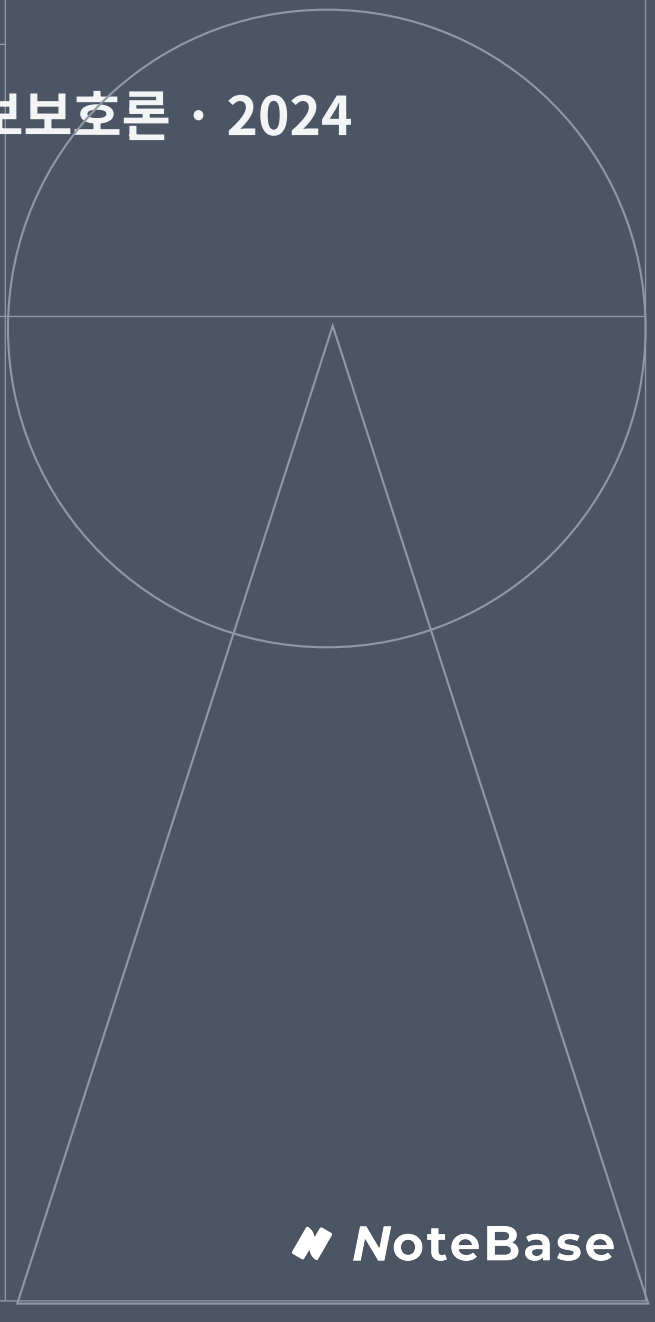
기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2024



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2024

공무원/경찰/경력채용 · 정보보호론 · 2024

문 1. 리눅스(Linux) 시스템 명령어에 관한 설명으로 가장 적절하지 않은 것은?

① su 명령으로 다른 계정의 사용자로 전환할 수 있다.

② sudo 명령으로 root 권한의 명령어를 수행할 수 있다.

③ pwd 명령으로 패스워드를 변경할 수 있다.

④ apt list 명령으로 패키지 목록을 출력할 수 있다.

정답 3번

간단한 해설

'pwd'는 **현재 작업 디렉터리의 경로**를 출력하는 명령이다. 패스워드를 변경하려면 **'passwd'**를 사용한다.

선지별 해설

① O: 'su'는 인증 및 계정 정책에 따라 다른 사용자의 권한으로 셸이나 명령을 실행하는 명령이다. 사용자 이름을 지정하면 **그 계정의 사용자로 전환**할 수 있으며, 사용자 이름을 생략하면 기본 대상은 root이다.

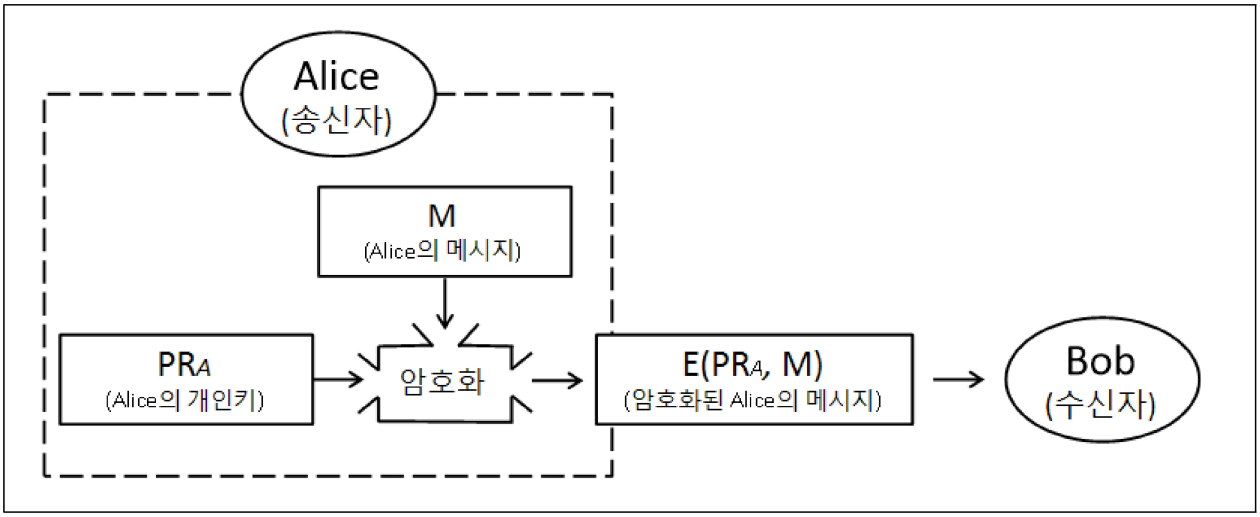
② O: 'sudo'는 보안 정책에서 허용한 사용자가 다른 사용자의 권한으로 명령을 실행하게 한다. 기본 실행 대상은 root이므로 **허용된 범위에서 root 권한의 명령**을 수행할 수 있다. 모든 사용자가 아무 명령이나 관리자 권한으로 실행할 수 있다는 뜻은 아니다.

③ X: 'pwd'는 'print working directory'의 약자로, **현재 작업 디렉터리의 경로를 출력**한다. 패스워드 변경에 사용하는 명령은 **'passwd'**이다.

④ O: 'apt list'는 APT 패키지 관리 도구에서 패키지 목록을 출력한다. Debian·Ubuntu와 같이 APT를 사용하는 환경에서 이용하며, 'apt list --installed'는 **설치된 패키지만** 추려서 보여 준다.

NoteBase

문 2. 다음 그림은 Alice가 자신의 개인키로 메시지를 암호화하여 Bob에게 암호문을 전송하는 과정이다. 그림에서 제공될 수 있는 보안 서비스로 가장 적절한 것은?



① 기밀성, 인증

② 인증, 부인방지

③ 기밀성, 부인방지

④ 무결성, 가용성

정답 2번

간단한 해설

송신자 Alice의 개인키를 사용하는 것은 전자서명의 취지로, 대응하는 공개키를 통해 **송신자를 확인**하고 **서명 사실의 부인을 어렵게** 한다. 공개키로 확인할 수 있는 방식이므로 수신자만 내용을 읽게 하는 기밀성을 보장하는 것은 아니다.

NoteBase

도식 해설

그림에서 Alice의 메시지 M과 **Alice 자신의 개인키**가 '암호화' 상자로 들어가고, 처리 결과가 오른쪽의 Bob에게 전달된다. 수신자인 Bob의 공개키를 사용한 그림이 아니라 송신자의 개인키를 사용한 그림이라는 점이 판단 기준이다.

이 도식은 송신자 개인키로 만든 결과를 대응하는 송신자 공개키로 확인하는 **전자서명의 원리**를 단순화한 것이다. 실제 안전한 전자서명에서는 정해진 해시·인코딩·서명 및 검증 절차를 사용하므로, 메시지에 개인키 연산만 하면 곧바로 안전한 서명이 완성된다는 뜻은 아니다.

인증: Bob이 신뢰할 수 있는 Alice의 공개키로 서명을 검증하면, 해당 메시지가 Alice의 개인키로 서명되었는지 확인할 수 있다. 개인키가 Alice에게만 안전하게 관리되고 공개키와 Alice의 신원이 올바르게 연결되어 있다는 전제에서 **송신자 인증**을 제공한다.

부인방지: Bob은 유효한 서명을 제3자에게 제시하여 Alice가 서명했다는 증거로 사용할 수 있다. 개인키 보호와 신원 연결 등 적절한 조건이 갖춰진 전자서명은 **서명 사실의 사후 부인을 어렵게** 한다. 어떤 상황에서도 부인이 절대 불가능하다는 뜻은 아니다.

기밀성·가용성과의 구별: Alice의 공개키는 공개되는 키이므로 그림처럼 송신자의 개인키를 사용한 처리는 Bob만 내용을 알게 하는 기밀성을 보장하지 않는다. 기밀성을 얻으려면 수신자만 복호화할 수 있는 별도의 암호화 방식이 필요하다. 전자서명은 변조 탐지를 통한 무결성도 제공할 수 있지만, 통신망이나 서비스의 지속적인 사용 가능성을 뜻하는 가용성을 보장하지는 않는다.

①과 ③은 기밀성을, ④는 가용성을 포함하므로 해당하지 않는다. 제공될 수 있는 서비스를 모두 바르게 짝지은 것은 ② 인증, 부인방지이다.

NoteBase

문 3. MAC(Message Authentication Code)에 관한 설명으로 가장 적절하지 않은 것은?

① 메시지의 손상 및 변경 여부를 확인할 수 있는 무결성 서비스를 제공한다.

② 수신자가 받은 메시지를 부인하지 못하도록 부인방지 서비스를 제공한다.

③ 키에 의존하는 일방향 해시함수(hash function)를 사용한다.

④ 송·수신자간에 비밀키가 공유되어야 한다.

정답 2번

간단한 해설

MAC은 송신자와 수신자가 같은 비밀키를 사용해 양쪽 모두 인증값을 만들 수 있으므로 **부인방지를 제공하지 않는다**. 메시지의 무결성과 인증을 확인하는 기능과 수신 사실을 제3자에게 증명하는 기능은 구별된다.

선지별 해설

① O: 송신자는 메시지와 비밀키로 MAC 값을 만들고, 수신자는 같은 키로 계산한 값과 전달받은 MAC 값을 비교한다. 메시지가 손상되거나 변경되면 검증이 실패하므로 **메시지 무결성**을 확인할 수 있다. 이는 메시지 내용을 숨기는 암호화와는 다른 기능이다.

② X: MAC은 **송신자와 수신자가 같은 비밀키를 공유**하므로 양쪽 모두 유효한 MAC 값을 만들 수 있다. 따라서 MAC만으로 제3자에게 누가 만들었는지 확정하거나 수신 사실을 부인하지 못하게 할 수 없다. MAC의 기본 서비스는 무결성과 메시지 인증이며, 수신 부인방지에는 수신자가 서명한 수신 확인 등 별도의 증거 체계가 필요하다.

③ O: 메시지와 비밀키를 이용하여 일정 길이의 인증값을 산출한다는 의미에서 MAC을 키에 의존하는 해시 기능으로 설명할 수 있다. 인증값에서 원래 메시지를 복원하는 방식은 아니다. 다만 이를 모든 MAC이 SHA 계열 등의 해시 알고리즘으로 구현된다는 뜻으로 읽어서는 안 된다. **HMAC은 해시함수 기반**이고 **CMAC은 블록 암호 기반**의 구현이다.

④ O: MAC 생성자와 검증자는 동일한 비밀키를 공유해야 한다. 송신자가 사용한 키와 다른 키로 계산하면 정상적인 인증값을 검증할 수 없으므로, 키의 안전한 공유와 비밀 유지가 전제된다.

NoteBase

문 4. TKIP(Temporal Key Integrity Protocol)에 관한 설명으로 가장 적절하지 않은 것은?

① WEP의 보안상 문제점을 개선하였다.

② 순서 규칙이 있는 24bit 초기벡터를 사용하여 키 재사용과 재생 공격을 방지한다.

③ 메시지 무결성 보장을 위해 MIC(Message Integrity Check) 알고리즘을 사용한다.

④ IEEE 802.11i의 무선 네트워킹 표준으로 사용되는 보안 프로토콜이다.

정답 2번

간단한 해설

TKIP의 순서 카운터는 **24비트가 아니라 48비트**이다. 24비트는 WEP의 초기벡터 길이이므로, 가장 적절하지 않은 설명은 ②이다.

선지별 해설

① O: TKIP는 기존 WEP 장비와의 호환성을 고려하면서 **WEP의 취약점을 보완**한 프로토콜이다. 패킷별 키 혼합, 순서 번호를 이용한 재생 방지, 메시지 무결성 검사를 추가하였다.

② X: TKIP는 **48비트의 TKIP 순서 카운터(TSC)**를 사용한다. 24비트는 WEP의 초기벡터 길이이므로 선지의 수치를 48비트로 고쳐야 한다. TKIP는 증가하는 TSC와 패킷별 키 혼합을 통해 키스트림 재사용 문제를 줄이고, 수신 측의 순서 검사로 이미 받은 패킷의 재생을 차단한다. 따라서 가장 적절하지 않은 설명은 ②이다.

③ O: TKIP는 **Michael 알고리즘으로 MIC를 계산**하여 메시지 변조 여부를 확인한다. 수신 측이 다시 계산한 MIC와 전달받은 값을 비교하는 방식으로, WEP의 CRC 기반 검사보다 강화된 무결성 보호를 제공한다.

④ O: TKIP는 **IEEE 802.11i에 포함된 무선 보안 프로토콜**이다. 기존 WEP 하드웨어의 활용을 고려한 보완 방식이며, 같은 표준의 AES 기반 CCMP와 구별된다. 표준에 포함된 기술이라는 설명이지 현재 새 무선망에 권장되는 최신 방식이라는 뜻은 아니다.

NoteBase

문 5. 다음은 IPSec(IP Security Protocol)의 AH/ESP 프로토콜 서비스에 관한 기능별 지원 여부(O, X)를 나타낸 표이다. ㉠~㉣에 해당하는 것으로 가장 적절하게 짝지어진 것은?

기능	AH	ESP
기밀성	㉠	O
인증	O	㉡
무결성	O	㉢
재전송 공격 방지	㉣	O

① ㉠ (X) ㉡ (O) ㉢ (O) ㉣ (X)

② ㉠ (O) ㉡ (O) ㉢ (X) ㉣ (X)

③ ㉠ (O) ㉡ (X) ㉢ (X) ㉣ (O)

④ ㉠ (X) ㉡ (O) ㉢ (O) ㉣ (O)

정답 4번

간단한 해설

AH는 인증·무결성·재전송 공격 방지를 지원하지만 **기밀성은 제공하지 않는다**. ESP는 암호화에 더해 **인증과 무결성**도 지원한다.

NoteBase

빈칸별 해설

표는 각 프로토콜이 지원할 수 있는 보안 서비스를 비교한다. O는 모든 연결에서 해당 기능이 반드시 활성화된다는 뜻이 아니며, 실제 서비스는 보안연관(SA)의 설정과 수신 측 처리에 따라 달라진다.

㉠ X: AH는 데이터 출처 인증과 무결성을 제공하지만, 데이터를 암호화하여 숨기는 **기밀성은 제공하지 않는다**. 따라서 기밀성 행에서 AH는 X이고, 암호화를 지원하는 ESP는 O이다.

㉡ O: ESP는 암호화뿐 아니라 **데이터 출처 인증**도 지원한다. 인증·무결성 보호에 사용하는 키와 통신 상대의 관계를 바탕으로, 수신한 데이터가 해당 상대에게서 왔는지 확인한다. 인증 기능이 AH에만 있는 것은 아니다.

㉢ O: ESP는 보호 대상 데이터가 전송 중 부당하게 변경되었는지 확인하는 **무결성 보호**를 지원한다. 이는 암호화로 내용을 숨기는 기밀성과 다른 기능이며, ESP의 인증·무결성 서비스를 사용해 제공한다.

㉣ O: AH는 **순서번호와 재전송 방지 윈도**를 이용한 재전송 공격 방지를 지원한다. 수신 측이 순서번호를 검사하여 이미 받은 패킷의 중복 수신 등을 거부한다. ESP도 이 기능을 지원하므로 재전송 공격 방지 행은 두 프로토콜 모두 O이다.

㉠ X, ㉡ O, ㉢ O, ㉣ O이므로 ④와 일치한다.

NoteBase

문 6. 다음은 국내 암호 알고리즘에 관한 설명이다. ㉠, ㉡에 들어갈 내용으로 가장 적절한 것은?

(㉠)는 국내 암호 알고리즘으로 미국표준 블록 암호인 AES와 동일한 입출력과 키 크기를 가지며, ISPN(Involutional SPN) 구조의 (㉡)비트 블록 암호로 3종류(128비트, 192비트, 256비트)의 키를 제공한다.

① ㉠: ARIA, ㉡: 128
② ㉠: LEA, ㉡: 64
③ ㉠: SEED, ㉡: 128
④ ㉠: HIGHT, ㉡: 64

정답 1번

간단한 해설

ISPN 구조를 사용하는 국산 블록 암호는 ARIA이다. 블록 크기는 128비트로 고정되며, 키 길이는 AES와 같이 128·192·256비트 중에서 선택한다.

빈칸별 해설

㉠ ARIA: 지문의 결정적 단서는 **ISPN(Involutional SPN) 구조**이다. ARIA는 이 구조를 사용하는 국산 블록 암호이며 128·192·256비트 키를 지원한다. LEA도 같은 세 가지 키 길이를 지원하지만 ARX 기반 구조이고, SEED는 Feistel 구조이므로 지문의 구조 조건과 다르다.

㉡ 128: ARIA가 한 번에 처리하는 평문 블록과 출력하는 암호문 블록의 크기는 모두 128비트이다. **블록 크기는 고정되고 키 길이는 선택된다**는 점을 구별해야 한다. 따라서 키가 192비트나 256비트여도 블록 크기는 128비트이며, 이는 AES의 입출력·키 길이 규격과 같다. HIGHT의 블록 크기는 64비트이고, LEA의 블록 크기는 128비트이므로 LEA를 64비트와 짝지은 조합도 맞지 않는다.

따라서 ㉠ ARIA, ㉡ 128로 짝지은 ①이 정답이다.

NoteBase

문 7. 유닉스(Unix)/리눅스(Linux) 시스템의 utmp 로그 파일에 관한 설명으로 가장 적절하지 않은 것은?

① binary 형태로 로깅 정보를 저장한다.

② 현재 시스템에 로그인한 사용자의 상태를 로깅한다.

③ cat, who, users, whodo 등의 명령으로 로그 정보를 확인할 수 있다.

④ w 명령으로 로그인된 사용자 계정과 로그인 시간, 실행 중인 프로세스의 종류를 확인할 수 있다.

정답 3번

간단한 해설

utmp는 바이너리 형식이므로 **cat의 단순 출력으로 로그인 기록을 해석할 수 없다**. who, users 등 형식을 이해하는 명령을 이용해야 하므로 ③이 정답이다.

선지별 해설

① O: utmp는 사용자 이름, 터미널, 로그인 시각 등의 정보를 구조화된 **바이너리 레코드**로 저장한다. 일반 텍스트 로그처럼 줄 단위의 문자열로 저장되는 파일은 아니다.

② O: utmp는 **현재 로그인한 사용자와 세션의 상태**를 파악하는 데 쓰인다. 과거의 로그인·로그아웃 이력을 계속 누적하는 wtmp와 구별한다.

③ X: cat은 파일의 바이트를 그대로 출력할 뿐, **utmp 레코드의 필드를 해석하지 않는다**. 따라서 cat을 일반적인 로그인 정보 확인 명령과 함께 제시한 부분이 부적절하다. 현재 로그인 사용자는 who나 users처럼 해당 형식을 해석하는 명령으로 확인한다. whodo도 이를 지원하는 유닉스에서 사용할 수 있지만, 모든 리눅스에 공통으로 설치되는 명령은 아니다.

④ O: w는 로그인 사용자, 로그인 시각, 현재 수행 중인 작업의 명령 등을 보여 준다. 이때 **로그인 정보와 프로세스 정보를 함께 조회**하므로, 실행 중인 작업에 관한 정보까지 모두 utmp에 저장된다는 뜻은 아니다. 전통적인 utmp 기반 시스템에서는 utmp와 프로세스 정보를 함께 이용하며, 실제 정보원은 운영체제와 구현에 따라 달라질 수 있다.

바이너리 로그인 기록을 cat으로 해석하여 확인할 수 있다는 ③이 가장 적절하지 않다.

NoteBase

문 8. 윈도우(Windows) 파일시스템에 관한 설명으로 가장 적절하지 않은 것은?

① NTFS가 FAT보다 높은 호환성과 보안성을 제공한다.

② FAT가 NTFS보다 저용량 볼륨에서 속도가 빠르다.

③ NTFS는 파일 접근 감사 기능을 제공한다.

④ FAT를 NTFS로 변환할 수 있다.

정답 1번

간단한 해설

NTFS는 접근 권한과 감사 기능 등으로 **보안성**이 높다. 여러 운영체제와 기기에서 폭넓게 사용할 수 있는 **호환성은 일반적으로 FAT 계열이 높다**.

선지별 해설

① X: NTFS는 파일·폴더의 접근 권한 설정과 감사 등으로 FAT보다 높은 보안성을 제공한다. 그러나 다양한 운영체제·기기 사이의 호환성은 일반적으로 **FAT 계열이 더 높다**. 따라서 NTFS가 보안성과 호환성 모두에서 우수하다고 묶은 설명은 적절하지 않다.

② O: FAT는 구조가 단순하고 파일시스템 관리에 필요한 **부가 부담이 작아** 저용량 볼륨에서 유리하다는 전통적인 비교이다. NTFS는 보안·복구 등을 위한 관리 정보를 유지하므로 작은 볼륨에서는 그 부담이 상대적으로 커질 수 있다. 다만 실제 속도는 저장장치, 파일 크기·개수, 작업 방식에도 좌우되므로 모든 저용량 환경에서 FAT가 반드시 빠르다는 성능 보장은 아니다.

③ O: NTFS는 파일이나 폴더에 대한 **접근 시도를 감사 기록으로 남기는 기능**을 지원한다. 감사 정책을 활성화하고 해당 파일·폴더의 감사 대상을 설정하면, 지정된 접근의 성공 또는 실패를 보안 로그에서 확인할 수 있다. 접근 권한을 허용·거부하는 기능과 접근 이력을 기록하는 감사 기능은 구별된다.

④ O: Windows의 'convert' 명령은 **FAT 또는 FAT32 볼륨을 NTFS로 변환**할 수 있으며, 기존 파일과 디렉터리를 유지하도록 설계되어 있다. 이는 파일시스템 변환 기능에 관한 설명이고, 같은 명령으로 NTFS를 FAT로 역변환하는 기능까지 제공한다는 뜻은 아니다.

NoteBase

문 9. 블록체인(Blockchain)에 관한 설명으로 가장 적절하지 않은 것은?

① 분산 컴퓨팅 기술 기반의 P2P 방식으로 서비스된다.

② 주식 및 부동산 등의 거래에 적용 가능하다.

③ 기술적 특성으로 투명성, 불변성, 기밀성, 중앙화가 있다.

④ 하이퍼레저 패브릭(hyperledger fabric)은 공개키 인증서를 이용하여 피어(peer)에 관한 신원 정보를 제공한다.

정답 3번

간단한 해설

블록체인의 기본 특성은 분산된 원장의 공유와 변조 저항성이다. **중앙화는 일반적인 핵심 특성이 아니며, 기밀성도 자동 보장되지 않으므로** ③이 정답이다.

선지별 해설

① O: 블록체인은 여러 노드가 원장 사본을 나누어 보관하고 거래·블록을 전파하는 **P2P 기반의 분산 구조**를 이용한다. 노드들은 정해진 검증·합의 규칙에 따라 원장을 갱신한다.

② O: 거래 기록과 자산의 이전 내역을 공동으로 관리할 수 있으므로 **주식·부동산 등 다양한 자산 거래**에도 적용할 수 있다. 예를 들어 주식의 발행·이전 기록이나 부동산 거래 절차의 진행 내역을 공유하는 데 이용할 수 있으며, 암호화폐에만 한정되지 않는다.

③ X: 원장을 공유하여 검증하는 투명성과 과거 기록의 변경을 어렵게 하는 불변성은 대표적인 특성이지만, **기밀성이 자동으로 보장되지는 않는다**. 공개형 원장의 거래 내용은 공개될 수 있으므로 비밀 유지에는 암호화·접근 통제 등 별도의 장치가 필요하다. 또한 일반적인 핵심 구조는 중앙화가 아니라 **분산·탈중앙화**이다. 허가형에서는 운영 주체의 통제가 강할 수 있고, 불변성도 어떤 공격에도 변경이 절대 불가능하다는 뜻이 아니라 정상적인 합의 운영 아래 변조를 탐지·억제한다는 의미이다.

④ O: 하이퍼레저 패브릭은 기본적으로 **X.509 공개키 인증서로 피어의 신원을 나타낸다**. 인증서에 담긴 신원과 공개키를 바탕으로 서명을 검증하고, 멤버십 서비스 제공자(MSP)의 신뢰 규칙과 정책에 따라 소속 조직·역할 및 권한을 판단한다.

기밀성의 자동 보장과 중앙화를 일반적인 특성으로 묶은 ③이 가장 적절하지 않다.

NoteBase

문 10. x.509 인증서에 관한 설명으로 가장 적절하지 않은 것은?

① 인증서의 발행과 폐기는 인증기관(CA)에서 수행한다.

② x.509 인증서는 SSL, SET, S/MIME과 같은 네트워크 보안 응용에 널리 사용되고 있다.

③ 인증서 정책(certificate policies)은 x.509 인증서 v3의 확장(extensions) 영역에 포함된다.

④ 서명 알고리즘 식별자(signature algorithm ID), 발행자 이름(issuer name), 발행자 유일 식별자(issuer unique identifier)는 필수항목에 포함된다.

정답 4번

간단한 해설

발행자 유일 식별자(issuerUniqueID)는 필수 항목이 아니다. 서명 알고리즘 식별자와 발행자 이름을 이 선택 항목과 함께 묶어 모두 필수라고 한 것이 잘못이다.

선지별 해설

① O: CA는 주체의 신원과 공개키의 연결을 인증서로 발행하고 서명하며, 발행한 인증서의 폐지 상태를 관리한다. 개인키 유출 등으로 더 이상 신뢰할 수 없으면 유효기간이 남아 있어도 폐지한다. 여기서 폐기는 파일 삭제가 아니라 **인증서의 효력을 중단하는 폐지**를 뜻한다.

② O: X.509는 공개키 인증서의 형식으로, SSL 계열의 통신 상대 인증, SET의 전자거래 참여자 인증, S/MIME의 전자우편 보안 등에 활용되어 왔다. 이 선지는 이러한 **인증서 활용 분야**를 설명한 것이다. 과거 응용인 SSL·SET까지 열거한 표현을 현재의 보급률이나 도입 권고로 해석하지는 않는다.

③ O: certificate policies는 인증서에 적용되는 정책을 식별하는 정보를 담는 **v3 확장 항목**이다. 정책 식별자(OID)와 선택적 부가 설명 등을 담아 발행 정책과 사용 목적 판단에 활용한다.

④ X: 서명 알고리즘 식별자와 발행자 이름은 기본 필수 필드이지만, **발행자 유일 식별자는 선택 항목**이다. issuerUniqueID는 X.509 v2·v3에서 사용할 수 있도록 정의된 항목이므로 세 항목 모두 필수라는 설명은 틀리다. 발행자 이름(issuer)과 발행자 유일 식별자(issuerUniqueID)를 구별해야 한다.

따라서 가장 적절하지 않은 설명은 ④이다.

NoteBase

문 11. 소인수분해 문제 기반으로 합성수 모듈러에 관해 제곱근을 찾기 어렵다는 사실로부터 안정성을 얻는 암호시스템으로 가장 적절한 것은?

① ECC

② KCDSA

③ ElGamal

④ Rabin

정답 4번

간단한 해설

Rabin 암호는 합성수를 법으로 하는 제곱 연산을 사용하며, 이를 거꾸로 푸는 **모듈러 제곱근 추출의 어려움**을 이용한다. 이 문제는 합성수의 소인수분해 문제와 밀접하게 연결된다.

핵심 풀이

발문의 핵심 단서는 **합성수를 법으로 하는 제곱근 추출**이다. Rabin 암호의 기본 연산은 서로 다른 큰 소수 p, q의 곱 $n = pq$를 공개하고, 메시지 m을 c≡ m^2±od n으로 바꾸는 것이다. 이를 역으로 풀려면 c의 모듈러 제곱근을 찾아야 하며, 비밀 정보인 p와 q를 알면 그 계산이 가능해진다. 일반적인 모듈러 제곱근 추출과 소인수분해 사이의 계산상 연결이 안전성 근거가 된다.

ECC는 **타원곡선 위의 이산대수 문제**를 이용하는 공개키 암호 기술이다. 합성수의 제곱근을 구하는 문제와 구별된다.

KCDSA는 **이산대수 문제 기반의 전자서명 알고리즘**이다. 메시지의 서명·검증에 쓰이며, 합성수 모듈러 제곱근 추출을 기반으로 하는 방식이 아니다.

ElGamal은 이산대수 문제를 토대로 하는 공개키 암호 계열이다. 기본 방식은 유한체의 곱셈군에서 거듭제곱 연산을 이용하므로, 발문의 소인수분해·제곱근 단서에 해당하지 않는다.

따라서 합성수 모듈러 제곱근 추출을 핵심으로 하는 암호시스템은 ④ Rabin이다.

NoteBase

문 12. 접근통제 단계에 관한 설명으로 가장 적절하지 않은 것은?

① 식별은 패스워드, 메모리카드 등을 접근 매체로 사용한다.

② 인증은 토큰, 스마트카드 등을 접근 매체로 사용한다.

③ 인가는 접근제어목록(ACL) 등을 사용한다.

④ 인증은 주체의 신원을 검증하기 위한 사용증명 활동이다.

정답 1번

간단한 해설

식별은 사용자 ID 등으로 **신원을 제시**하는 단계이고, 인증은 그 신원이 정당한지 **증거로 검증**하는 단계이다. 패스워드나 인증정보가 담긴 카드는 인증 수단이다.

선지별 해설

① X: 식별은 사용자 ID나 계정명 등을 제시하여 **자신이 누구인지 알리는 단계**이다. 패스워드는 그 신원을 증명하는 지식 기반 인증 수단이고, 인증정보를 담은 메모리카드는 소유 기반 인증 수단으로 활용된다. 선지의 수단은 식별과 구별되는 인증에 해당한다.

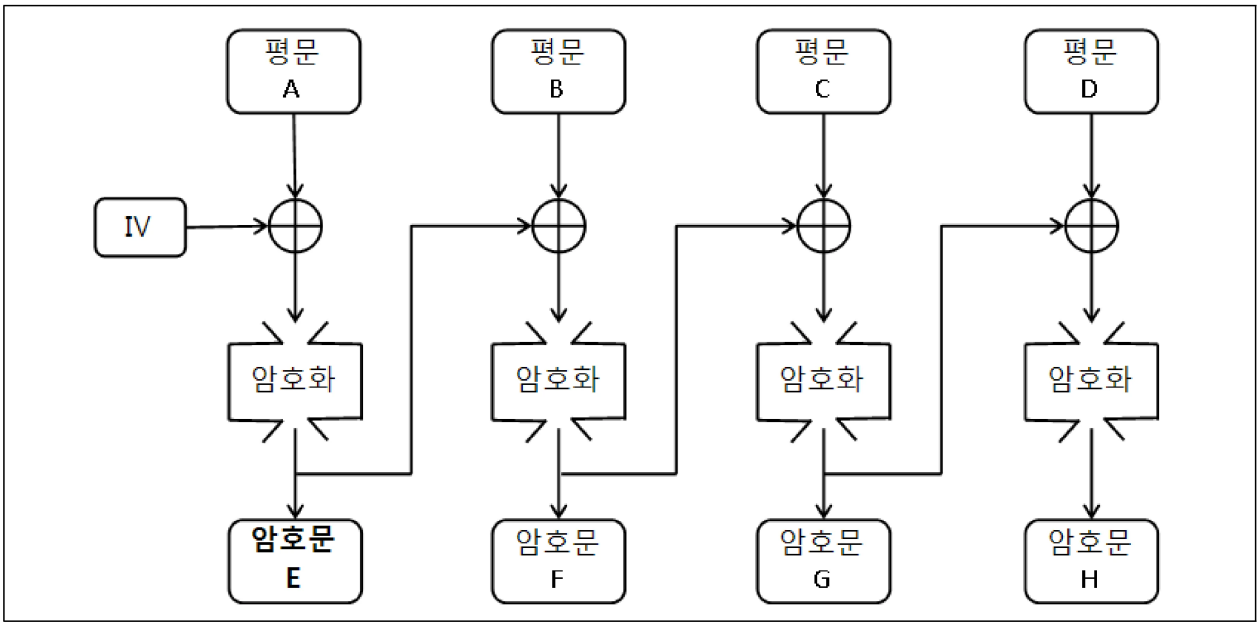
② O: 토큰이나 스마트카드는 사용자가 **소유한 것**을 이용하는 인증 수단이다. 토큰이 생성한 일회용 값이나 스마트카드의 인증정보 등을 검증하여 주장한 신원이 정당한지 확인한다. 단순히 사용자 ID를 입력하는 식별과 구별된다.

③ O: 인가는 인증된 주체가 **어떤 자원에 어떤 행위를 할 수 있는지** 결정하는 단계이다. 접근제어목록(ACL)은 객체에 대해 사용자·그룹별 읽기, 쓰기 등의 허용·거부 권한을 기록하므로 인가 판단에 사용할 수 있다.

④ O: 인증은 주체가 제시한 신원이 정당한지 **증거를 통해 검증**하는 활동이다. 패스워드, 소유한 인증 장치, 생체정보 등이 이러한 증거가 될 수 있다. 인증에 성공했다고 모든 자원의 접근 권한까지 자동으로 부여되는 것은 아니며, 허용 범위는 인가에서 정한다.

NoteBase

문 13. 다음 그림은 특정한 블록 암호 운영 모드에 관한 암호화 과정이다. 복호화 과정에서 암호문 E에 오류가 발생할 때 영향을 미치는 평문은 모두 몇 개인가? (단, 암호문 길이가 바뀌지 않았다고 가정한다. IV는 초기벡터, ⊕는 XOR 연산을 나타낸다.)



① 1개

② 2개

③ 3개

④ 4개

정답 2번

간단한 해설

그림은 CBC 모드이다. 암호문 E의 오류는 E를 직접 복호화하는 A와 E를 XOR에 사용하는 B에만 영향을 주므로, **A·B 두 블록**이 변하는 ②가 정답이다.

NoteBase

계산 과정

모드 판별: 그림은 첫 평문 A를 IV와 XOR한 뒤 암호화하고, 이후에는 이전 암호문을 다음 평문과 XOR한 뒤 암호화한다. 따라서 **이전 암호문을 연결하는 CBC 모드**이다.

복호화 관계: 키 K의 블록 복호화 함수를 Dec_K라고 하자. CBC는 현재 암호문을 복호화한 값에 **직전 암호문을 XOR**하여 평문을 얻는다. 그림의 기호로 쓰면 $A = \mathrm{Dec}_K(E) \oplus IV$, $B = \mathrm{Dec}_K(F) \oplus E$, $C = \mathrm{Dec}_K(G) \oplus F$, $D = \mathrm{Dec}_K(H) \oplus G$이다.

평문 A의 영향: 오류로 원래와 달라진 암호문을 E'라고 하면 $A' = \mathrm{Dec}_K(E') \oplus IV$이다. **블록 복호화 함수의 입력 자체가 바뀌므로** A가 달라진다. 오류가 원래 바뀐 비트 위치에만 한정되는 것은 아니지만, 모든 비트가 반드시 뒤집힌다는 뜻도 아니다.

평문 B의 영향: $B' = \mathrm{Dec}_K(F) \oplus E'$이므로 정상 평문과의 차이는 $B' \oplus B = E' \oplus E$이다. 즉, B에서는 **E의 오류와 같은 위치의 비트**가 바뀐다.

평문 C·D의 영향: C는 G와 F, D는 H와 G를 이용하므로 오류가 난 E를 입력으로 사용하지 않는다. 암호문 길이가 바뀌지 않고 E 이외의 암호문이 정상이라는 조건에서 두 블록은 영향받지 않는다. 복호화에는 앞서 복원한 평문 B가 아니라 수신한 암호문 F가 사용되므로 오류가 계속 전파되지 않는다.

영향을 받는 평문은 A와 B이므로 모두 **2개 블록**이며, 정답은 ②이다.

NoteBase

문 14. 다음에서 설명하는 용어로 가장 적절한 것은?

용량이 정해진 것에 전체 이득이 최대가 되도록 집어넣을 물건들을 결정하는 문제로 이 아이디어는 공개키 암호시스템을 만드는 토대가 되었다.

① 소인수분해 문제
② 이산대수 문제
③ 배낭 문제
④ 중국인의 나머지 정리

정답 3번

간단한 해설

용량 제한 안에서 이득이 최대가 되는 물건 조합을 고르는 것은 배낭 문제이다. 이 아이디어가 배낭 기반 공개키 암호 설계에도 활용되었으므로 정답은 ③이다.

핵심 풀이

핵심 단서: **정해진 용량 안에서 전체 이득을 최대화**하도록 물건을 고르는 문제는 **③ 배낭 문제**이다. 각 물건의 무게와 가치를 고려하여 용량 제한을 넘지 않는 조합 중 가치의 합이 가장 큰 조합을 찾는다.

공개키 암호와의 연결: 배낭 문제의 아이디어는 Merkle–Hellman 배낭 암호와 같은 공개키 암호 설계에 활용되었다. 암호에서는 주어진 수들 중 일부를 골라 특정 합을 만드는 **부분집합 합 문제** 형태를 이용한다. 지문의 이득 최대화라는 최적화 표현과 암호의 부분집합 합 표현은 구별하되, 둘 다 배낭 문제 계열이라는 점이 연결 단서이다.

소인수분해 문제와 이산대수 문제: 소인수분해는 주어진 합성수를 소수들의 곱으로 분해하는 문제이다. 이산대수는 유한군에서 밑과 거듭제곱 결과가 주어졌을 때 그 지수를 구하는 문제이다. 두 문제 모두 공개키 암호와 관련이 있지만, **용량 안에 넣을 물건을 선택**한다는 지문의 정의에는 해당하지 않는다.

중국인의 나머지 정리: 서로소인 여러 법에 대한 나머지 조건으로부터 그 조건들을 동시에 만족하는 수를 결합해 구할 수 있다는 정리이다. 여러 합동식을 함께 다루는 원리이므로, 제한된 용량에서 이득을 최대화하는 물건 선택 문제와 구별된다.

NoteBase

문 15. 해시함수(hash function)에 관한 설명으로 가장 적절하지 않은 것은?

① 임의의 길이 메시지로부터 고정길이의 해시값을 계산한다.

② 해시 결과값으로 입력값을 계산하는 것이 불가능하다.

③ 강한 충돌 내성(충돌저항성)을 위협하는 공격은 전사적 공격(brute force attack)이다.

④ SHA-1이 강한 충돌 내성(충돌저항성)이 깨져 SHA-3으로 대체되었다.

정답 3번

출제 포인트

암호학적 해시함수의 기본 성질과 역상 공격·충돌 공격의 차이를 구분하는 문제이다.

핵심 개념

해시함수는 길이가 다양한 메시지를 일정한 길이의 요약값으로 바꾸는 함수이다. 암호학적 해시함수에는 역상 저항성과 충돌 저항성 등이 요구된다.
역상 저항성은 주어진 해시값에 대응하는 입력을 찾기가 계산적으로 어렵다는 성질이다.
약한 충돌 내성은 주어진 메시지와 해시값이 같은 다른 메시지를 찾기가 어렵다는 성질이다.
강한 충돌 내성은 동일한 해시값을 갖는 서로 다른 메시지 두 개를 자유롭게 찾아내기가 어렵다는 성질이다.

선지별 해설

O/X는 이 문항에서의 선지 적절성 판단이다.
① O: 일반적인 해시함수는 입력 메시지의 길이가 달라도 선택한 알고리즘에 정해진 길이의 해시값을 출력한다.
② O: 역상 저항성을 설명한다. 여기서 “불가능하다”는 수학적으로 입력 후보가 존재하지 않는다는 뜻이 아니라, 주어진 해시값에 대응하는 입력을 현실적인 계산량으로 찾아내기 어렵다는 뜻이다. 해시는 암호문을 복호화하듯 원문을 되돌리는 함수가 아니다.
③ X: 강한 충돌 내성의 대표적인 일반 공격을 단순히 “전사적 공격”으로 설명한 점이 공격 방식의 구분을 묻는 취지에서 가장 적절하지 않다. 정확하게는 “강한 충돌 내성의 대표적인 일반 공격은 생일 공격이다”라고 설명한다. 생일 공격은 여러 입력의 해시값을 계산하고 그 값들 사이에서 일치하는 쌍을 찾으며, 특정 해시값에 맞는 입력 하나를 찾는 역상 탐색보다 적은 시도로 성공할 수 있다. 다만 생일 공격도 넓은 의미에서는 무차별 탐색에 포함되므로, 전사적 탐색으로 충돌을 찾을 수 없다는 뜻으로 이해하면 안 된다.
④ O: SHA-1의 충돌 저항성이 깨져 더 안전한 해시 알고리즘으로 전환한다는 취지이며, SHA-3은 그 대안 중 하나이다. 다만 “SHA-3으로 대체되었다”를 모든 사용처에서 SHA-3만으로 전환했다는 뜻으로 읽으면 지나친 표현이다. 정확하게는 SHA-1 대신 SHA-2 또는 SHA-3을 사용할 수 있다는 설명이다.

NoteBase

오답 포인트

③에서 “입력을 계속 시도한다”는 공통점만 보고 역상 탐색과 충돌 탐색을 같은 방식으로 판단하기 쉽다. 역상 탐색은 미리 정해진 해시값을 목표로 삼지만, 강한 충돌 공격은 어떤 두 입력이든 해시값만 같으면 성공한다. 이 차이 때문에 생일 공격이 대표적인 충돌 공격으로 구분된다.

다시 나오면 이렇게 판단

공격자가 찾는 대상을 먼저 구분한다. 주어진 해시값에 맞는 입력이면 역상 공격, 주어진 메시지와 같은 해시값을 갖는 다른 입력이면 제2역상 공격, 자유롭게 고른 두 입력의 해시값이 같으면 충돌 공격이다. 강한 충돌 내성의 대표 공격을 묻는 문항에서는 생일 공격과 연결한다.

암기 포인트

역상은 정해진 해시값의 입력 찾기, 약한 충돌은 정해진 메시지의 짝 찾기, 강한 충돌은 같은 해시값의 두 메시지 찾기이다. 강한 충돌의 대표 공격은 생일 공격이다.

NoteBase

문 17. 공개키 기반구조(PKI) 구성요소에 관한 설명으로 가장 적절하지 않은 것은?

① 인증기관은 인증서 취소 및 폐기목록을 관리한다.

② 등록기관은 사용자 인증서 요청에 서명하여 인증기관에 전송한다.

③ 사용자는 인증기관에 공개키 인증서를 요청하고 인증서를 받는다.

④ 저장소는 등록기관에서 관리한다.

정답 4번

간단한 해설

등록기관(RA)의 핵심 역할은 **신원 확인과 인증서 신청 처리**이다. 인증서와 폐기목록을 저장·제공하는 저장소의 운영 주체를 등록기관으로 정해 놓는 것은 PKI의 일반적인 역할 구분에 맞지 않는다.

선지별 해설

① O: 인증기관(CA)은 인증서를 발급하고 자신이 발급한 인증서의 **폐지 상태를 관리**한다. 폐기목록(CRL)은 유효기간이 끝나기 전에 폐지된 인증서 정보를 제공하는 수단이다. CA가 직접 발행하거나 별도의 CRL 발행자에게 그 기능을 위임할 수 있다.

② O: 등록기관(RA)은 신청자의 신원과 인증서 신청 내용을 확인하고, 확인한 요청을 인증기관에 전달한다. 이때 **RA의 전자서명을 붙여** 요청의 출처와 무결성을 인증기관이 확인하게 하는 방식이 사용된다. 이는 RA가 인증서 자체를 발급한다는 뜻은 아니며, 실제 요청 보호 방식은 프로토콜과 운영 정책에 따라 달라질 수 있다.

③ O: 사용자는 자신의 신원과 공개키를 연결하는 인증서의 발급을 신청하고, 인증기관이 발급한 인증서를 받는다. 신청·응답은 인증기관과 직접 주고받거나 등록기관을 거칠 수 있지만, **인증서의 발급 주체는 인증기관**이다.

④ X: 저장소는 인증서와 CRL을 보관하고 이용자에게 검색·배포하는 시스템이다. 이를 **등록기관이 관리하는 것으로 일반화할 수 없다**. 일반적인 역할 구분에서는 인증기관의 인증서·폐기 정보 발행 및 관리 기능과 연결되며, 별도 저장소 운영자가 서비스를 맡을 수도 있다. 등록기관의 주된 기능은 신청자의 신원 확인과 등록 처리이다.

NoteBase

문 18. 다음에서 설명하는 특수 전자서명으로 가장 적절한 것은?

서명자가 서명을 할 수 없는 상황에서 권한을 부여받은 다른 사람이 대신 서명할 수 있는 것이다.

① 부인방지 전자서명
② 위임 서명
③ 수신자 지정 서명
④ 은닉 서명

정답 2번

간단한 해설

권한을 부여받은 대리인이 원래 서명자를 대신해 서명하는 것은 위임 서명이다. 지문은 서명 권한의 위임을 설명하므로 정답은 ②이다.

핵심 풀이

핵심 단서: 원래 서명자가 직접 서명할 수 없을 때 **권한을 부여받은 다른 사람이 대신 서명**하는 것은 ② **위임 서명**이다. 원서명자가 서명 권한을 위임하고, 대리 서명자가 그 권한에 따라 서명하는 구조가 핵심이다.

부인방지 전자서명: 특수 서명 방식인 부인방지 서명은 **서명자의 참여를 거쳐 서명의 진위를 확인**하는 방식이다. 진짜 서명을 거짓으로 부인하지 못하도록 확인·부인 절차를 두는 것이 특징이며, 다른 사람에게 서명 권한을 넘기는 개념은 아니다.

수신자 지정 서명: **누가 서명의 유효성을 확인할 수 있는지**를 지정하는 데 초점이 있다. 지정된 수신자에게 서명의 유효성을 납득시키는 검증 기능과, 대리인에게 서명을 생성할 권한을 주는 위임 기능을 구별해야 한다.

은닉 서명: 서명할 메시지의 내용을 가린 상태에서 서명을 받아 **서명자가 메시지 내용을 알 수 없게** 하는 방식이다. 은닉을 해제하면 원래 메시지에 대한 유효한 서명을 얻을 수 있지만, 대리인에게 서명 권한을 부여한다는 의미는 아니다.

NoteBase

문 19. 암호학적으로 안전한 난수 성질로 가장 적절하지 않은 것은?

① 무작위성

② 예측 불가능성

③ 보편성

④ 재현 불가능성

정답 3번

간단한 해설

난수의 암호학적 안전성은 규칙성이나 공격자의 예측·재구성 가능성과 관련된다. **보편성은 이러한 보안 성질이 아니므로** ③이 정답이다.

개념 구분

무작위성: 난수열에 쉽게 드러나는 편향이나 규칙이 없어야 한다. 암호에 쓰는 난수는 무작위처럼 보여야 하지만, **통계적 무작위성만으로 안전성이 보장되지는 않는다**. 겉으로 고르게 분포하더라도 생성 규칙이나 비밀 상태를 알면 예측할 수 있는 수열이 있기 때문이다.

예측 불가능성: 지금까지의 출력이나 공개된 생성 알고리즘을 알고 있어도, **비밀 상태를 모르는 공격자가 다음 출력을 알아내기 어려워야 한다**. 암호학적 안전성은 단순히 복잡하게 보이는지보다 공격자가 가진 정보로 예측할 수 있는지를 기준으로 판단한다.

보편성: 여러 곳에서 널리 통용된다는 성질은 난수의 편향·규칙성이나 공격자의 예측 가능성을 말하지 않는다. 따라서 **보편성은 암호학적 난수의 보안 성질이 아니다**. 널리 사용되는 생성기라도 예측 가능하면 암호용으로 안전하지 않다.

재현 불가능성의 범위: 이 문항에서는 **비밀 seed·내부 상태를 모르는 공격자의 수열 재구성이 곤란하다**는 보안 맥락으로 이해해야 한다. 모든 안전한 난수가 본질적으로 비결정적이라는 뜻은 아니다. 암호학적으로 안전한 결정적 난수 생성기(DRBG)도 **같은 초기 비밀 상태와 같은 입력이면 같은 출력**을 만든다. 따라서 이 표현을 정당한 생성자조차 같은 조건에서 재현할 수 없다는 절대적 요건으로 확대하면 부정확하다.

보안상 요구되는 무작위성·예측 저항성과 직접 관계가 없는 보편성을 고르므로, 가장 적절하지 않은 것은 ③이다.

NoteBase

문 20. 접근통제 모델에 대하여 <보기 1>의 설명과 <보기 2>의 용어를 가장 적절하게 연결한 것은?

<보기 1>
(가) 자원마다 보안등급이 부여되며 정보에 대하여 비밀등급이 정해져 보안 레이블을 사용한다.
(나) 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙에 기반을 둔다.
(다) 사용자 계정에 기반하며 객체의 소유자가 해당 객체의 접근통제 방법을 변경할 수 있다.
(라) 객체의 내용에 따라 주체의 접근을 제어한다.
<보기 2>
㉠ 강제적 접근통제
㉡ 임의적 접근통제
㉢ 역할 기반 접근통제
㉣ 문맥 의존성 접근통제

① (가): ㉠, (나): ㉡, (다): ㉢, (라): ㉣
② (가): ㉠, (나): ㉢, (다): ㉡, (라): ㉣
③ (가): ㉡, (나): ㉠, (다): ㉣, (라): ㉢
④ (가): ㉢, (나): ㉡, (다): ㉣, (라): ㉠

정답 2번

간단한 해설

보안 레이블을 따르는 것은 강제적 접근통제, **역할에 권한을 연결**하는 것은 역할 기반 접근통제, **객체 소유자가 권한을 결정**하는 것은 임의적 접근통제이다. 이 세 기준을 구별하면 대응 관계가 결정된다.

NoteBase

대응 관계 해설

(가) ㉠ 강제적 접근통제: 객체의 비밀등급과 주체의 보안등급 등 **보안 레이블에 따른 정책**으로 접근을 통제한다. 객체 소유자가 임의로 접근 권한을 바꾸는 방식과 구별되므로, 보안등급·비밀등급·레이블이 핵심 단서이다.

(나) ㉢ 역할 기반 접근통제: 권한을 직무 등의 역할에 연결하고 사용자를 해당 역할에 배정한다. 사용자가 **맡은 역할을 통해 권한을 부여받는다**는 점이 핵심이며, 객체 소유자가 개인별로 권한을 정하는 방식과 구별된다.

(다) ㉡ 임의적 접근통제: 사용자 신원에 따라 접근 권한을 정하며 **객체 소유자가 권한을 결정·변경**할 수 있다. 소유자가 다른 사용자에게 자신의 파일에 대한 읽기나 쓰기 권한을 주는 경우가 이에 해당한다.

(라) ㉣ 문맥 의존성 접근통제: 이 문항에서는 ㉣을 **객체에 담긴 내용에 따라 접근을 제한**하는 설명에 대응시킨다. 예를 들어 문서나 레코드의 실제 내용에 민감정보가 포함되어 있는지를 기준으로 접근을 결정하는 경우이다. 이러한 내용 기준은 시간·위치·앞선 접근 이력 같은 상황 기준과 구별되므로, 국문 '문맥'이라는 명칭만으로 두 기준을 동일시하지 않는다.

따라서 (가)–㉠, (나)–㉢, (다)–㉡, (라)–㉣의 연결인 ②가 가장 적절하다.

NoteBase