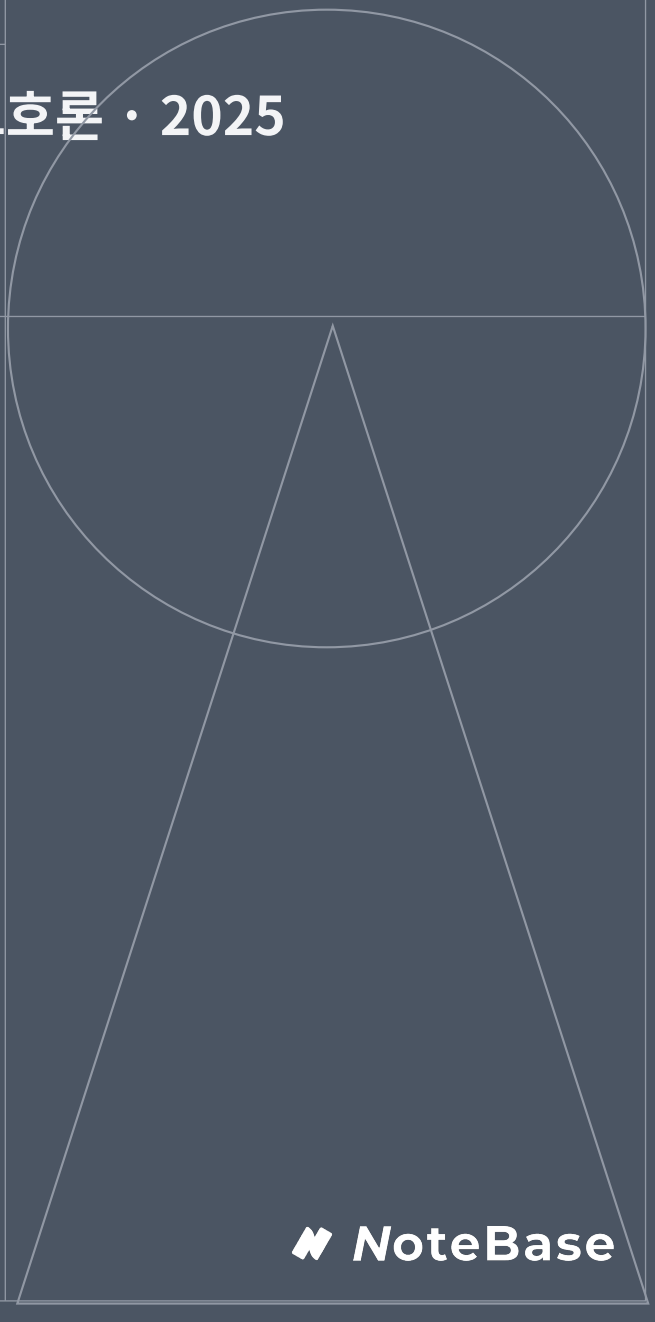
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2025



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2025

공무원/지방직/9급 · 정보보호론 · 2025

문 1. 정보보호에 대한 설명으로 옳지 않은 것은?

① 정보자산을 여러 가지 위협으로부터 보호하는 것이다.

② 정보보호의 범위에는 사이버안전이 포함될 수 없다.

③ 정보의 가용성과 보안 측면에서 정보보호는 정보의 활용과 정보의 통제 사이에서 균형 감각을 갖는 행위이다.

④ 정보보호의 대상이 되는 자산에는 소프트웨어, 하드웨어, 데이터, 인적자원이 포함될 수 있다.

정답 2번

간단한 해설

사이버안전은 해킹·악성코드 등 사이버공간의 위협으로부터 정보와 정보시스템을 보호하는 활동이므로 **정보보호의 범위에 포함될 수 있다**. 이를 정보보호에서 배제한 표현이 잘못되었다.

선지별 해설

① O: 정보보호는 정보자산을 유출·변조·파괴·서비스 중단 등의 위협으로부터 보호하는 활동이다. 허가받지 않은 정보 공개를 막는 기밀성, 정보가 무단으로 변경되지 않도록 하는 무결성, 필요한 때 정보를 이용할 수 있게 하는 가용성을 확보한다.

② X: 사이버안전은 사이버공간에서 해킹·악성코드 등의 위협으로부터 정보와 정보시스템을 보호하는 활동이다. 이 활동도 정보자산을 보호하므로 **정보보호의 범위에 포함될 수 있다**. 선지의 '포함될 수 없다'는 '포함될 수 있다'로 고쳐야 한다.

③ O: 정보보호는 무단 접근을 통제하면서도 **권한 있는 이용자가 필요한 때 정보를 활용**할 수 있도록 해야 한다. 예를 들어 모든 접근을 차단하면 정보 유출은 줄일 수 있어도 정상적인 업무까지 불가능해져 가용성을 해친다. 따라서 정보의 활용과 통제 사이에서 균형을 유지해야 한다.

④ O: 정보보호 대상은 **데이터 자체에 한정되지 않는다**. 데이터를 저장·처리하는 하드웨어와 소프트웨어, 관련 지식과 업무를 담당하는 인적자원도 정보의 안전한 관리와 이용에 영향을 미치므로 보호 대상 자산에 포함될 수 있다.

NoteBase

문 2. 포트 스캔에 대한 설명으로 옳지 않은 것은?

① 분석 대상 시스템에 어떤 서비스가 제공되고 있는지 확인하기 위한 정보수집 방법이다.

② 포트 번호는 0~65,535까지이며, 이 중 0~1,023은 잘 알려진 포트(well-known port)라고 한다.

③ Nmap은 오픈소스 기반 포트 스캔 도구이다.

④ TCP 포트 스캔 시 닫혀 있는 포트로부터 ICMP port Unreachable 패킷이 수신된다.

정답 4번

간단한 해설

TCP SYN 스캔에서 닫힌 포트는 **TCP RST 패킷**으로 응답한다. ICMP Port Unreachable은 **UDP 스캔에서 닫힌 포트**를 판단하는 응답이다.

선지별 해설

① O: 포트 스캔은 대상 시스템의 포트에 탐지 패킷을 보내고 응답을 분석하여 **포트의 개방 여부**를 확인하는 정보수집 방법이다. 열린 포트에서는 서비스가 요청을 기다리고 있으므로, 이를 통해 제공 중인 서비스에 관한 정보를 얻을 수 있다.

② O: TCP와 UDP의 포트 번호는 16비트로 표현하므로 범위는 0~65,535이다. 이 중 **0~1,023**은 잘 알려진 포트(well-known port) 범위로, 주요 서비스의 표준 포트 번호가 배정된다.

③ O: Nmap은 **오픈소스 네트워크 탐색·보안 점검 도구**로, TCP와 UDP 포트 스캔을 지원한다. 포트별 응답을 분석하여 열림·닫힘 등의 상태를 확인할 수 있다.

④ X: 방화벽 등에 의해 차단되지 않은 TCP SYN 스캔에서, 닫힌 포트는 연결을 수락할 서비스가 없으므로 **TCP RST 패킷**으로 응답한다. 열린 포트는 SYN/ACK 패킷으로 응답한다. 반면 UDP 스캔에서는 ICMP Port Unreachable 메시지를 수신하면 해당 포트를 닫힌 상태로 판단한다. 선지는 UDP의 닫힌 포트 판별 응답을 TCP에 적용한 것이다.

NoteBase

문 3. (가), (나)에 해당하는 정보보호 서비스를 바르게 연결한 것은?

메일 내용에 암호를 적용함으로써 (가)을 제공할 수 있고, 메일에 전자서명을 적용함으로써 (나)을/를 제공할 수 있다.

① (가): 기밀성, (나): 가용성
② (가): 기밀성, (나): 부인방지
③ (가): 가용성, (나): 기밀성
④ (가): 가용성, (나): 인증

정답 2번

간단한 해설

메일 내용의 암호화는 허가받지 않은 사람이 내용을 읽지 못하게 하는 **기밀성**을 제공한다. 전자서명은 서명자가 나중에 자신의 서명 사실을 부인하는 것을 막는 **부인방지**를 제공할 수 있다.

빈칸별 해설

(가) 기밀성: 메일 내용을 암호화하면 복호화에 필요한 키를 가진 수신자는 원문을 읽을 수 있지만, 권한 없는 사람은 암호문을 얻더라도 내용을 알기 어렵다. 이처럼 **허가받지 않은 정보 열람을 막는** 서비스가 기밀성이다. 가용성은 정당한 사용자가 필요할 때 정보나 서비스를 이용할 수 있게 하는 성질이므로, 내용의 암호화와는 구별된다.

(나) 부인방지: 전자서명은 송신자의 개인키로 생성하고 그에 대응하는 공개키로 검증한다. 개인키가 안전하게 관리된다는 전제에서 서명은 송신자가 해당 메일에 서명했다는 증거가 되어, 나중에 **자신의 서명 사실을 부인하는 것을 방지**할 수 있다. 전자서명은 송신자 인증과 메일의 무결성 확인에도 쓰이지만, 서명 자체가 메일 내용을 암호화하여 숨기는 것은 아니다.

따라서 (가)는 기밀성, (나)는 부인방지이며, 이는 ②의 조합과 일치한다.

NoteBase

문 4. (가)에 들어갈 용어는?

○ (가)은/는 1989년에 처음 등장한 것으로 알려져 있고 이후 2006년경에 GPCode라는 (가)이/가 등장하였다.
○ 최근의 (가)은/는 공격자의 개인키를 모르면 사실상 풀 수 없는 암호 알고리즘을 사용한다.

① 웜
② 바이러스
③ 랜섬웨어
④ DDoS

정답 3번

간단한 해설

파일을 **암호화해 사용할 수 없게 만든 뒤 복구 대가로 금전을 요구**하는 악성코드가 랜섬웨어이다. 공격자가 복호화에 필요한 개인키를 보유하면 피해자는 그 키 없이 암호화된 파일을 복구하기 어렵다.

핵심 풀이

랜섬웨어는 파일을 암호화하거나 시스템 사용을 막고, 이를 풀어 주는 대가로 금전을 요구하는 악성코드이다. 지문의 1989년은 최초로 알려진 랜섬웨어인 AIDS 트로이목마와 연결된다. 2006년경 활동한 GPCode도 파일을 암호화하고 복구 대가로 금전을 요구한 사례이므로, (가)는 랜섬웨어이다.

'공격자의 개인키를 모르면 사실상 풀 수 없다'는 표현은 **공개키 암호를 이용한 복구 통제**를 가리킨다. 공개키 암호에서는 암호화에 쓰는 공개키와 복호화에 쓰는 개인키가 다르다. 충분히 강한 알고리즘과 키를 올바르게 사용하면 공개키를 알아도 개인키를 구하기가 현실적으로 어렵다. 공격자는 개인키를 자신만 보유함으로써 피해자가 파일을 스스로 복호화하기 어렵게 만든다.

웜과 바이러스는 주로 **복제·전파 방식**으로 구분한다. 웜은 독립적으로 실행되며 스스로 전파되고, 바이러스는 다른 프로그램이나 파일 등에 붙어 실행될 때 복제된다. 이 분류만으로는 지문의 암호화와 금전 요구 특성을 설명할 수 없다. DDoS는 여러 시스템에서 트래픽이나 요청을 집중시켜 서비스를 이용하지 못하게 하는 공격으로, 파일을 암호화해 복구를 통제하는 방식과 구별된다.

NoteBase

문 5. (가), (나)에 해당하는 악성코드를 바르게 연결한 것은?

(가) DDoS 공격 시 지정된 공격을 수행하도록 하는 악성코드
(나) 사용자의 동의 없이 설치되어 사용자 또는 컴퓨터의 정보를 수집하여 전송하는 악성코드

① (가): 봇, (나): 스파이웨어
② (가): 봇, (나): 애드웨어
③ (가): 루트킷, (나): 스파이웨어
④ (가): 루트킷, (나): 애드웨어

정답 1번

간단한 해설

공격자의 명령에 따라 DDoS 공격을 수행하는 악성코드는 **봇**이다. 사용자 동의 없이 정보를 수집하여 외부로 전송하는 것은 **스파이웨어**의 특징이다.

대응 관계 해설

(가) 봇: 감염된 컴퓨터에서 공격자의 명령을 받아 지정된 작업을 수행하는 악성코드이다. 여러 감염 컴퓨터의 봇이 특정 서버에 동시에 대량의 트래픽을 보내면 DDoS 공격에 이용될 수 있다. 핵심은 **공격자의 명령에 따른 공격 수행**이며, 침입 흔적이나 악성 프로그램의 존재를 숨기는 데 쓰이는 루트킷과 구별된다.

(나) 스파이웨어: 사용자 동의 없이 설치되어 사용자나 컴퓨터의 정보를 수집하고 외부로 전송하는 악성코드이다. 핵심은 **동의 없는 정보 수집·전송**이며, 광고 표시가 주된 특징인 애드웨어와 구별된다.

(가)는 봇, (나)는 스파이웨어에 대응하므로 ①의 연결과 일치한다.

NoteBase

문 6. VPN에서 사용하는 프로토콜이 아닌 것은?

① IGMP

② IPSec

③ L2TP

④ PPTP

정답 1번

간단한 해설

IGMP는 **IPv4 멀티캐스트 그룹의 가입 정보를 관리**하는 프로토콜이다. VPN의 터널을 구성하거나 전송 데이터를 보호하기 위한 프로토콜과 구별한다.

선지별 해설

① X: IGMP(Internet Group Management Protocol)는 호스트가 어떤 IPv4 멀티캐스트 그룹에 속하는지를 인접 멀티캐스트 라우터에 알리는 프로토콜이다. 여러 수신자에게 데이터를 전달하기 위한 **그룹 가입 정보 관리**가 목적이며, VPN 터널을 구성하거나 통신 내용을 암호화하는 프로토콜은 아니다.

② O: IPSec은 IP 계층에서 통신을 보호하는 보안 프로토콜 체계로, VPN 구축에 사용된다. 인증과 무결성 검증으로 송신 출처와 데이터 변조 여부를 확인하고, 암호화로 기밀성을 제공할 수 있다. 특히 **터널 모드**에서는 원래 IP 패킷을 새로운 IP 패킷 안에 넣어 전송하므로 사설망 사이의 통신을 보호하는 데 활용된다.

③ O: L2TP(Layer Two Tunneling Protocol)는 PPP 프레임을 다른 네트워크를 통해 전달하는 터널링 프로토콜로, VPN 구성에 사용된다. 터널링은 전달할 데이터를 다른 프로토콜의 데이터 안에 넣어 운반하는 방식이다. L2TP는 **자체적으로 데이터 암호화를 제공하지 않으므로**, 암호화 등 보안 기능이 필요하면 IPSec과 결합하여 사용한다.

④ O: PPTP(Point-to-Point Tunneling Protocol)는 PPP 트래픽을 IP 네트워크를 통해 운반하여 VPN을 구성하는 터널링 프로토콜이다. **GRE 기반의 캡슐화**로 PPP 패킷을 전달한다. IGMP의 멀티캐스트 그룹 관리와 달리, 떨어진 지점 사이에 논리적인 통신 경로를 구성하는 데 사용된다.

NoteBase

문 7. (가)에 들어갈 용어는?

윈도우 운영체제에서 SAM이 사용자의 로그인 입력 정보(사용자 계정과 패스워드)와 SAM 데이터베이스 정보의 일치 여부를 확인하여 SRM에게 알리면 인증된 사용자에게 고유한 (가)가 부여된다. 또 SRM은 (가)를 기반으로 파일이나 디렉토리에 접근을 허용할지 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① GID

② SID

③ SetUID

④ SSID

정답 2번

간단한 해설

윈도우는 **SID(보안 식별자)**로 사용자 계정을 구별하고, 이를 접근 권한 검사에 사용한다. 로그인할 때 접근 토큰에 포함된 SID가 파일·디렉토리의 접근 제어 정보와 대조된다.

빈칸별 해설

(가) SID(Security Identifier, 보안 식별자): 윈도우에서 사용자·그룹 등 보안 주체를 구별하는 고유한 값이다. 사용자 계정의 SID는 계정 생성 시 부여되어 보안 데이터베이스에 저장되며, 로그인에 성공하면 해당 사용자의 접근 토큰에 포함된다. 지문에서 사용자 식별과 접근 권한 판단에 공통으로 사용되는 값이 SID이다.

SRM(보안 참조 모니터)은 접근 토큰의 사용자·그룹 SID와 파일·디렉토리의 접근 제어 목록에 지정된 권한을 대조하여 요청한 접근을 허용할지 판단한다. 계정과 패스워드로 본인 여부를 확인하는 인증을 거친 뒤, **SID를 이용해 해당 자원에 대한 권한을 검사**하는 것이다.

따라서 (가)에 들어갈 용어는 SID이며, ②와 대응한다.

NoteBase

문 8. 위험 처리 방법에 대한 설명으로 옳은 것은?

① 위험 수용: 위험에 처한 자산의 구조나 사용을 변경한다.

② 위험 감소: 위험을 발생시키는 행위나 시스템을 수행하지 않는다.

③ 위험 전가: 위험에 대응하여 보험을 들거나 다른 기관과 계약을 맺는다.

④ 위험 회피: 현재의 위험을 받아들이고 잠재적 손실 비용을 감수한다.

정답 3번

간단한 해설

보험 가입이나 다른 기관과의 계약을 통해 위험으로 인한 **손실 부담을 제3자에게 이전**하는 것이 위험 전가이다. 위험 자체가 사라지는 것은 아니며, 약정된 범위의 손실이나 책임을 다른 주체가 부담한다.

선지별 해설

① X: 위험 수용은 위험의 존재를 인정하고 **잠재적 손실을 감수**하는 방법이다. 위험을 처리하기 위해 자산의 구조나 사용을 변경하는 것은 위험을 그대로 받아들이는 수용과 구별된다.

② X: 위험을 발생시키는 행위나 시스템을 아예 수행하지 않는 것은 **위험 회피**이다. 위험 감소는 해당 활동을 계속하되 보안 통제 등을 적용하여 사고의 발생 가능성이나 피해 규모를 낮추는 방법이다.

③ O: 위험 전가는 보험이나 계약을 이용하여 **손실 부담의 전부 또는 일부를 다른 주체로 이전**하는 방법이다. 예를 들어 보험에 가입하면 사고가 발생했을 때 약정된 범위에서 보험자가 손실을 보상한다. 따라서 보험 가입이나 다른 기관과의 계약은 위험 전가의 수단이 된다.

④ X: 현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것은 **위험 수용**이다. 위험 회피는 위험을 유발하는 활동을 시작하지 않거나 중단하여 그 활동에서 발생하는 위험에 노출되지 않도록 하는 방법이다.

NoteBase

문 9. 공개키 암호 알고리즘이 아닌 것은?

① RSA

② 타원곡선암호

③ 배낭암호

④ A5/1

정답 4번

간단한 해설

A5/1은 송신자와 수신자가 같은 비밀키를 공유하는 **대칭키 스트림 암호**이다. 공개키와 개인키를 한 쌍으로 사용하는 공개키 암호와 구별된다.

선지별 해설

공개키 암호는 공개해도 되는 공개키와 비밀로 보관하는 개인키를 구분한다. 암호화할 때는 수신자의 공개키를 사용하고, 복호화할 때는 그에 대응하는 개인키를 사용한다. 아래 O/X는 각 알고리즘이 공개키 암호에 해당하는지를 나타낸다.

① O: RSA는 **큰 정수의 소인수분해가 어렵다는 성질**을 이용하는 공개키 암호이다. 두 큰 소수의 곱을 공개하더라도 그 소수들을 알아내기 어렵게 하여, 공개키로부터 개인키를 구하는 것을 어렵게 만든다.

② O: 타원곡선암호는 **타원곡선 위의 이산로그 문제**에 기반한 공개키 암호이다. 개인키에 해당하는 수만큼 기준점에 대한 점 덧셈을 반복하여 공개키를 만들며, 기준점과 공개키를 알아도 그 수를 역으로 구하기 어렵다는 성질을 이용한다.

③ O: 배낭암호는 **부분집합 합 문제**를 이용한 공개키 암호이다. 이는 주어진 수들 가운데 어떤 것들을 골라 더해야 목표 합이 되는지를 찾는 문제이다. 대표적인 메르클–헬먼 배낭암호는 쉽게 풀 수 있는 배낭 구조를 개인키로 숨기고, 이를 변환한 수열을 공개키로 사용한다.

④ X: A5/1은 GSM 이동통신의 무선 구간 암호화에 사용된 **대칭키 스트림 암호**이다. 송신자와 수신자가 공유한 비밀키로 같은 키스트림을 생성하고, 이를 데이터와 비트 단위 XOR하여 암호화하거나 복호화한다. 따라서 공개키 암호가 아니라 대칭키 암호로 분류해야 한다.

NoteBase

문 10. 다음에서 설명하는 보안 솔루션은?

◯ 조직 내 중요한 자료가 외부로 유출되는 것을 막는다.
◯ 사용자의 다양한 데이터 전송 수단인 USB 메모리 등과 같은 이동식 저장 매체, 이메일과 같은 네트워크 등을 제어한다.

① DRM
② DLP
③ IPS
④ SIEM

정답 2번

간단한 해설

USB 메모리나 이메일 같은 전송 경로를 제어하여 **중요 자료의 외부 유출을 방지**하는 것은 DLP의 기능이다. 문서 이용 권한을 관리하는 DRM과 달리, 자료가 조직 밖으로 빠져나가는 행위를 통제하는 데 초점이 있다.

핵심 풀이

DLP(Data Loss Prevention)는 조직의 중요 정보가 외부로 유출되지 않도록 감시하고 통제하는 솔루션이다. 지문의 '외부로 유출되는 것을 막는다'와 '이동식 저장 매체, 이메일 등을 제어한다'는 **자료의 반출 경로를 통제**한다는 뜻이다. 예를 들어 보안 정책에 따라 중요 파일의 USB 복사나 외부 이메일 첨부 전송을 차단하는 방식이 이에 해당한다.

DRM(Digital Rights Management)은 암호화와 권한 관리를 통해 **문서·콘텐츠의 열람·복사·인쇄 등 이용을 통제**한다. 중요 자료를 보호한다는 목적은 비슷하지만, 이 문항은 문서의 이용 권한보다 USB와 이메일을 통한 외부 반출 통제를 강조하므로 DLP에 해당한다.

IPS는 네트워크의 침입·공격을 탐지하고 차단하며,

SIEM은 여러 시스템의 로그와 보안 이벤트를 수집·연계 분석한다. 이들은 각각 공격 차단과 보안 이벤트 분석에 초점이 있어, 지문이 설명하는 자료 유출 경로 통제와 구별된다.

NoteBase

문 11. 다음 문제가 모두 해결된 블록암호 운용 모드는?

◯ 평문 블록이 동일하면 암호문 블록이 같아지는 문제
◯ 암호문 블록에 오류가 발생하면 다음 블록의 복호화에 오류가 전파되는 문제

① ECB(Electronic CodeBook)
② OFB(Output FeedBack)
③ CFB(Cipher FeedBack)
④ CBC(Cipher Block Chaining)

정답 2번

간단한 해설

OFB는 평문과 별도로 생성한 키스트림을 결합하므로 같은 평문이 반복되어도 암호문이 반드시 같아지지는 않는다. 또한 **암호문이 아닌 암호기의 출력값을 되먹임**하므로 암호문 비트 오류가 이후 블록으로 전파되지 않는다.

핵심 풀이

동일 평문 문제: OFB는 초기화 벡터(IV)를 암호화한 출력값을 다시 암호기에 입력하여 키스트림을 만들고, 이를 평문과 XOR하여 암호문을 얻는다. 평문 블록을 각각 독립적으로 암호화하는 ECB와 달리 **암호문은 평문과 키스트림에 함께 의존**하므로 같은 평문 블록이 반복되어도 암호문이 반드시 같아지지는 않는다. 같은 키로 여러 메시지를 암호화할 때는 IV를 재사용하지 않아야 한다.

오류 전파 문제: OFB가 다음 키스트림을 만드는 데 사용하는 것은 **암호문이 아니라 암호기의 출력값**이다. 따라서 전송 중 암호문의 한 비트가 뒤집혀도 복원된 평문의 같은 위치 비트만 바뀌고 이후 블록에는 오류가 전파되지 않는다. 반면 CBC와 CFB는 암호문을 다음 복호화에 사용하므로 암호문 오류가 후속 블록 또는 구간에 영향을 준다. 두 조건을 함께 만족하는 모드는 OFB이다.

NoteBase

문 12. 다음에서 설명하는 블루투스 취약점 공격은?

블루투스 장비 간의 취약한 연결 관리를 악용한 공격으로, 공격 장치와 공격 대상 장치를 연결하여 공격 대상 장치에서 임의의 동작을 실행한다. 블루투스 기기가 한 번 연결된 이후에는 다시 연결하지 않아도 자동으로 연결되는 인증 취약점을 이용한 공격이다.

① 블루버그(bluebug)
② 블루재킹(bluejacking)
③ 블루프린팅(blueprinting)
④ 블루스나프(bluesnarf)

정답 1번

간단한 해설

취약한 인증·연결 관리를 악용해 **대상 장치에서 임의의 동작을 실행**하는 것은 블루버그의 특징이다. 단순히 메시지를 보내거나 정보를 읽는 수준을 넘어 장치의 기능을 무단으로 제어한다.

개념 구분

블루버그(bluebug): 블루투스의 보안 취약점을 악용해 대상 장치에 접근하고 명령이나 기능을 무단으로 실행하는 공격이다. 지문에서는 취약한 인증·연결 관리를 이용해 **대상 장치에서 임의의 동작을 실행**하므로 블루버그에 해당한다. 한 번 연결된 뒤 자동으로 연결된다는 설명은 이 문항에서 악용되는 연결 관리상의 취약점을 나타낸다.

블루재킹(bluejacking): 블루투스를 통해 상대방이 원하지 않는 메시지를 보내는 행위이다. **메시지 전송**이 중심이며, 그 자체가 대상 장치의 명령을 무단으로 실행한다는 뜻은 아니다.

블루프린팅(blueprinting): 블루투스 장치가 드러내는 주소나 서비스 정보 등의 특성을 분석하여 **제조사·모델 등 장치의 특성을 식별**하는 기법이다. 장치를 식별하는 것과 장치의 동작을 제어하는 것은 구별된다.

블루스나프(bluesnarf): 블루투스 취약점을 악용해 대상 장치에 저장된 정보를 무단으로 가져오는 공격이다. **정보 탈취**가 중심이라는 점에서, 지문의 임의 동작 실행을 특징으로 하는 블루버그와 구별된다.

NoteBase

문 13. 유럽의 GDPR(General Data Protection Regulation)에 따른 정보주체의 권리가 아닌 것은?

① 개인정보의 처리에 대한 차단/제한을 요구할 권리
② 개인정보를 본인 또는 다른 사업자에게 전송하도록 요구할 권리
③ 개인정보의 삭제를 요구할 권리
④ 프로파일링 등 자동으로 이루어지는 모든 의사결정에 대해 거부할 권리

정답 4번

①

정보주체는 개인정보의 정확성을 다투는 경우 등 법정 요건에 해당하면 **자신의 개인정보 처리를 제한하도록 요구할 권리**를 가진다.

유럽연합 일반 개인정보보호법(GDPR) 제18조 제1항
제18조(처리 제한을 요구할 권리)
제1항 정보주체는 다음 중 어느 하나에 해당하는 경우 개인정보처리자에게 처리 제한을 요구할 권리를 가진다.
(a) 정보주체가 개인정보의 정확성에 이의를 제기한 경우: 처리자가 그 정확성을 확인하는 데 필요한 기간 동안
(b) 처리가 위법하지만 정보주체가 개인정보의 삭제에 반대하고 대신 그 이용의 제한을 요구하는 경우
(c) 처리자가 처리 목적상 개인정보를 더 이상 필요로 하지 않지만, 정보주체가 법적 청구권의 확립·행사 또는 방어를 위해 그 정보를 필요로 하는 경우
(d) 정보주체가 제21조 제1항에 따라 처리에 이의를 제기한 경우: 처리자의 정당한 근거가 정보주체의 근거보다 우선하는지를 확인할 때까지

NoteBase

②

개인정보 이동권은 **동의 또는 계약에 근거하여 자동화된 수단으로 처리되는, 정보주체가 제공한 자신의 개인정보**를 기계 판독 가능한 형식으로 받을 권리이다. **기술적으로 가능하면 다른 개인정보처리자에게 직접 전송하도록 요구**할 수도 있다.

유럽연합 일반 개인정보보호법(GDPR) 제20조 제1항, 유럽연합 일반 개인정보보호법(GDPR) 제20조 제2항
제20조(개인정보 이동권)
제1항 정보주체는 다음의 두 요건이 모두 충족되는 경우, 자신이 개인정보처리자에게 제공한 본인에 관한 개인정보를 체계적이고 통상적으로 사용되며 기계로 읽을 수 있는 형식으로 받을 권리와, 그 정보를 제공받은 처리자의 방해 없이 다른 처리자에게 전송할 권리를 가진다.
(a) 처리가 제6조 제1항 (a)호 또는 제9조 제2항 (a)호에 따른 동의나 제6조 제1항 (b)호에 따른 계약에 근거할 것
(b) 처리가 자동화된 수단으로 이루어질 것

제2항 제1항에 따른 개인정보 이동권을 행사할 때, 정보주체는 기술적으로 가능한 경우 한 개인정보처리자로부터 다른 개인정보처리자에게 개인정보를 직접 전송하도록 할 권리를 가진다.

NoteBase

③

정보주체는 수집 목적상 더 이상 필요하지 않거나 위법하게 처리된 경우 등에는 **자신의 개인정보 삭제를 요구할 권리**를 가진다. 다만 법적 보관 의무 이행 등에 필요한 경우에는 삭제 의무의 예외가 인정된다.

유럽연합 일반 개인정보보호법(GDPR) 제17조 제1항, 유럽연합 일반 개인정보보호법(GDPR) 제17조 제3항
제17조(삭제권: 잊힐 권리)
제1항 다음 중 어느 하나의 사유가 있는 경우, 정보주체는 개인정보처리자에게 본인에 관한 개인정보를 부당한 지체 없이 삭제하도록 요구할 권리를 가지며, 처리자는 부당한 지체 없이 이를 삭제할 의무를 진다.
(a) 개인정보가 수집되거나 그 밖의 방식으로 처리된 목적과 관련하여 더 이상 필요하지 않은 경우
(b) 정보주체가 제6조 제1항 (a)호 또는 제9조 제2항 (a)호에 따라 처리의 근거가 된 동의를 철회하고, 처리의 다른 법적 근거가 없는 경우
(c) 정보주체가 제21조 제1항에 따라 처리에 이의를 제기하고 처리를 정당화하는 우선적 근거가 없는 경우, 또는 제21조 제2항에 따라 처리에 이의를 제기한 경우
(d) 개인정보가 위법하게 처리된 경우
(e) 개인정보처리자에게 적용되는 유럽연합법 또는 회원국법상 법적 의무를 준수하기 위해 개인정보를 삭제해야 하는 경우
(f) 제8조 제1항에 규정된 정보사회서비스의 제공과 관련하여 개인정보가 수집된 경우

제3항 다음의 목적을 위해 처리가 필요한 범위에서는 제1항 및 제2항을 적용하지 않는다.
(a) 표현 및 정보의 자유에 대한 권리를 행사하기 위한 경우
(b) 개인정보처리자에게 적용되는 유럽연합법 또는 회원국법이 처리를 요구하는 법적 의무를 준수하기 위한 경우, 또는 공익을 위해 수행되는 업무나 처리자에게 부여된 공적 권한을 행사하여 수행되는 업무를 이행하기 위한 경우
(c) 제9조 제2항 (h)호·(i)호 및 같은 조 제3항에 따른 공중보건 분야의 공익상 이유가 있는 경우
(d) 제89조 제1항에 따른 공익적 기록보존, 과학적·역사적 연구 또는 통계 목적을 위한 경우로서, 제1항의 권리가 그 처리 목적의 달성을 불가능하게 하거나 심각하게 저해할 우려가 있는 범위에 해당하는 경우
(e) 법적 청구권을 확립·행사 또는 방어하기 위한 경우

NoteBase

④

대상이 되지 않을 권리는 **오로지 자동화된 처리에 근거하여 법적 효과 또는 이에 준하는 중대한 영향을 미치는 결정**에 적용된다. 계약 체결·이행에 필요한 경우, 적절한 보호조치를 정한 법률이 허용하는 경우, 명시적으로 동의한 경우에는 예외도 인정된다. 따라서 **모든 자동화된 의사결정을 거부할 권리**는 아니다.

유럽연합 일반 개인정보보호법(GDPR) 제22조 제1항, 유럽연합 일반 개인정보보호법(GDPR) 제22조 제2항
제22조(프로파일링을 포함한 자동화된 개별 의사결정)
제1항 정보주체는 프로파일링을 포함하여 오로지 자동화된 처리에 근거하고, 본인에 관한 법적 효과를 발생시키거나 그와 유사하게 본인에게 중대한 영향을 미치는 결정의 대상이 되지 않을 권리를 가진다.

제2항 그 결정이 다음 중 어느 하나에 해당하는 경우 제1항을 적용하지 않는다.
(a) 정보주체와 개인정보처리자 사이의 계약 체결 또는 이행에 필요한 경우
(b) 개인정보처리자에게 적용되는 유럽연합법 또는 회원국법이 그 결정을 허용하고, 그 법이 정보주체의 권리·자유 및 정당한 이익을 보호하기 위한 적절한 조치도 정하는 경우
(c) 정보주체의 명시적 동의에 근거한 경우

NoteBase

문 14. 안티 리버싱 기법에 해당하는 것만을 모두 고르면?

ㄱ. 난독화
ㄴ. 스택 실드
ㄷ. 안티 디버깅
ㄹ. 카나리아

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 1번

간단한 해설

안티 리버싱은 프로그램의 구조와 동작을 분석하기 어렵게 만드는 기법이다. **난독화**는 코드의 이해를 어렵게 하고, **안티 디버깅**은 실행 중 동작을 추적하는 분석을 방해한다.

NoteBase

보기별 해설

안티 리버싱은 역공학을 통한 프로그램 분석을 어렵게 만드는 기법이다. 각 기법이 분석을 방해하는지, 메모리 손상 공격을 막는지를 구분한다.

ㄱ. 난독화: **안티 리버싱 기법**이다. 프로그램의 기능은 유지하면서 변수·함수 이름이나 제어 흐름 등을 알아보기 어렵게 바꾸어 코드의 의미와 구조를 파악하기 어렵게 한다.

ㄴ. 스택 실드: **스택 버퍼 오버플로 공격에 대한 방어 기법**이다. 함수 호출 시 복귀 주소를 별도 영역에 보관하고, 함수가 끝날 때 이를 이용하여 복귀 주소가 덮어써지는 공격에 대응한다. 프로그램 분석을 방해하는 안티 리버싱과는 목적이 다르다.

ㄷ. 안티 디버깅: **안티 리버싱 기법**이다. 디버거는 프로그램을 실행하면서 중단점을 설정하거나 변수·메모리 상태를 관찰하는 분석 도구이다. 안티 디버깅은 디버거의 존재를 탐지하거나 디버깅을 방해하여 이러한 동적 분석을 어렵게 한다.

ㄹ. 카나리아: **스택 버퍼 오버플로를 탐지하는 보호값**이다. 스택의 버퍼와 복귀 주소 사이에 값을 두고 함수가 끝날 때 그 값이 변했는지 확인한다. 버퍼를 넘쳐 쓴 데이터가 카나리아를 훼손하면 이를 탐지하여 실행을 중단하는 방식으로, 역공학 분석 방해와 구별된다.

안티 리버싱에 해당하는 항목은 ㄱ과 ㄷ이며, 이 조합은 ①에 해당한다.

NoteBase

문 15. 「개인정보 보호법」상 개인정보의 파기에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

③ 개인정보처리자가 개인정보를 파기하지 아니하고 다른 법령에 따라 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장 · 관리하여야 한다.

④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 총리령으로 정한다.

정답 4번

①

보유기간 경과나 처리 목적 달성 등으로 불필요해진 개인정보는 **지체 없이 파기**하여야 한다. 다만, **다른 법령에 따라 보존하여야 하는 경우**에는 예외이다.

개인정보 보호법 제21조 제1항
개인정보 보호법 제21조(개인정보의 파기)
① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다. <개정 2023.3.14>

②

개인정보를 파기할 때에는 **복구 또는 재생되지 아니하도록** 조치하여야 한다.

개인정보 보호법 제21조 제2항
개인정보 보호법 제21조(개인정보의 파기)
② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

NoteBase

③

다른 법령에 따라 파기하지 않고 보존하는 개인정보 또는 개인정보파일은 **다른 개인정보와 분리하여 저장·관리**하여야 한다.

개인정보 보호법 제21조 제3항
개인정보 보호법 제21조(개인정보의 파기)
③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장 · 관리하여야 한다.

④

개인정보의 파기방법 및 절차 등에 필요한 사항은 **대통령령**으로 정한다. 총리령으로 정하는 것이 아니다.

개인정보 보호법 제21조 제4항
개인정보 보호법 제21조(개인정보의 파기)
④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

NoteBase

문 16. 다중문자 암호 방식에 해당하는 것만을 모두 고르면?

ㄱ. 비즈네르(Vigenère) 암호
ㄴ. 시저(Caesar) 암호
ㄷ. 플레이페어(Playfair) 암호
ㄹ. 아핀(Affine) 암호

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 1번

간단한 해설

비즈네르는 **키의 위치에 따라 치환 규칙을 달리**하고, 플레이페어는 **두 문자를 한 쌍으로 묶어 치환**한다. 두 방식은 평문 문자 하나를 항상 같은 암호문 문자로 바꾸는 단일문자 치환과 구별된다.

보기별 해설

ㄱ. 비즈네르 암호: 다중문자 암호에 해당한다. 키워드를 평문에 반복하여 대응시키고, 각 키 문자에 따라 서로 다른 이동량을 적용한다. 따라서 **같은 평문 문자라도 대응하는 키 문자에 따라** 암호문 문자가 달라질 수 있다. 예를 들어 A를 0으로 두는 표준 방식에서 평문 AA에 키 BC를 대응시키면 암호문은 BC가 된다.

ㄴ. 시저 암호: 단일문자 치환 방식이다. 하나의 키로 정한 **동일한 이동량**을 모든 문자에 적용하므로, 같은 평문 문자는 항상 같은 암호문 문자로 바뀐다. 예를 들어 세 칸 이동시키는 키에서는 평문의 A가 나타날 때마다 D로 바뀐다.

ㄷ. 플레이페어 암호: 다중문자 암호에 해당한다. 키로 구성한 5 × 5 문자표를 이용하여 평문을 **두 문자씩 묶어 치환**한다. 한 문자의 치환 결과는 짝을 이룬 다른 문자와 문자표에서의 위치 관계에 따라 달라지므로, 문자 하나마다 고정된 치환 결과를 갖는 방식과 구별된다.

ㄹ. 아핀 암호: 단일문자 치환 방식이다. 각 문자를 숫자에 대응시킨 뒤, 키로 정한 계수를 이용한 곱셈·덧셈과 나머지 연산으로 치환한다. **키가 고정되면 같은 평문 문자는 항상 같은 암호문 문자**로 바뀌므로, 연산이 시저 암호보다 복잡하더라도 다중문자 암호가 되는 것은 아니다.

다중문자 암호에 해당하는 보기는 ㄱ과 ㄷ이며, 이 조합은 ①과 일치한다.

NoteBase

문 17. 「개인정보 보호법」상 개인정보처리자가 개인정보의 제3자 제공과 관련하여 정보주체에게 동의를 받을 때 정보주체에게 알려야 하는 사항이 아닌 것은?

① 개인정보를 제공받는 자의 개인정보 이용 목적
② 동의에 따른 이익이 있는 경우에는 그 이익의 내용
③ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

정답 2번

①

제3자 제공 동의를 받을 때에는 **개인정보를 제공받는 자의 개인정보 이용 목적**을 정보주체에게 알려야 한다.

개인정보 보호법 제17조 제2항 제2호
개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
2. 개인정보를 제공받는 자의 개인정보 이용 목적

②

동의에 따른 이익의 내용은 법정 고지사항에 포함되지 않는다. 알려야 하는 것은 **동의를 거부할 권리가 있다는 사실과 거부에 따른 불이익이 있는 경우 그 불이익의 내용**이다.

개인정보 보호법 제17조 제2항
개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

NoteBase

③

동의를 거부할 권리가 있다는 사실을 알려야 하며, **동의 거부에 따른 불이익이 있는 경우에는 그 내용도** 알려야 한다.

개인정보 보호법 제17조 제2항 제5호
개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

④

제3자 제공 동의를 받을 때에는 **개인정보를 제공받는 자의 개인정보 보유 및 이용 기간**을 정보주체에게 알려야 한다.

개인정보 보호법 제17조 제2항 제4호
개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

NoteBase

문 18. 다음 표를 이용하여 24비트 입력 '01000001 01000010 01000011'에 Base64 부호화를 적용할 때, 출력되는 문자열은?

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/

① YWJj

② Q0JB

③ QUJD

④ Y2Jh

정답 3번

간단한 해설

입력 비트를 순서대로 **6비트씩 다시 묶으면** 각 묶음의 값은 16, 20, 9, 3이다. 표에서 이 값에 대응하는 문자를 차례로 연결하면 'QUJD'가 된다.

NoteBase

계산 과정

1. 비트 묶음 나누기: Base64는 6비트 묶음 하나를 표의 문자 하나로 바꾼다. 따라서 24비트 입력은 문자 4개로 변환된다. **원래의 8비트 경계에 구애받지 않고** 입력 비트를 왼쪽부터 6비트씩 나누면 다음과 같다.
01000001 01000010 01000011 → 010000 010100 001001 000011

2. 인덱스 계산: 6비트의 자릿값은 왼쪽부터 32, 16, 8, 4, 2, 1이다. 각 묶음에서 **비트가 1인 자리의 값만 더하면** 표의 Index 값이 된다.
010000 → 16
010100 → 16 + 4 = 20
001001 → 8 + 1 = 9
000011 → 2 + 1 = 3

3. 문자 대응: 표의 Index와 Char를 대응시키면 16은 Q, 20은 U, 9는 J, 3은 D이다. 이 문자들을 입력 비트의 순서대로 연결한 출력 문자열은 'QUJD'이며, ③의 문자열과 일치한다.

NoteBase

문 19. 개인정보 가명 처리 세부기술에 대한 설명으로 옳지 않은 것은?

① 총계 처리는 평균값, 최댓값, 최솟값, 최빈값, 중간값 등으로 처리한다.

② 일반 라운딩은 올림, 내림, 반올림 등의 기준을 적용하여 집계 처리하는 방법으로, 일반적으로 세세한 정보보다는 전체 통계 정보가 필요한 경우 많이 사용한다.

③ 로컬 일반화는 전체 정보집합물 중 특정 열 항목(들)에서 특이한 값을 가지거나 분포상의 특이성으로 인해 식별성이 높아지는 경우 해당 부분만 일반화를 적용하여 식별성을 낮추는 방법이다.

④ 순서보존 암호화는 원문에 대한 암호화의 적용만 가능하고 암호문에 대한 복호화 적용이 불가능한 암호화 기법이다.

정답 4번

간단한 해설

④의 '복호화 적용이 불가능하다'는 설명은 **일방향 해시 처리**의 특성이다. 순서보존 암호화는 **원본 값의 대소관계를 암호값에서도 유지**하며, 키를 이용한 복호화가 가능하다.

선지별 해설

① O: 총계 처리는 여러 개별 값을 평균값·최댓값·최솟값·최빈값·중간값 등의 **집단을 대표하는 통계값**으로 처리하는 방법이다. 개별 자료를 그대로 제시하는 대신 집단의 특성을 요약하여 표현한다.

② O: 일반 라운딩은 정한 자리나 단위를 기준으로 올림·내림·반올림을 적용하여 **수치의 세밀함을 줄이는** 방법이다. 예를 들어 나이 27세를 10세 단위로 반올림하여 30세로 처리하면 정확한 나이는 드러내지 않으면서 대략적인 통계 분석에 활용할 수 있다.

③ O: 로컬 일반화는 특이한 값이나 드문 분포 때문에 개인이 쉽게 식별될 수 있는 **일부 항목에만 일반화를 적용**하는 방법이다. 해당 값을 더 넓은 범주로 바꾸어 식별성을 낮추며, 전체 자료의 모든 값을 일괄적으로 일반화할 필요는 없다.

④ X: 순서보존 암호화는 원본 값 사이의 **대소관계를 암호값에서도 유지**하는 암호화 방식이다. 따라서 암호문을 복호화하지 않고도 값의 크기를 비교하거나 범위 검색을 할 수 있으며, 키를 이용하면 원문으로 복호화할 수 있다. '복호화 적용이 불가능하다'는 부분은 일방향 해시 처리의 특성이므로, 순서보존 암호화의 설명으로 바꾸어야 한다.

NoteBase

문 20. S/MIME에서 사용하는 암호 알고리즘과 기능을 옳게 짝지은 것은?

① DSS - 전자서명

② ElGamal - 메시지 인증

③ AES - 전자서명과 세션키 암호화

④ RSA - 메시지 암호화

정답 1번

간단한 해설

DSS는 **전자서명**을 위한 표준이며, DSA로 서명을 생성하고 검증한다. 이를 통해 메시지가 변조되지 않았는지와 서명자의 신원을 확인한다.

선지별 해설

① O: DSS(Digital Signature Standard)는 전자서명 표준이다. S/MIME에서 DSS에 따른 DSA를 사용하면 송신자는 개인키로 메시지의 해시값에 서명하고, 수신자는 송신자의 공개키로 서명을 검증한다. 이로써 **메시지 무결성과 송신자 인증**을 제공한다.

② X: ElGamal 암호화는 수신자의 공개키로 데이터를 암호화하고 수신자의 개인키로 복호화하여 **기밀성**을 제공하는 공개키 암호 방식이다. 이를 S/MIME의 메시지 인증 알고리즘으로 짝지은 것은 부적절하다. S/MIME에서 송신자 인증과 무결성을 위한 전자서명에는 DSA나 RSA 등을 사용한다.

③ X: AES는 대칭키 블록 암호로, S/MIME에서 **메시지 본문 암호화**에 사용한다. AES로 키를 감싸 보호하는 키 래핑도 가능하지만, AES는 전자서명 알고리즘이 아니므로 전자서명과 세션키 암호화를 함께 담당한다는 연결은 성립하지 않는다.

④ X: RSA 자체는 데이터를 암호화할 수 있지만, S/MIME의 암호화 구조에서는 메시지 본문이 아니라 **본문 암호화에 사용한 세션키**를 암호화하여 전달하는 데 사용한다. 예를 들어 본문은 AES로 암호화하고, 그 AES 키는 수신자의 RSA 공개키로 암호화한다. 수신자는 자신의 RSA 개인키로 AES 키를 복구한 뒤 본문을 복호화한다.

NoteBase