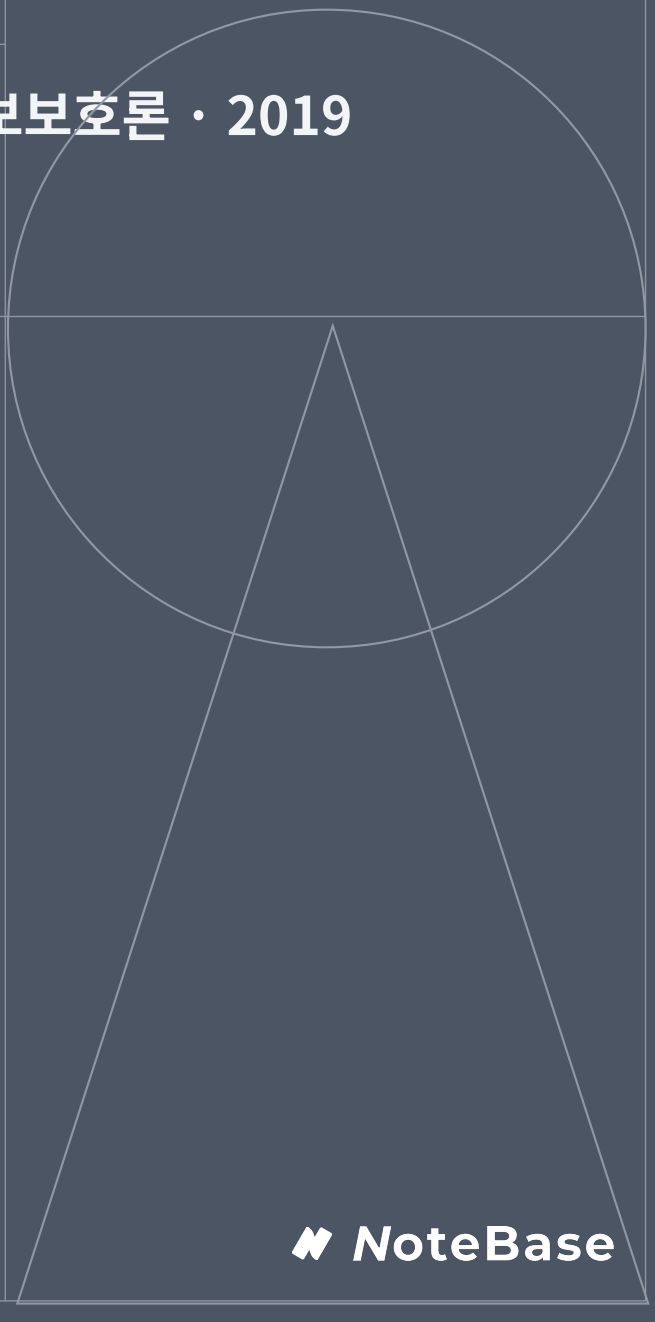
기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2019



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2019

공무원/경찰/경력채용 · 정보보호론 · 2019

문 1. 다음에 설명하는 정보보호의 목표로 가장 적절한 것은?

정당한 방법으로 권한을 받은 사용자가 자원을 필요로 할 때, 아무런 방해 없이 자원에 접근하고 사용할 수 있음을 보장한다.

① 기밀성(confidentiality)
② 무결성(integrity)
③ 가용성(availability)
④ 신뢰성(reliability)

정답 3번

간단한 해설

지문은 **권한 있는 사용자가 필요할 때 자원을 이용할 수 있음**을 강조한다. 이는 정보와 서비스의 접근·사용 가능성을 보장하는 가용성이다.

NoteBase

개념 구분

가용성: **권한 있는 사용자가 필요할 때 자원에 접근하고 사용할 수 있는 상태**를 보장하는 성질이다. 지문은 사용자의 정당한 권한을 전제로 자원 이용이 방해받지 않는다는 점을 강조하므로 가용성에 해당한다. 서비스 거부 공격이나 시스템 장애로 자원을 사용할 수 없게 되면 가용성이 침해된다.

기밀성: **권한 없는 사람에게 정보가 노출되지 않도록** 하는 성질이다. 정보를 누가 열람할 수 있는지가 중심이며, 권한 있는 사용자가 필요할 때 이용할 수 있는지를 묻는 지문의 초점과 구별된다.

무결성: 정보가 **허가 없이 변경되거나 훼손되지 않도록** 하여 정확성과 완전성을 유지하는 성질이다. 자원에 접속할 수 있는지보다 정보의 내용이 올바르게 보존되는지가 중심이다.

신뢰성: 시스템이 **정해진 조건과 기간 동안 요구된 기능을 제대로 수행**하는 성질이다. 가용성을 높이는 데 기여할 수 있지만, 지문처럼 권한 있는 사용자의 필요 시점 접근·이용을 직접 설명하는 정보보호 목표는 가용성이다.

따라서 지문의 정보보호 목표는 ③ 가용성이다.

NoteBase

문 2. 다음 대칭키 암호화에서 키 K값으로 가장 적절한 것은?

· 대칭키 암호화: 8비트 정보 P와 K의 배타적 논리합(XOR) 연산의 결과를 C라 함
· P=00101100
· C=10000110

① 11010010
② 10101010
③ 01010101
④ 10011001

정답 2번

간단한 해설

XOR는 같은 값을 두 번 적용하면 상쇄되므로 **평문과 암호문을 XOR**하면 키를 얻는다.
00101100 ⊕ 10000110 = 10101010이다.

계산 과정

XOR는 같은 자리의 두 비트가 **다르면 1, 같으면 0**이 되는 연산이다. 같은 비트열을 두 번 XOR하면 원래 값으로 돌아오므로, 암호화 관계 $C = P \oplus K$에서 키는 $K = P \oplus C$로 구한다.

주어진 평문 P는 00101100이고 암호문 C는 10000110이다. 두 값을 왼쪽부터 같은 자리끼리 XOR한다.
$K = 00101100 \oplus 10000110 = 10101010$
왼쪽에서 1·3·5·7번째 비트가 서로 다르므로 해당 자리는 1이고, 나머지 자리는 0이다.

구한 키를 평문에 다시 적용하면 00101100 ⊕ 10101010 = 10000110으로 주어진 암호문이 나온다.
따라서 키의 8비트와 자리 순서가 모두 일치한다.

키 K는 10101010이므로 ②와 일치한다.

NoteBase

문 3. 복호화 수식이 다음과 같을 때 블록 암호 운영모드로 가장 적절한 것은? (단, P_i: i번째 평문, C_i: i번째 암호문, $D_K(C_i)$: 복호화)

$P_i = D_K(C_i) \oplus C_{i-1}$

① CBC(Cipher Block Chaining, 암호블록 연쇄) 모드

② CFB(Cipher FeedBack, 암호 피드백) 모드

③ ECB(Electronic CodeBook, 전자코드북) 모드

④ CTR(Counter, 카운터) 모드

정답 1번

간단한 해설

현재 암호문을 복호화한 뒤 이전 암호문과 XOR하는 것은 CBC의 복호화 방식이다. 암호화할 때 평문에 결합했던 이전 암호문을 다시 XOR하여 평문을 복원한다.

핵심 풀이

주어진 $P_i = D_K(C_i) \oplus C_{i-1}$는 현재 암호문 블록을 복호화한 결과에 이전 암호문 블록을 XOR한다는 뜻이다. CBC는 암호화할 때 $C_i = E_K(P_i \oplus C_{i-1})$로 이전 암호문과 평문을 먼저 XOR하므로, 이를 되돌리면 제시된 복호화식이 된다. 첫 블록은 이전 암호문 대신 초기화 벡터를 사용하여 $P_1 = D_K(C_1) \oplus IV$로 복호화한다.

CFB는 **복호화에도 암호화 함수**를 사용하여 되먹임한 암호문으로 출력을 만들고, 그 출력과 현재 암호문을 XOR한다. 제시식처럼 현재 암호문에 복호화 함수를 적용하는 구조와 다르다.

ECB는 암호문 블록을 각각 독립적으로 복호화하므로 식이 $P_i = D_K(C_i)$이다. **이전 암호문과 XOR하는 항이 없다**.

CTR은 카운터 값을 암호화하여 만든 출력과 암호문을 XOR한다. 블록 사이를 이전 암호문으로 연결하는 대신 **카운터 값**을 사용하므로 제시식에 해당하지 않는다.

현재 암호문의 복호화 결과를 이전 암호문과 XOR하는 운영모드는 ①의 CBC이다.

NoteBase

문 4. 하이브리드 암호시스템에 대한 설명으로 가장 적절하지 않은 것은?

① 대칭키 암호시스템과 공개키 암호시스템의 장점을 조합하였다.

② 평문 메시지는 대칭키 암호로 암호화한다.

③ 암호화에서 사용하는 세션키는 의사난수 생성기를 이용하여 생성한다.

④ PGP(Pretty Good Privacy), SSL/TLS(Secure Socket Layer/Transport Layer Security), RSA에서 하이브리드 암호 시스템을 사용한다.

정답 4번

간단한 해설

RSA 자체는 공개키 암호 알고리즘이다. RSA를 대칭키 암호와 함께 사용하면 하이브리드 암호시스템을 구성할 수 있지만, RSA 자체가 두 방식을 결합한 시스템은 아니다.

선지별 해설

① O: 하이브리드 암호시스템은 **대칭키 암호의 처리 효율과 공개키 암호의 키 공유상 이점**을 결합한다. 데이터 본문에는 대칭키 암호를 사용하고, 그 키를 안전하게 전달하거나 합의하는 과정에는 공개키 기법을 이용한다.

② O: 대용량의 평문 메시지는 처리 부담이 작은 **대칭키 암호로 암호화**한다. 공개키 암호로 세션키를 전달하는 방식에서는, 세션키를 수신자의 공개키로 암호화하고 수신자는 자신의 개인키로 이를 복원한 뒤 본문을 복호화한다.

③ O: 세션키는 메시지나 통신 세션을 보호하는 대칭키이며 예측하기 어려워야 한다. 이를 생성할 때 **암호학적으로 안전한 의사난수 생성기**를 이용한다. 단순히 일정한 수열을 만드는 일반 난수 함수만으로는 암호용 키의 안전성을 보장할 수 없다.

④ X: PGP와 공개키 기반 SSL/TLS는 공개키 기법과 대칭키 암호를 결합하는 방식의 예이다. 반면 **RSA 자체는 공개키 암호 알고리즘**이며 하이브리드 암호시스템 전체를 뜻하지 않는다. RSA를 키 전달 등에 이용하고 AES 같은 대칭키 암호로 본문을 암호화하면 하이브리드 시스템을 구성할 수 있지만, RSA만을 하이브리드 방식의 사례로 나열한 것은 잘못이다.

NoteBase

문 5. 메시지 인증 코드와 전자서명에 대한 설명으로 가장 적절하지 않은 것은?

① 메시지 인증 코드와 전자서명 모두 무결성을 확인할 수 있다.

② 메시지 인증 코드는 부인방지(non-repudiation) 기능을 제공한다.

③ 전자서명은 서명자를 인증하는 기능이 있다.

④ 메시지 인증 코드는 메시지와 비밀키를 사용한다.

정답 2번

간단한 해설

MAC은 송신자와 수신자가 **같은 비밀키로 인증 값을 생성**할 수 있어, 누가 생성했는지 제3자에게 입증하기 어렵다. 따라서 일반적인 MAC은 **부인방지를 제공하지 않는다**.

선지별 해설

① O: 메시지 인증 코드(MAC)와 전자서명은 모두 메시지가 변경되었는지 검사하여 **무결성**을 확인할 수 있다. MAC은 공유 비밀키로 계산한 인증 값을 확인하고, 전자서명은 서명자의 공개키로 메시지에 대한 서명을 검증한다.

② X: 일반적인 MAC은 송신자와 수신자가 **같은 비밀키를 공유**하므로 둘 다 유효한 MAC을 만들 수 있다. 따라서 제3자에게 특정 송신자만 메시지를 생성했다고 입증하기 어려워 **부인방지를 제공하지 않는다**. 부인방지는 서명자가 자신의 개인키로 생성하고 제3자도 공개키로 검증할 수 있는 전자서명의 기능이다.

③ O: 전자서명은 서명자의 개인키로 생성하고 대응하는 공개키로 검증한다. 공개키와 서명자의 연결이 신뢰할 수 있고 개인키가 적절히 보호된다면, 그 개인키로 서명했다는 사실을 통해 **서명자를 인증**할 수 있다.

④ O: MAC은 **메시지와 공유 비밀키**를 입력으로 사용해 인증 값을 생성한다. 수신자는 같은 키로 수신한 메시지의 MAC을 다시 계산하여 전달받은 값과 비교한다. 비밀키 없이 메시지만 처리하는 일반 해시와 구별된다.

따라서 적절하지 않은 설명은 MAC이 부인방지를 제공한다고 한 ②이다.

NoteBase

문 6. 공개키 기반 구조(PKI: Public Key Infrastructure)에 대한 설명으로 가장 적절하지 않은 것은?

① 공개키 기반 구조의 구성요소로는 사용자(user), 등록기관(Registration Authority), 인증기관(Certification Authority), 저장소(repository) 등이 있다.

② 공개키 인증서를 발행하여 무결성, 인증, 부인방지를 보장한다.

③ 등록기관은 인증서와 인증서 취소 목록(Certificate Revocation List)을 발행하고, 공개키 등록 시 본인을 인증한다.

④ 저장소는 인증서를 보관해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 구성된 데이터베이스이다.

정답 3번

간단한 해설

등록기관(RA)은 **신청자의 신원 확인과 등록 심사**를 담당한다. 인증서 발급과 폐지 상태 정보 제공은 **인증기관(CA)의 책임**이므로 두 기관의 역할을 구별해야 한다.

선지별 해설

① O: PKI는 공개키와 그 소유자의 신원을 신뢰할 수 있게 연결하고 인증서를 관리하는 기반 구조이다. 사용자, 신청자의 신원을 확인하는 등록기관(RA), 인증서를 발급하는 인증기관(CA), 인증서 등을 보관·배포하는 저장소가 구성요소에 포함된다.

② O: 공개키 인증서는 **소유자 정보와 공개키의 연결**을 CA의 전자서명으로 확인할 수 있게 한다. 이처럼 신뢰할 수 있는 공개키를 이용해 전자서명을 검증하면 메시지의 무결성과 작성자 인증을 확인하고, 서명자가 자신의 서명 행위를 부당하게 부인하지 못하도록 하는 부인방지 서비스를 지원한다.

③ X: **등록기관의 본인확인 업무와 인증기관의 발급 업무**를 혼동했다. RA는 인증서 신청자의 신원을 확인하고 등록 신청을 심사하는 역할을 맡는다. 인증서 발급과 그 인증서의 폐지 상태 정보 제공은 CA의 책임이며, 기본적인 PKI 구조에서는 CA가 인증서와 CRL에 서명하여 발행한다. CRL은 유효기간이 끝나기 전에 폐지되어 더 이상 신뢰하면 안 되는 인증서의 목록이다.

④ O: 저장소는 인증서를 보관하고 PKI 이용자가 필요한 인증서를 **검색·입수할 수 있도록 배포**하는 시스템이다. 인증서뿐 아니라 폐지 여부 확인에 필요한 CRL도 저장·제공할 수 있다. 저장소의 역할은 인증서 정보를 제공하는 것이며, 신청자의 신원 심사나 인증서 발급과 구별된다.

따라서 등록기관과 인증기관의 역할을 잘못 연결한 ③이 적절하지 않은 설명이다.

NoteBase

문 7. 다음 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

(㉠) 공격은 소스 IP주소와 목적지 IP주소가 동일한 다량의 패킷을 특정 공격 대상 시스템으로 전송하면, 응답이 자기 자신에게 되돌아오도록 하여 시스템의 과부하를 유발한다.
(㉡) 공격은 ICMP Echo 메시지를 큰 패킷으로 만들어, 공격 대상 시스템에 분할된 많은 양의 패킷을 도달시켜, 패킷 재결합으로 인한 시스템 과부하를 유발한다.
(㉢) 공격은 ICMP 프로토콜과 브로드캐스팅 개념을 사용한 공격으로, 공격대상 호스트의 IP 주소를 source 주소로 갖는 ICMP Echo 요청 패킷을 directed 브로드캐스트 함으로써, 많은 양의 ICMP Echo 응답 패킷을 공격대상 호스트에 전송한다. 이는 공격대상 시스템의 자원을 고갈시킨다.

① ㉠: LAND, ㉡: ICMP Flooding, ㉢: Ping of Death
② ㉠: LAND, ㉡: Ping of Death, ㉢: ICMP Flooding
③ ㉠: Ping of Death, ㉡: ICMP Flooding, ㉢: LAND
④ ㉠: Ping of Death, ㉡: LAND, ㉢: ICMP Flooding

정답 2번

간단한 해설

출발지와 목적지 IP 주소가 같은 것은 **LAND**의 단서이다. Ping of Death는 단순한 재조립 부하보다 **허용 크기를 넘는 패킷의 재조립 처리 취약점**이 핵심이다. 위조된 출발지 주소와 브로드캐스트로 ICMP 응답을 집중시키는 것은 **Smurf 방식의 ICMP Flooding**이다.

NoteBase

빈칸별 해설

㉠: LAND. **출발지와 목적지 IP 주소를 공격 대상의 주소로 같게** 만드는 것이 결정적인 단서이다. 전형적인 LAND는 출발지·목적지 포트도 같게 만든 TCP SYN 패킷으로 취약한 시스템의 처리를 방해한다. ICMP Echo를 이용한 나머지 두 설명과 구별된다.

㉡: Ping of Death. 큰 ICMP Echo 패킷과 분할·재조립이라는 단서로 구별한다. 다만 지문의 '패킷 재결합으로 인한 시스템 과부하'는 정확한 원인을 충분히 설명하지 못한다. 전형적인 Ping of Death는 **재조립된 IP 패킷이 허용 최대 크기를 넘도록** 하여 이를 제대로 처리하지 못하는 구현의 취약점을 악용한다. 정상적인 큰 패킷의 분할·재조립 자체가 공격인 것은 아니다.

㉢: ICMP Flooding. 피해자의 IP 주소를 출발지로 위조한 Echo 요청을 브로드캐스트하면 여러 호스트의 Echo 응답이 피해자에게 집중된다. 이 구체적인 방식은 **Smurf 공격**이며, 반사·증폭된 ICMP 트래픽으로 자원이나 대역폭을 소모시키는 ICMP flooding의 한 형태이다. 모든 ICMP flooding이 브로드캐스트를 사용하는 것은 아니지만, 이 문항은 해당 방식을 ICMP Flooding으로 제시한다.

따라서 ㉠ LAND, ㉡ Ping of Death, ㉢ ICMP Flooding의 연결은 ②와 일치한다.

NoteBase

문 8. 다음 TCP/IP 프로토콜의 계층별 역할에 대한 설명 중 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

(㉠) 계층에서는 송수신지 사이의 패킷을 전달한다. 이를 위해 IP 주소 지정, 패킷화, 단편화가 제공된다.
(㉡) 계층에서는 근거리 통신망(LAN)에서 전송 매체에 데이터(프레임)를 송수신하는 역할을 담당한다.
(㉢) 계층에서는 종단간 통신 서비스 제공을 담당한다. TCP와 UDP가 대표적인 프로토콜이다.

① ㉠: 네트워크, ㉡: 데이터링크, ㉢: 전송
② ㉠: 네트워크, ㉡: 전송, ㉢: 데이터링크
③ ㉠: 전송, ㉡: 데이터링크, ㉢: 네트워크
④ ㉠: 전송, ㉡: 네트워크, ㉢: 데이터링크

정답 1번

간단한 해설

IP 주소와 패킷 전달은 네트워크 계층, **LAN에서의 프레임 송수신**은 데이터링크 계층의 역할이다. TCP·UDP를 이용한 종단간 통신은 전송 계층에 해당한다.

빈칸별 해설

㉠: **네트워크 계층**이다. IP 주소를 이용하여 출발지 호스트에서 목적지 호스트로 패킷을 전달한다. IP 패킷의 구성과 필요한 단편화는 이 계층의 역할이므로, 'IP 주소 지정'과 '패킷'이 구별 단서이다.

㉡: **데이터링크 계층**이다. LAN과 같은 개별 링크에서 데이터를 프레임으로 구성하여 연결된 장치 사이에 전달한다. 여러 네트워크를 거치는 전체 경로의 패킷 전달과 달리, 해당 링크에서의 프레임 송수신을 담당한다.

㉢: **전송 계층**이다. 통신 양 끝의 응용 프로그램에 종단간 통신 서비스를 제공한다. TCP와 UDP가 이 계층에 속하며, TCP는 신뢰성 있는 연결형 서비스를, UDP는 비연결형 데이터그램 서비스를 제공한다.

따라서 ㉠ 네트워크, ㉡ 데이터링크, ㉢ 전송으로 연결한 ①과 일치한다.

NoteBase

문 9. 다음 사이버 공격 유형에 대한 설명 중 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

(㉠)은 공격자가 도메인을 탈취하여 사용자가 정확한 URL 주소를 입력해도 가짜 사이트로 연결되도록 하는 방법이다.
(㉡)은 이메일 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여 신용정보 등의 기밀을 부정하게 얻으려는 사회공학기법을 사용한다.
(㉢)은 문자메시지를 신뢰할 수 있는 사람이 보낸 것처럼 가장하여, 링크 접속을 유도한 뒤 개인정보를 빼내는 방법이다.

① ㉠: 스미싱(Smishing), ㉡: 피싱(Phishing), ㉢: 파밍(Pharming)
② ㉠: 스미싱(Smishing), ㉡: 파밍(Pharming), ㉢: 피싱(Phishing)
③ ㉠: 파밍(Pharming), ㉡: 피싱(Phishing), ㉢: 스미싱(Smishing)
④ ㉠: 파밍(Pharming), ㉡: 스미싱(Smishing), ㉢: 피싱(Phishing)

정답 3번

간단한 해설

정확한 URL을 입력해도 **연결 대상을 가짜 사이트로 바꾸는** 것은 파밍이다. 신뢰할 만한 발신자를 사칭해 정보를 얻는 것은 피싱이며, 특히 **문자메시지를 이용한 피싱**은 스미싱이다.

빈칸별 해설

㉠ 파밍: 도메인이나 이름 해석 정보 등을 조작하여 **정확한 URL을 입력해도 가짜 사이트로 연결**되게 하는 공격이다. 제시문에서는 도메인 탈취로 정상 주소의 연결 대상을 바꾸었다는 점이 결정적인 단서이다. 사용자가 사칭 메시지의 링크를 누르도록 속이는 방식과 구별된다.

㉡ 피싱: 신뢰할 만한 사람이나 기업을 사칭한 이메일·메신저 등으로 사용자를 속여 **기밀정보를 스스로 제공하도록 유도**하는 사회공학적 공격이다. 메시지 발신자의 신뢰성을 가장하여 신용정보 등을 얻으려는 설명이 이에 해당한다.

㉢ 스미싱: 문자메시지(SMS)를 이용한 피싱이다. 제시문처럼 **문자메시지의 링크 접속을 유도**해 개인정보를 빼내는 것이 특징이다. 피싱이라는 넓은 범주 안에서 문자메시지를 이용한다는 전달 수단을 구체적으로 나타낸다.

㉠은 파밍, ㉡은 피싱, ㉢은 스미싱이므로 이 연결을 제시한 ③과 일치한다.

NoteBase

문 10. 소인수분해의 어려움을 기반으로 한 RSA 암호 알고리즘에서 개인키 d는 7, 합성수 n은 33, 평문 값이 5일 때, 이를 암호화한 암호문의 값으로 가장 적절한 것은?

① 12

② 13

③ 21

④ 26

정답 4번

간단한 해설

암호화에는 개인키 지수 d가 아니라 **공개키 지수 e**를 사용한다. d = 7에 대응하는 e를 3으로 잡으면 5^333=26이므로 암호문은 26이다.

계산 과정

소인수와 오일러 함수: n = 33을 소인수분해하면 3 × 11이다. 서로 다른 두 소수의 곱이므로 $\varphi(33) = (3-1)(11-1) = 20$이다.

공개키 지수: RSA 암호화에는 주어진 개인키 지수 d가 아니라 **공개키 지수 e**를 사용한다. ed≡1±od(n)을 만족하도록 e를 구하면 7e≡1±od20이다. 7 × 3 = 21이고 21을 20으로 나눈 나머지가 1이므로 e = 3을 사용할 수 있다.

암호문 계산: 평문 m = 5와 공개키 지수 e = 3을 c=m^e n에 대입한다. 따라서 c=5^333=12533이다. 125 = 33 × 3 + 26이므로 **나머지 26이 암호문**이다.

계산한 암호문 26은 ④와 일치한다.

NoteBase

문 11. IEEE 802.11i에서 데이터를 보호하기 위해서 AES 알고리즘을 사용한 암호화 운영모드와 메시지 인증기법으로 가장 적절하게 짝지은 것은?

① CBC 모드, HMAC 인증

② CBC 모드, CBC-MAC 인증

③ CTR 모드, HMAC 인증

④ CTR 모드, CBC-MAC 인증

정답 4번

간단한 해설

IEEE 802.11i의 AES 기반 CCMP는 **CTR 모드로 기밀성**을, **CBC-MAC으로 메시지 인증과 무결성**을 제공한다.

대응 관계 해설

IEEE 802.11i에서 AES를 사용하는 데이터 보호 방식은 CCMP이며, 그 바탕이 되는 CCM은 기밀성과 메시지 인증을 함께 제공한다. 암호화와 메시지 인증에는 각각 다른 기법이 대응된다.

암호화 운영모드: **CTR 모드**이다. 카운터 값을 AES로 암호화하여 얻은 값과 평문을 배타적 논리합(XOR)으로 결합함으로써 데이터의 기밀성을 보호한다. 이전 암호문 블록을 다음 평문 블록과 연쇄시키는 CBC 암호화 모드를 사용하는 것이 아니다.

메시지 인증기법: **CBC-MAC**이다. 메시지 블록을 AES로 연쇄 처리해 인증값을 만들고, 수신 측이 이를 검증하여 데이터의 무결성과 출처 인증을 확인한다. 이름에 CBC가 들어가는 것은 인증값 계산 방식 때문이며, 데이터 암호화에 CBC 모드를 쓴다는 뜻은 아니다. HMAC은 해시 함수를 바탕으로 하는 메시지 인증코드로, 이 문항의 CCMP 인증 방식에 해당하지 않는다.

따라서 암호화 운영모드와 메시지 인증기법의 짝은 CTR 모드와 CBC-MAC 인증이며, ④에 해당한다.

NoteBase

문 12. 이메일 보안 S/MIME에 대한 설명 중 가장 적절한 것은?

① 동봉된 데이터(enveloped data)는 암호화된 내용과 서명자의 공개키로 구성된다.

② 서명된 데이터(signed data)는 메시지 다이제스트 값을 서명자의 공개키로 암호화한 후, 그 값을 Base64로 부호화한다.

③ 명문-서명 데이터(clear-signed data)는 내용과 내용에 대한 전자서명으로 구성되며, 전자서명만 Base64로 부호화한다.

④ 서명되고 동봉된 데이터(signed and enveloped data)에서 서명만 되거나 암호화된 개체는 중첩될 수 없다.

정답 3번

간단한 해설

명문-서명 방식은 **본문을 읽을 수 있게 두고 전자서명을 분리**하여 제공한다. 서명 부분을 Base64로 부호화하므로 서명 검증 기능이 없는 수신 프로그램도 본문을 읽을 수 있다.

선지별 해설

① X: 동봉된 데이터는 암호화된 본문과 수신자가 내용을 복호화하는 데 필요한 키 전달 정보로 구성된다. 공개키 방식의 키 전달에서는 본문을 대칭키로 암호화하고, 그 대칭키를 **수신자의 공개키로 암호화**하여 함께 보낸다. '서명자의 공개키'가 동봉 데이터의 핵심 구성이라는 설명은 잘못되었다.

② X: 전자서명은 **서명자의 개인키로 생성**하고, 대응하는 공개키로 검증한다. 메시지 다이제스트에 서명 알고리즘을 적용하는 것이므로 '서명자의 공개키로 암호화'한다는 부분을 바로잡아야 한다. Base64는 전송을 위한 부호화이며, 서명을 생성하는 암호학적 연산과는 별개이다.

③ O: 명문-서명 데이터는 **읽을 수 있는 본문과 분리된 전자서명**을 함께 제공한다. 서명 부분을 Base64로 부호화하므로, 서명을 처리하지 못하는 수신 프로그램도 본문을 읽을 수 있다. 이는 본문과 서명을 하나의 불투명한 서명 데이터로 감싸는 방식과 구별하는 설명이며, 본문 자체의 MIME 전송 인코딩까지 금지한다는 뜻은 아니다.

④ X: 서명된 개체와 암호화된 개체는 **중첩할 수 있다**. 예를 들어 메시지에 먼저 서명한 뒤 그 결과를 암호화하거나, 암호화된 개체에 다시 서명할 수 있으므로 '중첩될 수 없다'는 설명은 잘못되었다.

NoteBase

문 13. 웹사이트와 브라우저에 대한 공격 유형에 관한 설명 중 ㉠과 ㉡에 들어갈 용어로 가장 적절하게 연결된 것은?

(㉠) 공격법의 한 예로는 URL에 인자 형태로 악성 스크립트를 포함시킨 메일을 사용자에게 보낸 후, 사용자가 URL을 클릭하면 서버로부터 반송된 오류 메시지에 포함된 악성 스크립트가 실행되는 방법이 있다.
(㉡) 공격법의 한 예로는 로그인 상태인 사용자의 세션 쿠키와 다른 인증정보를 취약한 웹 애플리케이션에 자동으로 포함시키고, 공격자가 의도한 HTTP 요청을 사용자가 보낸 것처럼 자동으로 보내는 방법이 있다.

① ㉠: Reflected XSS, ㉡: CSRF

② ㉠: SQL 인젝션, ㉡: Reflected XSS

③ ㉠: CSRF, ㉡: SQL 인젝션

④ ㉠: Reflected XSS, ㉡: S-HTTP

정답 1번

간단한 해설

요청에 포함된 스크립트가 **서버 응답에 반사되어 브라우저에서 실행**되면 Reflected XSS이다. 로그인 상태의 브라우저가 인증정보를 자동으로 보내는 점을 이용하여 **사용자 의사와 다른 요청을 수행**시키면 CSRF이다.

빈칸별 해설

㉠: Reflected XSS. 공격자가 URL의 인자에 넣은 스크립트가 사용자의 클릭으로 서버에 전달되고, **서버 응답에 반사되어 돌아온 뒤 브라우저에서 실행**된다. 지문의 오류 메시지가 바로 그 응답이다. 코드가 사이트에 저장된 후 다른 요청에서 전달되는 저장형 XSS와 구별된다. SQL 인젝션은 데이터베이스 질의를 조작하는 공격이므로 이 브라우저 실행 흐름과 다르다.

㉡: CSRF. 로그인된 사용자의 브라우저가 해당 사이트의 **인증정보를 자동으로 포함하는 요청**을 악용하여 사용자가 의도하지 않은 작업을 서버에 수행시키는 공격이다. 서버가 세션 쿠키만 보고 이를 정상 사용자의 의도에 따른 요청으로 받아들이는 점을 노린다. 공격자가 쿠키 값을 직접 알아내거나 훔치는 것이 필수는 아니다. XSS의 핵심은 악성 스크립트 실행이고, CSRF의 핵심은 인증된 사용자의 권한을 이용한 요청 위조이다. S-HTTP는 HTTP 메시지를 보호하기 위한 프로토콜이므로 공격 명칭이 아니다.

따라서 ㉠ Reflected XSS, ㉡ CSRF의 연결은 ①과 일치한다.

NoteBase

문 14. 다음에 설명하는 서명기법을 사용하는 응용보안 프로토콜로 가장 적절한 것은?

사용자의 신용카드 번호와 같은 지불정보는 은행의 공개키로 암호화하여 상점에 숨기고, 주문정보는 상점의 공개키로 암호화하여 은행이 알지 못하도록 하는 서명기법

① PGP(Pretty Good Privacy)

② SET(Secure Electronic Transaction)

③ IPsec(IP Security)

④ Bitcoin

정답 2번

간단한 해설

주문정보와 지불정보를 따로 보호하면서 두 정보가 같은 거래에 속하도록 연결하는 기법은 **SET의 이중서명**이다. 상점과 은행이 서로에게 불필요한 전체 정보를 보지 않고도 거래의 연계를 확인한다.

핵심 풀이

문제의 핵심은 주문정보와 지불정보를 **각 수신자에게 필요한 범위로 나누어 공개**한다는 점이다. 상점에는 주문정보를, 은행 측에는 지불정보를 전달하면서 상대방에게 불필요한 정보는 숨기는 구조이다.

SET: 신용카드 전자결제를 보호하는 프로토콜이며 **이중서명**을 사용한다. 주문정보와 지불정보를 각각 해시한 뒤 두 해시를 결합해 다시 해시한 값에 서명하여, 서로의 전체 내용을 공개하지 않고도 두 정보가 같은 거래에 속함을 확인하게 한다. 암호화는 정보의 비밀성을, 이중서명은 두 정보의 연계와 무결성을 뒷받침한다.

PGP: 전자우편이나 파일의 암호화와 전자서명을 제공한다. 상점과 은행에 주문·지불정보를 나누고 이중서명으로 연결하는 신용카드 결제 프로토콜을 가리키지는 않는다.

IPsec: IP 계층에서 패킷의 인증·무결성·기밀성 등을 보호하는 보안 프로토콜 집합이다. 문제의 주문정보와 지불정보 분리 구조를 식별하는 단서는 아니다.

Bitcoin: 중앙 결제기관 없이 거래를 검증·기록하는 분산형 전자화폐 시스템이다. 은행과 상점이 신용카드 지불정보와 주문정보를 분담하는 SET의 이중서명 구조와 구별된다.

따라서 제시된 서명기법을 사용하는 응용보안 프로토콜은 ② SET이다.

NoteBase

문 15. 웹 보안을 위한 TLS 프로토콜의 핸드셰이크 과정에서 클라이언트와 서버가 Cipher Suite로 TLS_RSA_WITH_AES_128_CBC_SHA256을 채택하였다. 다음 설명 중 가장 적절하지 않은 것은?

① RSA 알고리즘을 이용하여 상호 인증을 수행한다.

② 레코드 프로토콜에서 데이터를 암호화할 때, 128비트 키 AES 알고리즘을 CBC 모드로 사용한다.

③ 사용 중인 AES 알고리즘은 암호명세변경(ChangeCipherSpec) 프로토콜을 통해 변경할 수 있다.

④ 레코드 프로토콜에서 메시지 인증 값은 해시함수 SHA256을 CBC-MAC 방식으로 사용하여 만든다.

정답 4번

간단한 해설

이 암호군에서 CBC는 AES의 암호화 모드이고, SHA256은 **HMAC-SHA256** 메시지 인증을 뜻한다. 암호화 모드와 메시지 인증 방식을 구별해야 한다.

선지별 해설

① X — 이 암호군을 선택했다는 사실만으로 **상호 인증**이 보장되지는 않는다. RSA는 서버의 RSA 인증서에 기초한 키 교환에 사용된다. 클라이언트까지 인증하려면 서버의 인증서 요청과 클라이언트의 인증서·서명 검증 등 별도 절차가 필요하므로, 선지의 표현에는 조건이 빠져 있다.

② O — AES_128_CBC는 데이터를 **128비트 키의 AES**로 암호화하고 CBC 운영 모드를 사용한다는 뜻이다. 여기서 CBC는 메시지 인증 방식이 아니라 데이터 암호화 모드이다.

③ O — 재협상으로 다른 암호 명세를 정한 뒤 ChangeCipherSpec을 보내면, 이후 레코드에 그 명세와 키를 적용할 수 있다는 의미이다. 다만 **ChangeCipherSpec은 이미 협상된 대기 상태를 현재 상태로 적용**하는 메시지이며, 새 알고리즘을 직접 선택하거나 협상하지는 않는다.

④ X — 이 암호군의 메시지 인증 값은 **HMAC-SHA256**으로 만든다. CBC-MAC은 블록 암호의 CBC 연쇄 구조를 이용하는 MAC이므로, SHA256 해시함수를 CBC-MAC 방식으로 사용한다는 설명은 잘못이다. AES의 CBC 암호화 모드와 SHA256을 이용한 HMAC을 혼동하였다.

①의 상호 인증 표현에도 추가 조건이 필요하지만, 이 암호군의 메시지 인증 방식을 직접 잘못 설명한 인정 정답은 ④이다.

NoteBase

문 16. 운영체제의 이중 모드에 대한 설명 중 ㉠과 ㉡에 들어갈 용어로 가장 적절하게 연결된 것은?

운영체제의 구조는 이중 모드(dual mode)로 되어 있는데, 이는 사용자 모드(user mode)와 커널 모드(kernel mode)이다. 이 중 사용자 모드에서 하드웨어 자원을 사용하려고 하면 (㉠)가(이) 발생해서 운영체제에 도움을 요청한다. 또한, 사용자 모드로 실행 중인 프로그램에서 포인터를 사용하여 커널 주소 영역 메모리를 접근하려 하면 (㉡)를(을) 발생시켜 커널 영역을 보호한다.

① 시스템 호출 / 교착상태

② 예외 / 스케줄링

③ 시스템 호출 / 예외

④ 교착상태 / 시스템 호출

정답 3번

간단한 해설

사용자 프로그램이 운영체제에 자원 사용을 요청하는 통로는 **시스템 호출**이고, 허용되지 않은 커널 메모리 접근을 감지했을 때 발생하는 것은 **예외**이다.

빈칸별 해설

㉠ 시스템 호출: 사용자 모드에서는 장치 제어 등 보호된 작업을 직접 수행할 수 없다. 파일 입출력처럼 운영체제의 도움이 필요한 작업은 시스템 호출로 요청하며, 커널이 권한을 확인하고 서비스를 수행한다.

㉡ 예외: 사용자 프로그램이 접근 권한이 없는 커널 주소 영역을 읽거나 쓰려 하면 메모리 보호 위반이 감지되어 예외가 발생한다. 이때 제어가 운영체제의 예외 처리기로 넘어가므로, 프로그램이 커널 메모리를 임의로 변경하는 접근은 허용되지 않는다.

따라서 ㉠은 시스템 호출, ㉡은 예외이므로 ③이다.

NoteBase

문 17. 보안 운영체제의 설계 원리와 이에 대한 설명으로 가장 적절하지 않은 것은?

① 최소권한: 각각의 사용자와 프로그램은 가능한 최소한의 권한을 사용하여 시스템 자원을 사용하여야 한다.

② 허용에 근거한 접근: 접근 검토에 대한 기본 값은 접근 허용이며, 설계자는 접근을 차단하여야 하는 항목의 식별에 주의하여야 한다.

③ 완전한 조정: 직접적인 접근 시도와 접근 통제 메커니즘을 우회하려는 접근 시도를 완전히 검사하여야 한다.

④ 권한분리: 객체에 대한 권한은 두 개 이상의 조건에 의존하여야 한다.

정답 2번

간단한 해설

'허용에 근거한 접근'은 **기본 거부 후 명시적으로 허용**하는 방식이다. 접근 허용을 기본값으로 두고 차단 대상만 찾는다는 설명은 이 원리와 반대이다.

선지별 해설

① O: '최소권한'은 사용자와 프로그램에 **업무 수행에 필요한 최소한의 권한**만 부여하는 원리이다. 불필요한 권한을 줄여 오용이나 프로그램 침해가 다른 자원에 미치는 피해를 제한한다.

② X: '허용에 근거한 접근'은 **기본적으로 접근을 거부**하고, 명시적으로 허용된 조건에 해당할 때만 접근시키는 원리이다. 따라서 설계자는 차단 대상을 빠짐없이 찾는 방식이 아니라 허용할 접근 조건을 식별해야 한다. 선지는 기본 거부와 기본 허용을 반대로 설명했다.

③ O: '완전한 조정'은 **모든 객체 접근에 대해 권한을 검사**하는 원리이다. 정상적인 접근 경로뿐 아니라 우회 경로를 통한 접근도 권한 검사 없이 자원에 도달하지 못하게 해야 한다.

④ O: '권한분리'는 중요한 접근 권한을 **둘 이상의 독립적인 조건**이 충족되어야 행사할 수 있게 하는 원리이다. 하나의 조건이나 단일 권한만으로 보호를 해제하지 않도록 하여, 한 요소의 실패나 오용이 곧바로 전체 접근 허용으로 이어지지 않게 한다.

NoteBase

문 18. BLP(Bell-LaPadula) 보안모델이 가지고 있는 특성과 규칙에 대한 설명으로 가장 적절하지 않은 것은?

① 정보의 불법적인 파괴나 변조를 방지하기 보다 비밀정보의 허가없는 접근을 방지하는 것이 목표이다.

② 강제적 정책에 의한 접근통제를 원할 때에 대한 통제 규칙을 정의한다.

③ 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 높으면 주체는 객체에 쓰기를 할 수 없다.

④ 주체가 객체를 읽기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 낮아야 한다.

정답 4번

간단한 해설

BLP의 읽기 규칙은 **No Read Up**이다. 주체가 객체를 읽으려면 주체의 허가 수준이 객체의 분류 수준보다 낮아야 하는 것이 아니라 **같거나 높아야 한다**.

선지별 해설

① O: BLP는 비밀정보가 허가되지 않은 낮은 보안 수준으로 유출되지 않게 하는 **기밀성** 중심 모델이다. 불법 변경·파괴 방지라는 무결성을 주된 목표로 하는 모델과 구별된다.

② O: 주체의 비밀 취급 허가 수준과 객체의 보안 분류를 비교하여 **강제적 접근통제** 규칙을 적용한다. 소유자의 임의 허가만으로 보안등급 규칙을 무시할 수 없다.

③ O: 기본 별표 속성(*-property)은 **하위 보안 수준으로의 쓰기 금지(No Write Down)**를 요구한다. 높은 등급의 주체가 낮은 등급의 객체에 비밀정보를 기록하면 낮은 등급 사용자에게 정보가 유출될 수 있기 때문이다.

④ X: 단순 보안 속성은 **상위 보안 수준의 읽기 금지(No Read Up)**이다. 따라서 등급에 관한 읽기 조건은 주체의 허가 수준이 객체의 분류 수준과 같거나 높아야 한다는 것이다. 선지의 '낮아야 한다'는 방향이 반대이므로 가장 적절하지 않은 설명은 ④이다.

NoteBase

문 19. 다음과 같은 사례를 방지하기 위한 데이터베이스 보안통제로 가장 적절한 것은?

낮은 비밀 취급 등급자가 레코드 입력 시, 오류를 통하여 자신보다 높은 비밀 취급 등급자가 있다는 사실을 알게 되는 사례

① 접근 통제
② 추론 통제
③ 흐름 통제
④ 무결성 통제

정답 2번

간단한 해설

오류 메시지를 단서로 권한 밖의 사실을 알아내는 것은 추론에 의한 정보 노출이다. 이를 막는 **추론 통제**가 필요하므로 정답은 ②이다.

핵심 풀이

사례의 단서는 높은 등급의 정보를 직접 조회하지 않았는데도 **레코드 입력 오류로 숨겨진 사실을 알아냈다**는 점이다. 허용된 정보나 시스템의 응답을 단서로 권한 밖의 정보를 유추하는 문제가 발생했다.

② 추론 통제는 사용자가 볼 수 있는 정보나 응답으로부터 **접근할 수 없는 정보를 유추하는 것**을 막는 통제이다. 따라서 오류를 통해 높은 비밀 취급 등급자의 존재를 알아내는 사례에 직접 대응한다.

① 접근 통제는 사용자의 권한에 따라 데이터의 조회·입력·수정 등 **직접적인 접근과 연산**을 허용하거나 제한한다. 허용된 연산의 결과에서 비밀을 유추하는 문제와 구별된다.

③ 흐름 통제는 데이터가 보안 등급이나 영역 사이에서 **어느 방향으로 이동할 수 있는지**를 관리한다. 사례의 핵심인 오류 응답에 근거한 추론을 가리키는 명칭은 아니다.

④ 무결성 통제는 데이터의 부당한 변경을 막고 제약 조건 등을 통해 **정확성과 일관성**을 유지한다. 오류를 단서로 비밀이 드러나는 문제는 데이터의 정확성 보장만으로 해결되지 않는다.

따라서 가장 적절한 보안통제는 ② 추론 통제이다.

NoteBase

관련 개념 정리

다중 인스턴스화(polyinstantiation)는 다단계 보안 데이터베이스에서 **같은 키를 가진 레코드를 보안 등급별로 구분**하여 둘 수 있게 하는 기법이다. 예를 들어 높은 등급의 레코드와 키가 같아도 낮은 등급의 레코드 입력을 허용하면, 중복 키 오류로 숨겨진 레코드의 존재를 추론하는 일을 줄일 수 있다. 다만 등급별 레코드의 일관성 관리는 별도로 필요하다.

NoteBase

문 20. 소프트웨어 개발과정에서 소스코드에 존재하는 버퍼 오버플로우에 취약한 함수, 하드 코드된 패스워드 등 잠재적인 취약점을 제거하고, 보안을 고려하여 기능을 구현할 때 지켜야 할 보안활동으로 가장 적절한 것은?

① 안전한 코딩(secure coding)

② 위험분석(risk analysis)

③ 모의 침투(penetration test)

④ 디지털 포렌식(digital forensics)

정답 1번

간단한 해설

소스코드의 잠재적 취약점을 제거하면서 보안을 고려해 기능을 구현하는 활동은 **안전한 코딩**이다. 취약한 함수의 사용과 패스워드의 하드 코딩을 피하는 것이 대표적인 예이다.

개념 구분

안전한 코딩: **소스코드를 작성·수정하는 단계에서 보안 약점을 예방하고 제거**하는 활동이다. 버퍼의 크기를 넘는 입력을 처리하는 취약한 함수를 안전하게 대체하거나 입력 길이를 검사하고, 패스워드를 코드에 직접 넣지 않도록 구현하는 것이 해당한다.

위험분석: 자산에 대한 위협과 취약점을 파악하고 **발생 가능성과 피해 영향을 평가**하여 대응 우선순위를 정하는 활동이다. 위험의 크기를 판단하는 것이 중심이므로, 보안을 고려한 코드 구현 자체를 가리키는 명칭과 구별된다.

모의 침투: 허용된 범위에서 실제 공격을 모방하여 **취약점의 악용 가능성과 보안 통제의 효과를 시험**하는 활동이다. 구현된 시스템의 방어 수준을 시험하는 것이 중심이며, 소스코드 작성 때 준수하는 보안활동의 명칭은 아니다.

디지털 포렌식: 디지털 정보를 **무결성을 유지하면서 수집·보존·분석**하여 사실관계나 증거를 확인하는 활동이다. 소스코드의 잠재적 보안 약점을 예방하는 구현 활동과 목적이 다르다.

따라서 제시된 활동에 해당하는 것은 ① 안전한 코딩이다.

NoteBase