는 대상을 기준으로 판단한다. 전자우편과 원격 로그인처럼 사용자 응용 서비스를 직접 보호하면 응용계층이고, IP 패킷을 보호하면 인터넷 계층이며, 2계층 프레임 기반 터널링이면 데이터링크 계층이다.

암기 포인트

메일은 S/MIME, 원격 접속은 SSH, IP 패킷은 IPsec, Layer 2 터널은 L2TP이다.

NoteBase

17. 802.1x/EAP에서 제공하는 기능으로 옳지 않은 것은?

① 디렉터리 리스팅
② 사용권한의 중앙관리
③ 인증서, 스마트카드 등 다양한 인증 제공
④ 세션별 암호화키 제공
⑤ 사용자 인증

정답 1번

출제 포인트

802.1X/EAP가 네트워크 접속 인증과 접근 제어를 위해 제공하는 기능인지, 파일 시스템이나 디렉터리 서비스의 기능인지를 구별하는 문제이다.

핵심 개념

802.1X는 단말이 네트워크에 접속하기 전에 인증을 거치게 하는 포트 기반 네트워크 접근 제어 표준이다.
EAP는 인증서, 스마트카드, 비밀번호 등 여러 인증 방식을 수용하는 인증 프레임워크이며, 802.1X는 EAP 메시지를 전달하여 사용자 인증, 중앙 집중식 접근 제어, 세션 키 생성을 지원한다.
디렉터리 리스팅은 디렉터리에 있는 파일이나 하위 항목의 목록을 보여 주는 기능으로, 802.1X/EAP의 인증 기능과 관계가 없다.

선지별 해설

① X — 디렉터리 리스팅은 파일 시스템이나 웹 서버가 디렉터리의 항목 목록을 표시하는 기능이며, 802.1X/EAP가 제공하는 네트워크 인증·접근 제어 기능이 아니다. 틀린 표현인 '디렉터리 리스팅'은 '포트 기반 네트워크 접근 제어'로 고쳐야 한다.
② O — 802.1X는 인증 서버와 연계하여 사용자별 인증 결과와 정책에 따라 네트워크 접근 권한을 중앙에서 관리할 수 있게 한다.
③ O — EAP는 하나의 고정된 인증 방식이 아니라 여러 EAP 인증 방식을 수용하는 프레임워크이므로 인증서, 스마트카드 등 다양한 인증 수단을 지원할 수 있다.
④ O — 키 생성 기능이 있는 EAP 인증 방식은 인증 과정에서 세션별 키 자료를 만들고, 이를 무선 구간 등의 암호화 키 설정에 활용할 수 있게 한다.
⑤ O — 802.1X/EAP의 핵심 목적은 네트워크 접속을 요청한 사용자나 단말을 인증한 뒤 접근 허용 여부를 결정하는 것이다.

NoteBase

오답 포인트

③의 다양한 인증 수단과 ④의 세션 키 지원처럼 EAP 방식이 제공하는 기능까지 802.1X/EAP 체계의 기능으로 본다는 점이 함정이다. 반면 ①의 디렉터리 리스팅은 '디렉터리'라는 정보 시스템 용어가 들어갈 뿐 접속 인증과 무관하다.

다시 나오면 이렇게 판단

선지가 인증, 접근 권한, 인증 서버, EAP 인증 방식, 세션 키와 관련되면 802.1X/EAP의 범위로 판단한다. 파일 목록 표시처럼 네트워크 접속 통제와 관계없는 기능이면 범위 밖으로 판단한다.

암기 포인트

802.1X는 접속 통제, EAP는 다양한 인증 방식, 디렉터리 리스팅은 무관이다.

NoteBase

18. 윈도우에서 제공하는 기본 프로세스 중 다음 설명에 해당하는 것은?

> 이 서비스는 DLL이 실행하는 프로세스에 대한 기본 프로세스로, 하나의 시스템상에서 동시에 여러 개가 수행될 수 있으며 백그라운드 서비스를 처리할 수 있다.

① winlogon.exe
② smss.exe
③ svchost.exe
④ spoolsv.exe
⑤ explorer.exe

정답 3번

출제 포인트

Windows 기본 프로세스의 역할을 구분하고, DLL 형태로 구현된 백그라운드 서비스를 호스팅하는 프로세스를 찾는 문제이다.

핵심 개념

svchost.exe는 DLL 형태로 구현된 Windows 서비스를 메모리에 불러와 실행하는 범용 서비스 호스트 프로세스이다. 여러 서비스 그룹을 나누어 담당하므로 한 시스템에서 여러 svchost.exe 인스턴스가 동시에 실행될 수 있다.
winlogon.exe는 대화형 로그온·로그오프를 관리하고, smss.exe는 시스템 초기화 단계에서 세션을 구성한다. spoolsv.exe는 인쇄 작업을 관리하며, explorer.exe는 바탕 화면·작업 표시줄·파일 탐색기 등의 사용자 셸을 제공한다.

NoteBase

선지별 해설

① X — winlogon.exe는 사용자의 대화형 로그온과 로그오프를 관리하는 프로세스이므로 DLL 기반 백그라운드 서비스의 범용 호스트가 아니다. 제시문에 맞게 고치면 winlogon.exe가 아니라 svchost.exe이다.
② X — smss.exe는 부팅 초기에 시스템 세션을 만들고 주요 사용자 모드 프로세스의 시작을 준비하는 세션 관리자이다. 제시문에 맞게 고치면 smss.exe가 아니라 svchost.exe이다.
③ O — svchost.exe는 DLL 기반 Windows 서비스를 호스팅하여 백그라운드에서 실행하며, 서비스 그룹별로 여러 인스턴스가 동시에 동작할 수 있다.
④ X — spoolsv.exe는 인쇄 작업을 대기열에 저장하고 프린터로 전달하는 인쇄 스풀러 서비스 프로세스이다. 제시문에 맞게 고치면 spoolsv.exe가 아니라 svchost.exe이다.
⑤ X — explorer.exe는 바탕 화면, 작업 표시줄, 시작 메뉴와 파일 탐색 기능을 제공하는 Windows 사용자 셸 프로세스이다. 제시문에 맞게 고치면 explorer.exe가 아니라 svchost.exe이다.

오답 포인트

보기의 프로세스가 모두 Windows에서 흔히 관찰되는 기본 프로세스라서 이름만으로는 혼동하기 쉽다.
제시문의 결정적 표현은 ‘DLL 기반 서비스의 호스트’, ‘백그라운드 서비스 처리’, ‘여러 개가 동시에 수행’이며, 이 세 특징을 함께 만족하는 것은 svchost.exe이다.

다시 나오면 이렇게 판단

Windows 프로세스 문제에서는 역할 키워드를 먼저 대응한다. DLL 서비스·복수 인스턴스는 svchost, 로그온은 winlogon, 세션 초기화는 smss, 인쇄 대기열은 spoolsv, 사용자 셸은 explorer로 구분한다.

암기 포인트

svchost는 Service Host이다. DLL 서비스들을 품고 여러 개가 동시에 실행된다.

NoteBase

19. 다음 SQL 쿼리문에 대한 설명으로 옳지 않은 것은?

```
SELECT * FROM user WHERE name = '' or ''='';
```

① SQL 인젝션 공격에 취약한 문장이다.
② WHERE절에서 user의 모든 레코드를 반환받을 가능성이 있다.
③ 위 SQL 쿼리문의 취약점 해결 방법으로 prepared statements를 사용하는 것이 좋다.
④ 입력값 검증을 위하여 블랙리스트 방식으로 유효한 값만 허용하는 것이 좋다.
⑤ JPA, Hibernate 등 ORM으로 데이터를 추상화하는 것이 좋다.

정답 4번

출제 포인트

SQL 인젝션이 WHERE 조건을 항상 참으로 만드는 원리와 안전한 입력 검증·쿼리 실행 방법을 구별하는 문제이다.

핵심 개념

SQL 인젝션은 입력값이 SQL 명령의 일부로 해석되어 공격자가 쿼리의 구조나 조건을 바꾸는 공격이다. 제시된 조건식에서는 ''=''가 항상 참이므로 OR로 연결된 WHERE 조건 전체가 참이 될 수 있다.
prepared statement는 SQL 구조와 입력 데이터를 분리해 입력값을 명령이 아닌 매개변수 값으로 처리한다.
화이트리스트는 미리 정한 유효한 값·형식만 허용하고, 블랙리스트는 알려진 위험 문자나 패턴만 차단한다.

선지별 해설

① O — WHERE 조건에 OR로 연결된 ''=''가 항상 참이므로 공격자가 조건을 우회할 수 있는 SQL 인젝션 취약 문장이다.
② O — OR 뒤의 조건이 참이어서 WHERE 조건 전체가 참이 될 수 있으므로 user 테이블의 모든 레코드가 반환될 가능성이 있다.
③ O — prepared statement를 사용하면 SQL 문장 구조와 외부 입력값이 분리되고 입력값이 매개변수로 바인딩되므로 SQL 인젝션 방어에 효과적이다.
④ X — 틀린 표현은 '블랙리스트 방식으로 유효한 값만 허용'이다. 유효한 값만 허용하는 방식은 화이트리스트이며, 블랙리스트는 알려진 위험 값이나 패턴을 거부하는 방식이어서 우회 가능성이 있다.
올바르게는 입력값의 형식과 허용 범위를 화이트리스트 방식으로 검증하는 것이 좋다.
⑤ O — JPA, Hibernate 같은 ORM을 사용해 매개변수 바인딩 중심으로 데이터를 처리하면 문자열 결합으로 SQL을 직접 만드는 일을 줄일 수 있어 SQL 인젝션 위험을 낮추는 데 도움이 된다. 다만 ORM에서도 입력값을 쿼리 문자열에 직접 이어 붙이면 안전하지 않다.

NoteBase

오답 포인트

④는 '위험한 것을 막는다'는 블랙리스트와 '유효한 것만 허용한다'는 화이트리스트를 바꾸어 놓았다. 또한 ORM을 사용하기만 하면 자동으로 안전하다고 단정해서는 안 되지만, ⑤는 데이터 추상화와 매개변수 바인딩을 활용하는 방향이 좋다는 설명이므로 옳다.

다시 나오면 이렇게 판단

OR 뒤에 항상 참인 비교식이 있는지 먼저 확인한다. 방어 방법은 SQL과 입력값을 분리하는 prepared statement, 허용 형식만 통과시키는 화이트리스트, 안전한 매개변수 바인딩인지로 판단한다.

암기 포인트

항상 참인 OR 조건은 인증·조건 우회, 유효한 값만 허용하는 것은 화이트리스트이다.

NoteBase

20. RSA 암호에서 암호문이 C=2, 공개키가 (e=3, n=33)일 때, 평문 M은?

① 8
② 10
③ 17
④ 19
⑤ 29

정답 5번

출제 포인트

RSA에서 공개키로부터 오일러 피 함수와 개인키 지수 d를 구한 뒤, 암호문을 복호화하여 평문을 계산하는 문제이다.

조건 정리

주어진 값: 암호문 $C = 2$, 공개 지수 $e = 3$, 법 $n = 33$이다.
구해야 할 값: C ≡ M^e ±od n을 만족하는 평문 M이다.
주의할 조건: $n = 33 = 3 \times 11$로 소인수분해한 뒤 $\varphi(n)$과 개인키 지수 d를 구해야 한다.

사용할 공식

$\varphi(n) = (p-1)(q-1)$
ed≡1±od(n)
M≡ C^d±od n

RSA 복호화에서는 공개 지수 e의 $\varphi(n)$에 대한 곱셈 역원인 d를 구하고, 암호문 C를 d제곱하여 평문을 복원하므로 이 공식을 사용한다.

계산 과정

1. $n = 33 = 3 \times 11$이므로 $p = 3, q = 11$이다.
2. $\varphi(33) = (3-1)(11-1) = 20$이다.
3. 3d≡1±od20을 만족하는 값은 $d = 7$이다. 실제로 3×7=21≡1±od20이다.
4. 복호화하면 M≡2^7=128≡29±od33이다.
5. 검산하면 29^3≡2±od33이므로 주어진 암호문과 일치한다.

NoteBase

선지 판단

① X — 선지의 8은 틀리다. 8^3≡17±od33이므로 암호문 2를 만들지 못한다. 올바른 평문은 29이다.
② X — 선지의 10은 틀리다. 10^3≡10±od33이므로 암호문 2를 만들지 못한다. 올바른 평문은 29이다.
③ X — 선지의 17은 틀리다. 17^3≡29±od33이므로 암호문 2를 만들지 못한다. 올바른 평문은 29이다.
④ X — 선지의 19는 틀리다. 19^3≡28±od33이므로 암호문 2를 만들지 못한다. 올바른 평문은 29이다.
⑤ O — 29^3≡2±od33이므로 평문 29를 공개키로 암호화하면 주어진 암호문 2가 된다. 따라서 계산 결과와 일치한다.

오답 포인트

암호문에 공개 지수 $e = 3$을 다시 적용하는 것이 아니라, e의 모듈러 역원인 개인키 지수 $d = 7$을 먼저 구해 C^d n을 계산해야 한다. 또한 $\varphi(33)$을 32로 보는 것이 아니라, $33 = 3 \times 11$에서 $(3-1)(11-1) = 20$으로 계산해야 한다.

다시 나오면 이렇게 판단

RSA 복호화 문제는 n 소인수분해 → $\varphi(n)$ 계산 → ed≡1±od(n)에서 d 결정 → M≡ C^d±od n 계산 → M^e n 검산의 순서로 판단한다.

암기 포인트

RSA는 공개키로 C≡ M^e±od n, 개인키로 M≡ C^d±od n이며, ed≡1±od(n)이다.

NoteBase