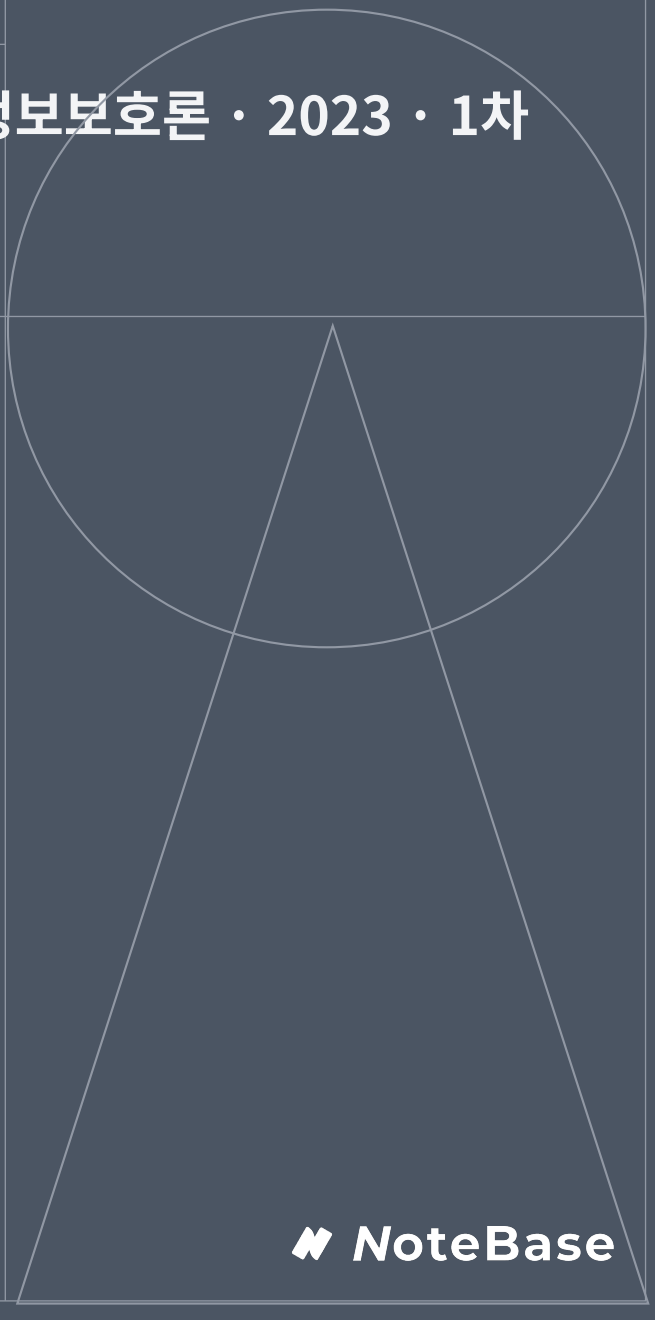
기출OX 해설집

공무원/경찰/공채(순경) · 정보보호론 · 2023 · 1차



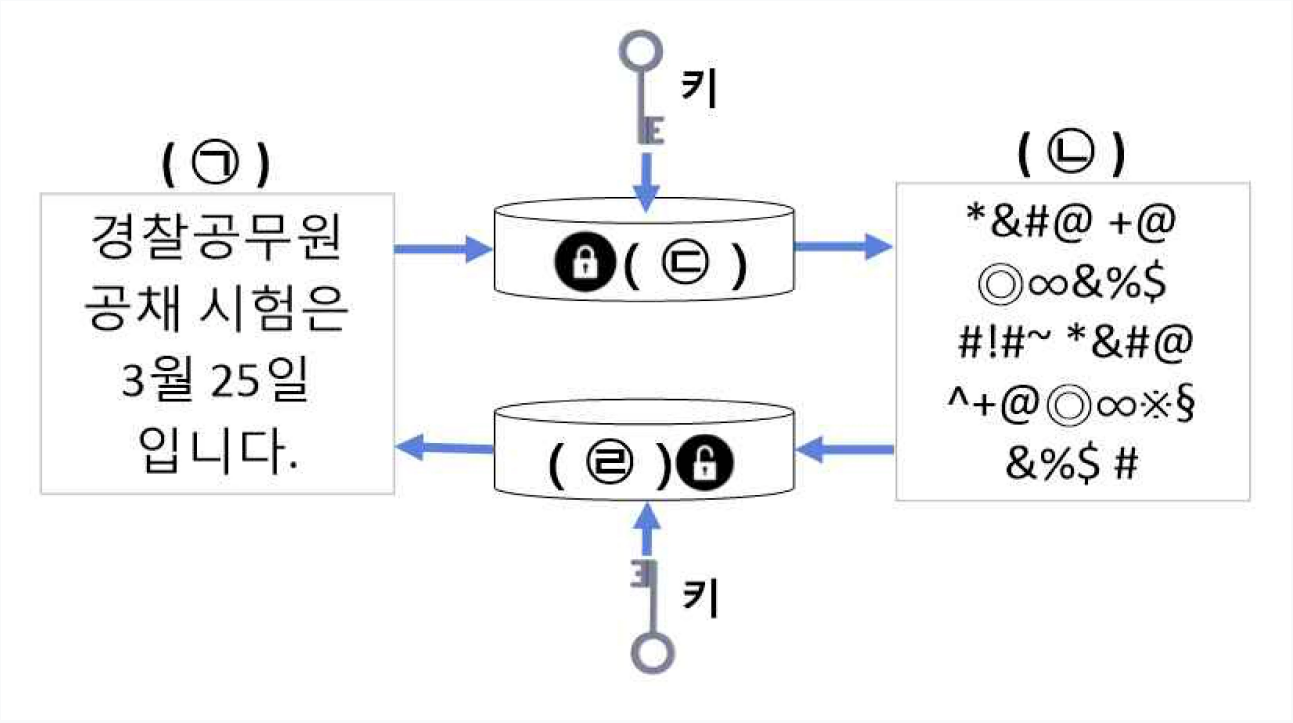
NoteBase

기출OX 해설집

공무원/경찰/공채(순경) · 정보보호론 · 2023 · 1차

공무원/경찰/공채(순경) · 정보보호론 · 2023 · 1차

문 1. 다음 그림에서 빈칸 ㉠~㉣에 들어갈 용어를 올바르게 짝지은 것으로 가장 적절한 것은?



① ㉠: 평문, ㉡: 암호문, ㉢: 암호화, ㉣: 복호화

② ㉠: 평문, ㉡: 암호문, ㉢: 복호화, ㉣: 암호화

③ ㉠: 암호문, ㉡: 평문, ㉢: 암호화, ㉣: 복호화

④ ㉠: 암호문, ㉡: 평문, ㉢: 복호화, ㉣: 암호화

정답 1번

출제 포인트

이 문제는 원래 읽을 수 있는 문장이 암호 알고리즘을 거쳐 알아볼 수 없는 형태로 바뀌고, 다시 원래 문장으로 돌아오는 도식에서 평문·암호문·암호화·복호화를 구분하는 문제이다.

NoteBase

선지별 해설

① O — ㉠은 사람이 읽을 수 있는 원래 정보이므로 평문이고, ㉡은 암호화되어 알아보기 어렵게 변환된 정보이므로 암호문이다. ㉠에서 ㉡으로 바꾸는 위쪽 과정 ㉢은 암호화이고, ㉡에서 ㉠으로 되돌리는 아래쪽 과정 ㉣은 복호화이다.
② X — ㉢과 ㉣을 서로 바꾸어 적은 점이 틀렸다. 올바르게는 ㉢이 암호화이고 ㉣이 복호화이다.
③ X — ㉠과 ㉡을 서로 바꾸어 적은 점이 틀렸다. 올바르게는 읽을 수 있는 원문인 ㉠이 평문이고, 변환된 기호 형태인 ㉡이 암호문이다.
④ X — 평문과 암호문뿐 아니라 암호화와 복호화도 모두 반대로 짝지었다. 올바르게는 ㉠은 평문, ㉡은 암호문, ㉢은 암호화, ㉣은 복호화이다.

오답 포인트

화살표의 방향을 놓치면 ㉢과 ㉣을 뒤바꾸기 쉽다. 읽을 수 있는 문장에서 기호 형태로 향하는 위쪽 화살표가 암호화이고, 기호 형태에서 원래 문장으로 돌아오는 아래쪽 화살표가 복호화이다.

다시 나오면 이렇게 판단

도식의 양쪽 결과부터 확인한다. 원래 의미를 읽을 수 있는 입력은 평문, 변환되어 바로 읽기 어려운 출력은 암호문이다. 평문에서 암호문으로 가면 암호화, 암호문에서 평문으로 돌아오면 복호화로 판단한다.

암기 포인트

평문 → 암호화 → 암호문 → 복호화 → 평문이다.

NoteBase

문 2. 디지털콘텐츠에 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술로 가장 적절한 것은?

① 홀로그램(hologram)
② 스테가노그래피(steganography)
③ 디지털 사이니지(digital signage)
④ 디지털 핑거프린팅(digital finger printing)

정답 4번

출제 포인트

디지털 콘텐츠에 구매자마다 서로 다른 식별 정보를 삽입하여 불법 유통 경로를 추적하는 기술을 구별하는 문제이다.

핵심 개념

디지털 핑거프린팅은 콘텐츠 사본마다 구매자나 사용자에 대응하는 고유 식별 정보를 삽입하고, 유출된 사본에서 그 정보를 검출하여 최초 구매자 또는 배포자를 추적하는 기술이다.
홀로그램은 빛의 간섭과 회절을 이용하여 입체 정보를 기록·재현하는 기술이고, 스테가노그래피는 다른 매체 안에 비밀정보의 존재 자체를 숨기는 기술이며, 디지털 사이니지는 디지털 디스플레이로 정보나 광고를 제공하는 매체이다.

선지별 해설

① X — 홀로그램은 빛의 간섭무늬를 기록하여 입체 영상을 재현하거나 위·변조 방지 표식 등에 활용하는 기술이다. 틀린 부분은 '구매자의 정보를 삽입하여 최초 배포자를 추적하는 기술'과 홀로그램을 연결한 것이다. 올바르게는 구매자별 식별 정보를 삽입해 유출자를 추적하는 기술은 디지털 핑거프린팅이다.
② X — 스테가노그래피는 이미지·음성 등 다른 데이터 안에 비밀정보를 숨겨 정보가 존재한다는 사실을 알아채기 어렵게 하는 기술이다. 틀린 부분은 '구매자 식별 및 불법 배포자 추적'을 스테가노그래피의 주목적으로 본 것이다. 올바르게는 스테가노그래피의 핵심 목적은 비밀정보의 은닉이다.
③ X — 디지털 사이니지는 디지털 디스플레이를 이용해 광고·안내 등의 콘텐츠를 표시하고 관리하는 시스템이다. 틀린 부분은 '콘텐츠 내부에 구매자 정보를 삽입하는 추적 기술'과 디지털 사이니지를 연결한 것이다. 올바르게는 디지털 사이니지는 정보를 보여 주는 전자 표시 매체이다.
④ O — 디지털 핑거프린팅은 판매되는 콘텐츠 사본에 구매자별 고유 정보를 삽입한다. 불법 배포된 사본에서 그 정보를 찾아 최초 구매자 또는 배포자를 추적할 수 있으므로 제시된 설명에 해당한다.

NoteBase

오답 포인트

②의 스테가노그래피도 데이터를 매체 안에 감춘다는 점 때문에 혼동하기 쉽다. 그러나 '비밀정보의 존재를 숨김'은 스테가노그래피이고, '구매자별 표식을 넣어 유출자를 추적'은 디지털 핑거프린팅이다.

다시 나오면 이렇게 판단

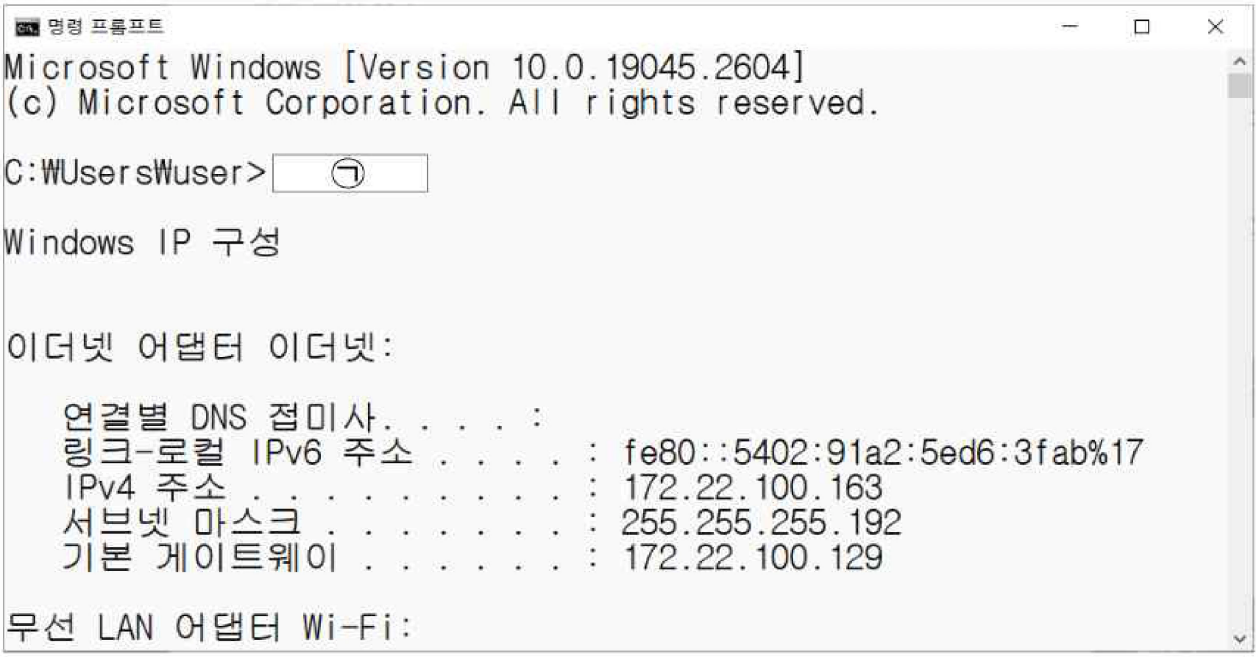
문장에서 삽입 정보의 목적을 확인한다. 비밀 통신을 위해 정보의 존재를 숨기면 스테가노그래피이고, 구매자마다 다른 식별 정보를 넣어 불법 복제·배포자를 추적하면 디지털 핑거프린팅이다.

암기 포인트

숨겨서 전달하면 스테가노그래피, 구매자별 흔적을 남겨 추적하면 디지털 핑거프린팅이다.

NoteBase

문 3. 다음 그림은 빈칸 ㉠의 명령어를 실행한 결과의 일부이다. 빈칸 ㉠의 명령어로 옳은 것은?



① ping

② protocol

③ ipmask

④ ipconfig

정답 4번

출제 포인트

명령 실행 결과에 나타난 'Windows IP 구성'과 IPv4 주소, 서브넷 마스크, 기본 게이트웨이를 보고 해당 Windows 네트워크 설정 확인 명령어를 식별하는 문제이다.

NoteBase

선지별 해설

① X
- ping은 ICMP 에코 요청과 응답을 이용해 대상 호스트와의 통신 가능 여부 및 응답 시간을 확인하는 명령어이므로, 그림과 같은 로컬 IP 구성 정보를 출력하지 않는다. 틀린 표현 ‘ping’은 ‘ipconfig’로 고쳐야 한다.

② X
- protocol은 Windows에서 IPv4 주소, 서브넷 마스크, 기본 게이트웨이를 표시하는 표준 명령어가 아니다. 틀린 표현 ‘protocol’은 ‘ipconfig’로 고쳐야 한다.

③ X
- ipmask는 Windows의 표준 네트워크 구성 확인 명령어가 아니다. 서브넷 마스크는 별도의 ipmask 명령으로 조회하는 것이 아니라 ipconfig 실행 결과의 한 항목으로 표시된다. 틀린 표현 ‘ipmask’는 ‘ipconfig’로 고쳐야 한다.

④ O
- ipconfig는 Windows의 TCP/IP 네트워크 구성 정보를 표시하며, 그림처럼 어댑터별 IPv4 주소, 서브넷 마스크, 기본 게이트웨이 등을 출력한다.

오답 포인트

그림에 IP 주소가 나온다는 이유만으로 통신 상태를 확인하는 ping과 혼동하기 쉽다. ‘Windows IP 구성’ 아래에 로컬 어댑터의 주소·마스크·게이트웨이가 함께 제시되면 ipconfig의 출력이다.

다시 나오면 이렇게 판단

출력 화면에서 무엇을 확인하는지 구분한다. 로컬 PC의 IP 설정 정보가 나열되면 ipconfig이고, 특정 대상에 대한 응답과 왕복 시간이 연속해서 표시되면 ping이다.

암기 포인트

IP 구성(config) 확인은 ipconfig, 연결 응답 확인은 ping이다.

NoteBase

문 4. 다음 대칭키 암호 운영모드의 암호화 과정에서 병렬처리가 가능한 것을 모두 고른 것은?

㉠ CTR(CounTeR)
㉡ CFB(Cipher-FeedBack)
㉢ CBC(Cipher Block Chaining)
㉣ ECB(Electronic CodeBook)

① ㉠㉡
② ㉠㉣
③ ㉡㉢
④ ㉢㉣

정답 2번

출제 포인트

블록마다 암호화 입력을 독립적으로 만들 수 있는지를 기준으로 대칭키 암호 운영모드의 암호화 병렬처리 가능 여부를 구분하는 문제이다.

핵심 개념

CTR: 서로 다른 카운터 값을 각각 암호화하므로 각 블록을 독립적으로 처리할 수 있다.
CFB: 앞 블록의 암호문을 다음 블록의 암호화 입력으로 되먹임하므로 암호화가 순차적으로 진행된다.
CBC: 현재 평문 블록을 앞 블록의 암호문과 결합한 뒤 암호화하므로 암호화가 순차적으로 진행된다.
ECB: 각 평문 블록을 서로 독립적으로 암호화하므로 병렬처리가 가능하다.

선지별 해설

① X — ㉠ CTR은 병렬처리가 가능하지만 ㉡ CFB는 앞 암호문 블록의 출력이 다음 블록에 필요하므로 암호화 병렬처리가 불가능하다. 틀린 부분은 ㉡이며, 올바른 조합은 ㉠㉣이다.
② O — ㉠ CTR은 블록별 카운터 입력이 독립적이고, ㉣ ECB는 각 평문 블록을 독립적으로 암호화하므로 둘 다 암호화 병렬처리가 가능하다.
③ X — ㉡ CFB는 앞 암호문을 되먹임하고, ㉢ CBC는 앞 암호문과 현재 평문을 결합하므로 둘 다 암호화가 순차적이다. ㉡㉢이 아니라 병렬처리가 가능한 것은 ㉠㉣이다.
④ X — ㉣ ECB는 병렬처리가 가능하지만 ㉢ CBC는 앞 암호문 블록이 있어야 다음 블록을 암호화할 수 있다. 틀린 부분은 ㉢이며, 올바른 조합은 ㉠㉣이다.

NoteBase

오답 포인트

CTR, CFB, CBC, ECB가 모두 블록 암호 운영모드라는 점만 보고 병렬처리 가능 여부도 같다고 판단하기 쉽다. 핵심 함정은 암호화 과정에서 앞 블록의 암호문을 기다려야 하는 CFB·CBC와, 블록별 입력이 독립적인 CTR·ECB를 혼동하는 데 있다.

다시 나오면 이렇게 판단

현재 블록을 암호화할 때 앞 블록의 암호문이 필요한지를 확인한다. 필요하면 암호화는 순차적이고, 블록별 입력을 미리 독립적으로 정할 수 있으면 병렬처리가 가능하다.

암기 포인트

암호화 병렬처리는 CTR·ECB, 앞 암호문을 기다리는 CFB·CBC는 순차 처리이다.

NoteBase

문 5. 다음은 악성 프로그램에 의한 피해 사례를 보도한 신문 기사이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?

7월 콜택시 콜센터 서버를 공격, 서비스를 마비시킨 ㉠에 의한 추가 피해가 확산되고 있다. 서버를 주요 공격 대상으로 삼고 있어 피해 규모가 작지 않은 것으로 추정된다. 인터넷상 서버 노출을 자제하는 등 각별한 주의가 요구된다.
7월 콜택시 시스템을 공격한 ㉠는 '매스스캔'이다. 당시 콜택시 시스템 운영사 서버 파일은 모두 'masscan'이라는 명칭으로 변환됐다. 이와 함께 '복구정보' 파일에 복호화 비용, 방법 등을 기재했다. 콜택시 공격을 기점으로 매스스캔에 의한 피해 사례는 빠르게 확산되고 있다. 현재 확인된 기업 피해 사례만 4건 이상이다. 제약·바이오 등 업종도 다양하다.
- ◯◯ 신문 -

① 애드웨어(adware)
② 라이트웨어(liteware)
③ 스파이웨어(spyware)
④ 랜섬웨어(ransomware)

정답 4번

출제 포인트

파일을 사용할 수 없게 만든 뒤 복구 대가를 요구하는 악성 프로그램의 유형을 식별하는 문제이다.

핵심 개념

랜섬웨어는 파일을 암호화하거나 시스템 접근을 차단한 뒤 이를 복구해 주는 대가로 금전을 요구하는 악성 프로그램이다. 기사에서 서버 파일의 명칭이 바뀌고 복구정보 파일에 복호화 비용과 방법이 적혔다는 점이 결정적 단서이다.
애드웨어는 광고 노출, 스파이웨어는 정보 수집, 랜섬웨어는 사용 불능 상태를 이용한 금전 요구가 핵심이다.

NoteBase

선지별 해설

① X — 애드웨어는 광고를 표시하거나 광고성 프로그램을 설치하는 소프트웨어이다. 틀린 표현은 '애드웨어'이며, 파일을 사용할 수 없게 하고 복호화 비용을 요구하는 이 사례의 올바른 용어는 '랜섬웨어'이다.
② X — 라이트웨어는 정식 제품보다 기능을 줄여 배포하는 제한판 소프트웨어를 뜻하며, 파일 복구를 대가로 금전을 요구하는 악성 프로그램이 아니다. 틀린 표현은 '라이트웨어'이며, 올바르게는 '랜섬웨어'이다.
③ X — 스파이웨어는 이용자 몰래 개인정보나 사용 행태를 수집·전송하는 악성 프로그램이다. 틀린 표현은 '스파이웨어'이며, 파일을 사용할 수 없게 한 뒤 복구 비용을 요구하는 경우는 '랜섬웨어'이다.
④ O — 랜섬웨어는 파일 암호화나 시스템 접근 차단으로 피해자의 데이터를 사용할 수 없게 한 뒤 복구 또는 복호화를 조건으로 대가를 요구한다. 기사의 파일 변환과 복호화 비용 안내가 이 특징에 해당한다.

오답 포인트

'서버 공격'이라는 넓은 표현만 보고 모든 악성 프로그램을 후보로 보는 것이 함정이다. 이 문항에서는 복구정보 파일에 적힌 '복호화 비용'이 랜섬웨어를 가르는 핵심 표현이다.

다시 나오면 이렇게 판단

광고가 핵심이면 애드웨어, 몰래 정보 수집이 핵심이면 스파이웨어, 기능을 제한한 배포판이면 라이트웨어, 파일 암호화·접근 차단 뒤 복구 대가를 요구하면 랜섬웨어로 판단한다.

암기 포인트

광고는 애드웨어, 감시는 스파이웨어, 복구 대가는 랜섬웨어이다.

NoteBase

문 6. 다음 AES와 RSA 암호화 알고리즘에 관한 설명으로 옳은 것을 모두 고른 것은?

㉠ AES는 56bits 키 크기를 갖는 암호화 알고리즘이다.
㉡ AES는 암호화 키와 복호화 키가 같은 대칭키 암호화 알고리즘이다.
㉢ RSA는 소인수분해 기반의 공개키 암호화 알고리즘이다.
㉣ RSA는 암호화 키와 복호화 키가 다른 대칭키 암호화 알고리즘이다.

① ㉠
② ㉠㉣
③ ㉡㉢
④ ㉡㉢㉣

정답 3번

출제 포인트

AES와 RSA를 키의 관계, 키 길이, 안전성의 기반으로 구분할 수 있는지를 묻는 문제이다.

핵심 개념

AES는 암호화와 복호화에 같은 비밀키를 사용하는 대칭키 블록 암호이며, 키 길이는 128비트·192비트·256비트이다.
RSA는 서로 다른 공개키와 개인키를 사용하는 공개키 암호이며, 큰 정수의 소인수분해가 어렵다는 성질에 안전성의 기반을 둔다.
따라서 ㉠은 X, ㉡은 O, ㉢은 O, ㉣은 X이다.

선지별 해설

① X — ㉠만 고른 선택지이다. ㉠의 '56bits 키 크기'가 틀렸다. AES의 키 길이는 128비트·192비트·256비트이므로, 옳은 문장은 ㉡과 ㉢이다.
② X — ㉠과 ㉣을 고른 선택지인데 둘 다 틀렸다. ㉠은 AES의 키 길이를 128비트·192비트·256비트로 고쳐야 하고, ㉣의 '대칭키'를 '공개키(비대칭키)'로 고쳐야 한다.
③ O — ㉡의 AES는 같은 키를 사용하는 대칭키 암호라는 설명과 ㉢의 RSA는 소인수분해 문제에 기반한 공개키 암호라는 설명이 모두 옳다.
④ X — 옳은 ㉡과 ㉢에 틀린 ㉣을 추가한 선택지이다. RSA는 암호화 키와 복호화 키가 서로 다른 공개키 암호이므로, ㉣의 '대칭키 암호화 알고리즘'은 '공개키(비대칭키) 암호화 알고리즘'으로 고쳐야 한다.

NoteBase

오답 포인트

㉣은 '암호화 키와 복호화 키가 다르다'는 앞부분은 맞지만 이를 '대칭키'라고 부른 뒷부분이 틀린 함정이다. 또한 56비트는 AES의 키 길이가 아니므로 ㉠도 제외해야 한다.

다시 나오면 이렇게 판단

같은 키를 쓰면 대칭키 암호, 공개키와 개인키처럼 서로 다른 키를 쓰면 공개키 암호로 판단한다. AES는 대칭키와 128·192·256비트, RSA는 공개키와 소인수분해를 연결한다.

암기 포인트

AES는 같은 키·128/192/256비트, RSA는 공개키와 개인키·소인수분해이다.

NoteBase

문 7. 인증서 폐기 목록(CRL, Certificate Revocation List)에 관한 설명으로 가장 적절하지 않은 것은?

① CRL은 더 이상 사용할 수 없는 인증서들의 목록이다.

② 인증서를 발행한 인증기관(CA)은 정기적으로 CRL을 발행한다.

③ Version, Authority key identifier는 CRL의 기본 필드이다.

④ Issuer alternative name, CRL number는 CRL의 확장 필드이다.

정답 3번

출제 포인트

CRL의 역할과 CRL을 구성하는 기본 필드·확장 필드의 구분을 묻는 문제이다.

핵심 개념

CRL은 인증서의 유효기간이 끝나기 전에 폐기되어 더 이상 신뢰할 수 없는 인증서 정보를 인증기관이 서명하여 배포하는 목록이다.
CRL의 기본 필드에는 Version, Signature, Issuer, This Update, Next Update, Revoked Certificates 등이 포함된다. Authority Key Identifier, Issuer Alternative Name, CRL Number 등은 CRL 확장 필드에 해당한다.

선지별 해설

① O — CRL은 유효기간 만료 전에 폐기되어 더 이상 사용할 수 없는 인증서들의 정보를 담은 목록이다.
② O — 인증서를 발행한 인증기관(CA)은 폐기 상태를 이용자에게 알리기 위해 CRL을 정기적으로 발행한다.
③ X — 틀린 표현은 'Authority key identifier는 CRL의 기본 필드'이다. Version은 기본 필드이지만, Authority Key Identifier는 CRL 발행자의 공개키를 식별하는 확장 필드이다. 올바르게는 'Version은 CRL의 기본 필드이고, Authority Key Identifier는 CRL의 확장 필드이다'이다.
④ O — Issuer Alternative Name은 CRL 발행자의 대체 이름을 나타내고 CRL Number는 CRL에 순차적인 번호를 부여하는 항목으로, 둘 다 CRL 확장 필드이다.

오답 포인트

③은 Version과 Authority Key Identifier를 한 묶음으로 제시해 둘 다 기본 필드인 것처럼 보이게 한다. Version은 기본 필드이지만 'Identifier', 'Alternative Name', 'Number'와 같은 부가 식별 정보는 확장 필드에서 다룬다는 점이 함정이다.

다시 나오면 이렇게 판단

CRL의 발행자·발행 시각·다음 발행 시각·폐기 인증서 목록처럼 CRL 본체를 구성하는 항목은 기본 필드로 판단한다. 발행자 키 식별자, 대체 이름, CRL 번호처럼 추가 식별 기능을 제공하는 항목은 확장 필드로 판단한다.

NoteBase

암기 포인트

Version은 기본 필드, Authority Key Identifier·Issuer Alternative Name·CRL Number는 확장 필드이다.

NoteBase

문 8. DES(Data Encryption Standard)에서 입력값 $101100_{(2)}$이 다음 S-Box를 통과할 때 출력값으로 옳은 것은?

S-Box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	07	02	12	05	10	14	01
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

① $0011_{(2)}$

② $0111_{(2)}$

③ $1000_{(2)}$

④ $1111_{(2)}$

정답 1번

출제 포인트

DES의 S-Box에서 6비트 입력의 첫째·여섯째 비트로 행을 정하고, 둘째부터 다섯째 비트로 열을 정해 4비트 출력을 구하는 문제이다.

조건 정리

주어진 입력: $101100_{(2)}$
행을 정하는 비트: 첫째 비트와 여섯째 비트
열을 정하는 비트: 둘째부터 다섯째 비트
S-Box의 10진수 출력은 4비트 이진수로 변환한다.

사용할 원리

6비트 입력을 $b_1b_2b_3b_4b_5b_6$라고 하면 행은 $(b_1b_6)_{(2)}$, 열은 $(b_2b_3b_4b_5)_{(2)}$로 정한다. DES S-Box가 바깥쪽 두 비트와 가운데 네 비트를 서로 다른 좌표로 사용하기 때문이다.

NoteBase

계산 과정

1. $101100_{(2)}$의 첫째·여섯째 비트는 $10_{(2)} = 2$이므로 행은 2이다.
2. 가운데 네 비트는 $0110_{(2)} = 6$이므로 열은 6이다.
3. 제시된 S-Box의 2행 6열 값은 03이다.
4. $3_{(10)} = 0011_{(2)}$이므로 출력값은 $0011_{(2)}$이다.

선지별 해설

① O — 2행 6열의 값 03을 4비트 이진수로 바꾸면 $0011_{(2)}$이므로 옳다.
② X — $0111_{(2)}$은 10진수 7이지만, 올바른 좌표의 표 값은 3이다. 틀린 출력 $0111_{(2)}$은 $0011_{(2)}$로 고쳐야 한다.
③ X — $1000_{(2)}$은 10진수 8이지만, 2행 6열의 값은 3이다. 틀린 출력 $1000_{(2)}$은 $0011_{(2)}$로 고쳐야 한다.
④ X — $1111_{(2)}$은 10진수 15이지만, 2행 6열의 값은 3이다. 틀린 출력 $1111_{(2)}$은 $0011_{(2)}$로 고쳐야 한다.

오답 포인트

입력 $101100_{(2)}$ 전체를 하나의 이진수로 읽거나, 앞의 두 비트를 행으로 정하면 좌표가 달라진다. 행은 서로 떨어진 첫째·여섯째 비트, 열은 가운데 네 비트로 정한다. 또한 표의 03은 10진수 3이므로 4비트 출력에서는 앞의 0을 생략하지 않고 $0011_{(2)}$로 쓴다.

다시 나오면 이렇게 판단

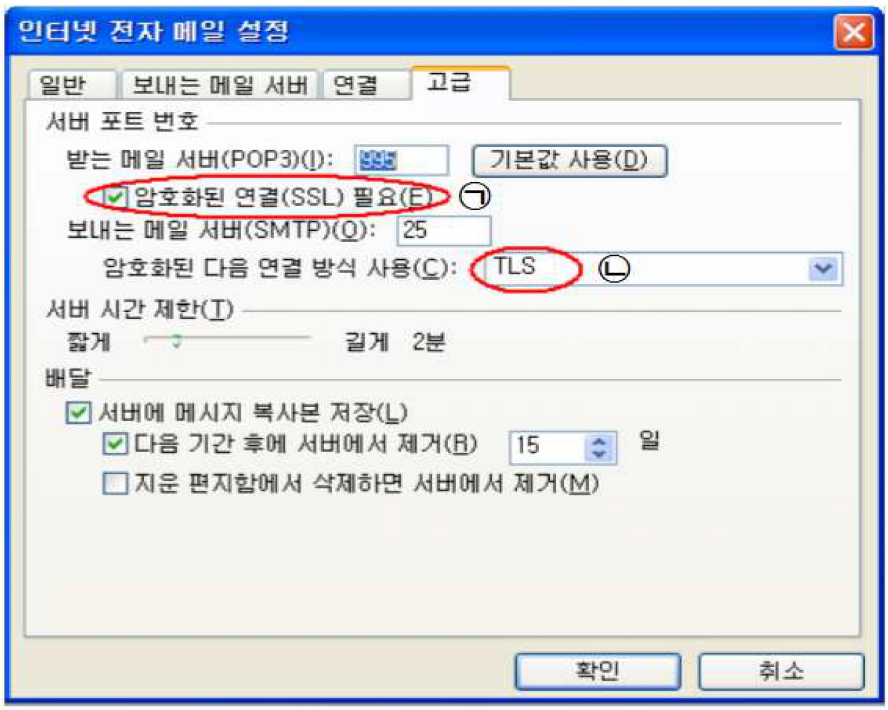
DES S-Box 문제는 바깥쪽 두 비트로 행 결정 → 가운데 네 비트로 열 결정 → 표 조회 → 결과를 4비트 이진수로 변환하는 순서로 판단한다.

암기 포인트

DES S-Box의 6비트 입력은 '양끝은 행, 가운데는 열'로 읽고, 출력은 항상 4비트로 표시한다.

NoteBase

문 9. 다음 그림은 인터넷 전자메일 설정화면이다. ㉠과 ㉡에 관한 설명으로 가장 적절하지 않은 것은?



① ㉠의 SSL과 ㉡의 TLS는 기밀성, 무결성, 인증을 보장하는 프로토콜이다.

② ㉠의 SSL과 ㉡의 TLS는 메일 송·수신을 위한 SMTP, POP3, IMAP4 프로토콜의 상위계층에 위치한다.

③ ㉠의 SSL과 ㉡의 TLS는 대칭키 암호화 알고리즘을 이용해서 기밀성을 제공하고, 메시지 인증코드를 이용하여 메시지 무결성을 제공한다.

④ ㉡의 TLS는 ㉠의 SSL 3.0을 기반으로 IETF가 만든 프로토콜로서 클라이언트-서버 환경에서 TCP 기반의 애플리케이션에 대한 보안 서비스를 제공한다.

정답 2번

출제 포인트

SSL과 TLS가 제공하는 보안 기능과 TCP/IP 계층에서의 위치를 구분하는 문제이다.

핵심 개념

SSL은 TCP를 사용하는 응용 프로그램에 보안 통신 기능을 제공하는 프로토콜이며, TLS는 SSL 3.0을 바탕으로 IETF가 표준화한 후속 프로토콜이다.
계층 관계는 'SMTP·POP3·IMAP4 등 응용 프로토콜 → SSL/TLS → TCP'로 이해할 수 있다. SSL/TLS는 핸드셰이크에서 상대를 인증하고 키를 설정한 뒤, 레코드 계층에서 기밀성과 무결성을 제공한다.

NoteBase

선지별 해설

① O — SSL과 TLS는 암호화를 통한 기밀성, 메시지 인증을 통한 무결성, 인증서 등을 이용한 상대 인증 기능을 제공한다.
② X — 틀린 부분은 ‘SMTP, POP3, IMAP4 프로토콜의 상위계층에 위치한다’이다. 실제로는 SMTP·POP3·IMAP4와 같은 응용계층 프로토콜이 SSL/TLS의 위에서 동작하고, SSL/TLS는 이들 응용 프로토콜과 TCP 사이에 위치한다.
③ O — SSL/TLS는 핸드셰이크에서 정한 대칭키 암호 방식으로 전송 데이터의 기밀성을 제공하고, 메시지 인증코드 등으로 데이터의 무결성을 확인한다.
④ O — TLS는 SSL 3.0을 기반으로 IETF가 표준화한 프로토콜이며, 클라이언트-서버 환경에서 TCP 기반 응용 프로그램에 보안 서비스를 제공한다.

오답 포인트

②의 함정은 ‘보안 기능을 응용 프로그램에 제공한다’는 설명을 ‘응용 프로토콜의 상위계층에 있다’로 뒤집은 데 있다. SSL/TLS의 서비스 대상은 응용 프로토콜이지만, 계층 위치는 응용 프로토콜의 아래이자 TCP의 위이다.

다시 나오면 이렇게 판단

SSL/TLS의 위치를 묻는 경우 응용 프로토콜과 TCP 사이에 있는지를 먼저 확인한다. 기능을 묻는 경우 기밀성·무결성·인증을, 계보를 묻는 경우 SSL 3.0에서 TLS로 이어지는 관계를 확인한다.

암기 포인트

응용 프로토콜 아래, TCP 위에는 SSL/TLS가 위치한다.

NoteBase

문 10. SSO(Single Sign On)의 구성요소에 관한 설명으로 가장 적절하지 않은 것은?

① 인증 서버는 ACL을 통한 통합 인증 서비스를 제공한다.

② SSO Agent는 각 정보시스템에 자동 인증 정보를 송·수신한다.

③ LDAP는 네트워크 자원을 식별하고, 사용자와 애플리케이션들이 자원에 접근할 수 없도록 하는 네트워크 디렉토리 서비스이다.

④ 사용자는 SSO를 구현한 포털(Portal)에 자신의 ID와 Password로 한 번만 로그인하면 연동된 시스템에 재인증 절차없이 편리하게 접근할 수 있다.

정답 3번

출제 포인트

이 문제는 SSO의 핵심 구성요소인 인증 서버, SSO Agent, LDAP의 역할과 한 번의 로그인으로 여러 연동 시스템을 이용하는 원리를 구별하는 문제이다.

핵심 개념

SSO는 한 번의 사용자 인증으로 서로 연동된 여러 정보시스템에 다시 로그인하지 않고 접근하게 하는 통합 인증 방식이다. 인증 서버는 사용자의 인증과 접근 권한을 통합 관리하고, SSO Agent는 인증 정보를 각 정보시스템과 연계한다. LDAP는 사용자·조직·장치 등 네트워크 자원의 정보를 계층적으로 저장하고 검색·조회할 수 있게 하는 디렉터리 서비스이다.

선지별 해설

① O — 인증 서버는 사용자 인증 정보를 통합 관리하고 ACL을 이용해 사용자나 그룹별 접근 권한을 확인·제어하므로 통합 인증 서비스를 제공하는 구성요소에 해당한다.
② O — SSO Agent는 인증 서버와 각 정보시스템 사이에서 인증 정보를 자동으로 송·수신하여 사용자가 시스템마다 다시 인증하지 않게 한다.
③ X — 틀린 표현은 '자원에 접근할 수 없도록'이다. LDAP는 네트워크 자원을 식별하고 사용자와 애플리케이션이 필요한 자원 정보를 조회하여 권한에 따라 접근할 수 있도록 지원하는 디렉터리 서비스이다.
④ O — 사용자는 SSO 포털에 ID와 Password로 한 번 로그인하면 인증 정보가 연동 시스템에 전달되므로 별도의 재인증 절차 없이 접근할 수 있다.

오답 포인트

③은 LDAP가 접근 통제에 활용될 수 있다는 점을 '접근할 수 없도록 하는 서비스'로 바꾸어 놓았다. LDAP의 본질은 접근 차단 자체가 아니라 네트워크 자원과 사용자 정보를 저장·검색·제공하는 디렉터리 서비스라는 점이 함정이다.

NoteBase

다시 나오면 이렇게 판단

구성요소별 동사를 기준으로 판단한다. 인증 서버는 인증·권한 관리, SSO Agent는 인증 정보 연계, LDAP는 디렉터리 정보의 저장·검색, SSO 사용자는 한 번의 로그인 후 연동 시스템 이용에 대응한다.

암기 포인트

인증 서버는 인증·권한, Agent는 전달·연계, LDAP는 디렉터리 조회, SSO는 한 번 로그인이다.

NoteBase

문 11. 다음 C언어 소스 코드를 실행할 때 발생하는 시스템 자원 고갈 공격으로 가장 적절한 것은?

```
#include <stdio.h>
#include <stdlib.h>

void main()
{
    char *chM;
    while(1)
        chM = (char *)malloc(1000);
}
```

① 가용 메모리 자원 고갈 공격

② 가용 디스크 자원 고갈 공격

③ 가용 프린터 자원 고갈 공격

④ 가용 네트워크 자원 고갈 공격

정답 1번

출제 포인트

반복문 안에서 동적 메모리를 계속 할당하면서 이전에 할당한 영역을 해제하지 않을 때 어떤 시스템 자원이 고갈되는지를 판단하는 문제이다.

사례 정리

핵심 사실 1: while(1)은 종료 조건이 없는 무한 반복문이다.
핵심 사실 2: 반복할 때마다 malloc(1000)이 새로운 동적 메모리 영역을 요청한다.
판단에 중요한 조건: 이전에 할당받은 주소를 free로 해제하지 않고 포인터 변수 chM에 새 주소를 계속 덮어쓴다.

핵심 개념

메모리 누수는 더 이상 사용하거나 해제할 수 없는 동적 메모리 영역이 계속 남는 현상이다. 이 코드에서는 반복적인 malloc 호출과 free의 부재로 가용 메모리가 지속적으로 소모된다.

NoteBase

적용 기준

반복해서 호출되는 자원 할당 함수와 그 자원의 해제 여부를 확인한다. malloc은 메모리를 할당하므로 이 코드가 직접 고갈시키는 대상은 메모리 자원이다.

선지별 해설

① O — 무한 반복 중 malloc(1000)으로 메모리를 계속 할당하고 free하지 않으므로 가용 메모리 자원 고갈 공격에 해당한다.
② X — 틀린 표현은 '디스크 자원'이다. 파일 생성이나 디스크 기록 동작이 없으며, 올바르게는 '가용 메모리 자원 고갈 공격'이다.
③ X — 틀린 표현은 '프린터 자원'이다. 인쇄 작업을 생성하거나 출력 대기열을 점유하는 동작이 없으며, 올바르게는 '가용 메모리 자원 고갈 공격'이다.
④ X — 틀린 표현은 '네트워크 자원'이다. 소켓 생성, 연결 요청, 패킷 전송과 같은 네트워크 동작이 없으며, 올바르게는 '가용 메모리 자원 고갈 공격'이다.

오답 포인트

무한 반복문이라는 사실만 보고 모든 종류의 자원 고갈 공격으로 넓혀 판단하면 안 된다. 실제 반복 실행되는 함수가 malloc이므로 고갈되는 자원은 메모리이다.

다시 나오면 이렇게 판단

무한 반복 여부를 확인한 뒤 반복문 안의 자원 할당 함수와 대응하는 해제 함수가 있는지를 본다.
malloc·calloc·realloc의 반복 호출에 free가 없으면 메모리 고갈로 판단한다.

암기 포인트

무한 malloc + free 없음 = 메모리 누수 누적 = 가용 메모리 고갈이다.

NoteBase

문 12. 커버로스(Kerberos)의 구성요소에 관한 설명으로 가장 적절하지 않은 것은?

① Ticket은 사용자의 인증을 확인하는 토큰이다.

② TGS(Ticket Granting Service)는 모든 사용자에게 Ticket을 발행한다.

③ AS(Authentication Service)는 각 서버와 유일한 비밀키를 공유한다.

④ KDC(Key Distribution Center)는 모든 사용자와 서비스의 비밀키를 보관한다.

정답 2번

출제 포인트

Kerberos에서 Ticket, AS, TGS, KDC가 각각 어떤 역할을 하는지 구별하는 문제이다.

핵심 개념

Kerberos는 신뢰할 수 있는 제3자인 KDC가 비밀키 기반의 티켓을 발급하여 사용자와 서비스의 인증을 지원하는 방식이다.
AS는 사용자의 최초 인증을 처리하고 보통 TGT(Ticket Granting Ticket)를 발급한다. TGS는 이미 인증되어 유효한 TGT를 제시한 사용자에게 특정 서비스를 이용하기 위한 서비스 티켓을 발급한다. KDC는 AS와 TGS의 기능을 포함하며 사용자와 서비스의 비밀키 정보를 관리한다.

선지별 해설

① O — Ticket은 클라이언트의 신원과 세션키 등의 정보를 서버의 비밀키로 보호한 인증용 토큰이다. 클라이언트는 Ticket과 Authenticator를 서버에 제시하여 자신의 신원을 입증한다.
② X — 틀린 표현은 '모든 사용자에게'이다. TGS는 아무 사용자에게나 Ticket을 발행하는 것이 아니라, AS의 인증을 거쳐 유효한 TGT를 제시한 사용자에게 요청한 서비스의 서비스 티켓을 발급한다.
③ O — Kerberos의 기본 인증 과정에서 AS는 사용자의 비밀키(패스워드)를 데이터베이스에 보관할 뿐 아니라, 각 서버와도 서버마다 서로 다른 고유한 비밀키를 미리 공유한다. AS가 이 서버별 비밀키로 Ticket을 암호화하므로 해당 서버만 Ticket을 복호화하여 내용을 확인할 수 있다. 실제 구현에서도 AS와 TGS는 KDC 안에서 같은 키 데이터베이스를 사용하므로, AS가 각 서버와 유일한 비밀키를 공유한다는 설명은 적절하다.
④ O — KDC는 사용자와 서비스에 등록된 장기 비밀키를 중앙에서 관리하며, AS와 TGS 기능을 통해 TGT와 서비스 티켓을 발급한다.

오답 포인트

②는 TGS가 티켓을 발급한다는 앞부분은 맞지만, 대상을 '모든 사용자'로 넓힌 것이 함정이다. TGS의 서비스 티켓 발급에는 먼저 AS에서 받은 유효한 TGT가 필요하다.

NoteBase

다시 나오면 이렇게 판단

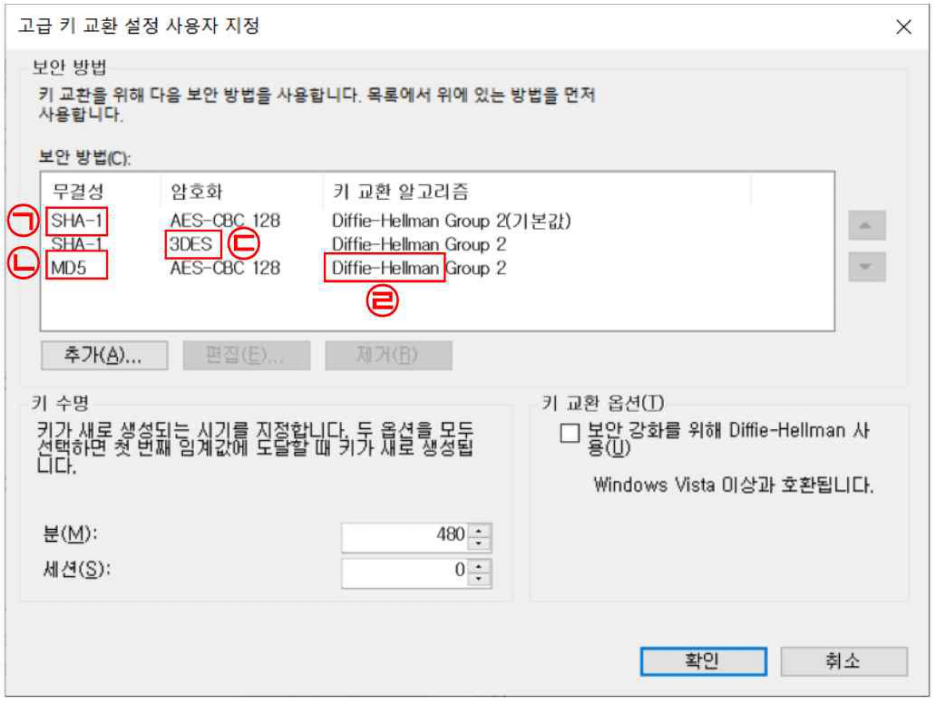
최초 로그인 단계의 TGT 발급은 AS, TGT를 제시한 뒤의 서비스 티켓 발급은 TGS로 구분한다. ‘모든 사용자’, ‘인증 없이’처럼 인증 절차를 생략하는 표현이 있으면 틀린 선지인지 확인한다.

암기 포인트

AS는 최초 인증과 TGT, TGS는 인증된 사용자의 서비스 티켓, KDC는 사용자·서비스 비밀키의 중앙 관리이다.

NoteBase

문 13. 다음 그림은 Windows Defender 방화벽의 IPsec 설정화면이다. ㉠~㉣에 관한 설명으로 가장 적절하지 않은 것은?



① ㉠ SHA-1의 해시값 길이는 160bits 이다.

② ㉡ MD5의 해시값 길이는 128bits 이다.

③ ㉢ 3DES는 256bits의 키 크기를 갖는 일방향 해시함수이다.

④ ㉣ Diffie-Hellman은 두 사용자 간에 공통키를 안전하게 공유할 수 있는 키 교환 알고리즘이다.

정답 3번

출제 포인트

그림에서 ㉠은 SHA-1, ㉡은 MD5, ㉢은 3DES, ㉣은 Diffie-Hellman을 가리킨다. 각 알고리즘이 해시함수, 대칭키 암호, 키 교환 중 어디에 속하는지와 대표적인 길이를 구분하는 문제이다.

NoteBase

선지별 해설

① O — SHA-1은 입력을 160비트 길이의 해시값으로 변환하는 일방향 해시함수이다.
② O — MD5는 128비트 길이의 해시값을 출력하는 일방향 해시함수이다.
③ X — '256비트의 키 크기를 갖는 일방향 해시함수'라는 표현이 틀렸다. 3DES는 DES를 세 번 적용하는 대칭키 블록 암호이며, 해시함수가 아니다. 세 개의 독립적인 DES 키를 사용하는 방식의 키 길이는 패리티 비트를 제외하고 168비트이다.
④ O — Diffie-Hellman은 통신 당사자가 공개된 통신로에서 공통 비밀값을 만들어 공유할 수 있게 하는 키 교환 알고리즘이다.

오답 포인트

③은 3DES라는 암호 알고리즘을 SHA-1·MD5와 같은 해시함수로 혼동하게 만든다. 그림에서 3DES가 '암호화' 열에 있고 SHA-1·MD5가 '무결성' 열에 있다는 위치도 이 구분을 보여 준다.

다시 나오면 이렇게 판단

먼저 그림의 열 제목과 알고리즘 이름을 연결한다. SHA-1·MD5는 고정 길이 해시값을 만드는 해시함수, 3DES는 대칭키 블록 암호, Diffie-Hellman은 공통 비밀값을 합의하는 키 교환 알고리즘으로 분류한다.

암기 포인트

SHA-1은 160비트, MD5는 128비트 해시값을 출력하며, 3DES는 해시가 아닌 대칭키 암호이고 Diffie-Hellman은 키 교환이다.

NoteBase

문 14. 다음은 네트워크 공격에 대한 설명이다. 빈칸 ㉠에 들어갈 용어로 옳은 것은?

스니핑 공격의 주된 종류로는 ARP 우회공격(ARP redirect), ICMP 우회공격(ICMP redirect), 포트 미러링(Port mirroring), 스위치 재밍(Switch Jamming) 등이 있다.
㉠ 공격은 위조된 매체 접근 제어(MAC) 주소를 지속적으로 네트워크로 흘려보내 스위치 저장 기능을 혼란시켜 더미 허브(dummy hub)처럼 작동토록 하는 공격이다. 스위치를 직접 공격하며, MAC 테이블을 위한 캐시 공간에 버퍼 오버플로우 공격을 실시하는 것과 같다. 스위치는 자신이 가지고 있는 MAC 테이블 저장 공간이 가득 차면 네트워크 패킷을 브로드캐스트하는 특성이 있는데 이를 이용한 공격 방법이라고 할 수 있다.

① ARP 우회공격(ARP redirect)
② ICMP 우회공격(ICMP redirect)
③ 포트 미러링(Port mirroring)
④ 스위치 재밍(Switch Jamming)

정답 4번

출제 포인트

위조한 MAC 주소를 대량으로 보내 스위치의 MAC 테이블을 가득 채우고, 프레임을 모든 포트로 흘려보내게 만드는 공격을 구별하는 문제이다.

핵심 개념

스위치 재밍은 다수의 위조된 출발지 MAC 주소를 스위치에 보내 MAC 테이블의 저장 공간을 소진시키는 공격이다. MAC 테이블이 포화되면 스위치는 목적지 포트를 특정하지 못한 프레임을 여러 포트로 플러딩하므로, 공격자가 다른 장치의 통신을 스니핑할 수 있게 된다.
ARP 우회공격은 위조 ARP 정보를 이용해 피해자의 ARP 캐시를 변조하고 통신이 공격자를 거치게 하는 방식이고, ICMP 우회공격은 위조 ICMP Redirect 메시지로 패킷의 경로를 바꾸는 방식이다. 포트 미러링은 지정한 포트의 트래픽을 감시용 포트로 복제하는 스위치 기능이다.

NoteBase

선지별 해설

① X — ARP 우회공격은 위조 ARP 응답 등으로 ARP 캐시의 IP 주소와 MAC 주소 대응 관계를 변조해 트래픽을 공격자 쪽으로 우회시킨다. 틀린 표현은 ‘MAC 테이블의 저장 공간을 가득 채운다’는 공격 방식과 ARP 우회공격을 연결한 부분이며, 올바르게는 ARP 캐시를 변조하는 공격이다.
② X — ICMP 우회공격은 위조된 ICMP Redirect 메시지를 보내 호스트의 라우팅 경로를 공격자가 원하는 방향으로 바꾸는 공격이다. 틀린 표현은 ‘위조 MAC 주소를 계속 보내 스위치의 MAC 테이블을 포화시킨다’는 동작을 ICMP 우회공격으로 본 부분이며, 올바르게는 ICMP 메시지를 악용해 경로를 변경하는 공격이다.
③ X — 포트 미러링은 특정 포트의 송수신 트래픽을 별도의 감시 포트로 복제하는 스위치의 관리·분석 기능이다. 틀린 표현은 포트 미러링이 ‘위조 MAC 주소로 MAC 테이블을 넘치게 하는 공격’이라는 부분이며, 올바르게는 설정된 트래픽을 감시 포트로 복사하는 기능이다.
④ O — 스위치 재밍은 대량의 위조 MAC 주소를 흘려보내 스위치의 MAC 테이블을 포화시키고, 스위치가 프레임을 여러 포트로 플러딩하게 만든다. 제시문의 공격 방식과 정확히 일치한다.

오답 포인트

네 공격 모두 스니핑과 관련될 수 있어 결과만 보면 혼동하기 쉽다. 제시문의 결정적 표현은 ‘위조된 MAC 주소를 지속적으로 전송’, ‘MAC 테이블 저장 공간 포화’, ‘더미 허브처럼 브로드캐스트’이며, 이는 ARP 캐시 변조나 경로 변경이 아니라 스위치 재밍의 특징이다.

다시 나오면 이렇게 판단

MAC 테이블을 대량의 가짜 주소로 채워 플러딩을 유발하면 스위치 재밍, ARP 캐시의 주소 대응을 속이면 ARP 우회공격, ICMP Redirect로 경로를 바꾸면 ICMP 우회공격, 트래픽을 감시 포트로 복제하면 포트 미러링으로 판단한다.

암기 포인트

가짜 MAC 대량 주입 → MAC 테이블 포화 → 허브처럼 플러딩 = 스위치 재밍이다.

NoteBase

문 15. 사물인터넷에 사용되는 무선통신 프로토콜로 가장 적절하지 않은 것은?

① NFT

② LoRA

③ ZigBee

④ Bluetooth

정답 1번

출제 포인트

사물인터넷에서 기기 간 무선 연결에 쓰이는 통신 기술과, 통신 기술이 아닌 디지털 자산 개념을 구별하는 문제이다.

핵심 개념

LoRa, ZigBee, Bluetooth는 통신 거리·전력 소비·전송 속도에는 차이가 있지만 모두 사물인터넷 기기의 무선 연결에 활용된다. 반면 NFT는 블록체인에서 자산의 고유성과 소유 관계를 나타내는 대체 불가능 토큰으로, 무선통신 프로토콜이 아니다.

선지별 해설

① X — NFT는 블록체인 기반의 대체 불가능 토큰을 뜻하며, 사물인터넷 기기가 무선으로 데이터를 주고받기 위한 통신 프로토콜이 아니다. 틀린 표현은 '사물인터넷에 사용되는 무선통신 프로토콜로서의 NFT'이며, 올바르게는 NFT가 디지털 자산의 고유성과 소유 관계를 표현하는 토큰이라고 해야 한다.
② O — 문항의 LoRA는 일반적으로 LoRa를 가리키는 표현이다. LoRa는 저전력으로 장거리 통신을 지원하여 센서 등 사물인터넷 기기의 통신에 활용되는 LPWAN 계열 기술이다.
③ O — ZigBee는 저전력·저속·근거리 무선 네트워크에 적합하여 스마트홈 센서와 제어 장치 등 사물인터넷 환경에 활용된다.
④ O — Bluetooth는 근거리 무선통신 기술이며, 특히 Bluetooth Low Energy는 낮은 전력 소비가 필요한 웨어러블과 각종 사물인터넷 기기에 널리 활용된다.

오답 포인트

NFT가 블록체인·디지털 기술 용어라는 이유만으로 통신 기술이라고 착각하기 쉽다. 핵심은 '디지털 분야의 용어인가'가 아니라 '기기 사이의 무선 데이터 전송을 담당하는가'이다.

다시 나오면 이렇게 판단

각 용어가 무선 연결 방식인지 먼저 확인한다. 통신 거리, 전력 소비, 주파수, 데이터 전송과 관련된 기술이면 무선통신 후보이고, 자산의 소유권이나 고유성을 나타내는 토큰이면 통신 프로토콜에서 제외한다.

NoteBase

암기 포인트

LoRa·ZigBee·Bluetooth는 무선 연결, NFT는 블록체인 토큰이다.

NoteBase

문 16. i-PIN(Internet Personal Identification Number)에 관한 설명으로 가장 적절하지 않은 것은?

① i-PIN 노출시 폐지/신규 발급이 가능하다.

② 주민등록번호 유출의 위험을 예방할 수 있다.

③ 주민등록번호는 개별 웹사이트에 저장된다.

④ 신원 확인 후 본인 확인 기관에서 i-PIN을 발급한다.

정답 3번

출제 포인트

이 문제는 i-PIN이 주민등록번호를 개별 웹사이트에 제공하지 않고 온라인에서 본인을 확인하게 하는 대체수단이라는 점을 묻는다.

핵심 개념

i-PIN은 인터넷에서 주민등록번호 대신 사용하는 개인 식별번호이다. 본인확인기관이 신원을 확인한 뒤 발급하며, 이용자는 개별 웹사이트에 주민등록번호를 제공하지 않고 본인확인을 할 수 있다.

선지별 해설

① O — i-PIN이 노출된 경우 기존 i-PIN을 폐지하고 새로 발급받을 수 있으므로 노출에 대응할 수 있다.
② O — 개별 웹사이트에 주민등록번호를 직접 제공하지 않으므로 웹사이트를 통한 주민등록번호 유출 위험을 줄일 수 있다.
③ X — 틀린 표현은 '주민등록번호는 개별 웹사이트에 저장된다'이다. 올바르게는 개별 웹사이트가 주민등록번호를 저장하는 대신 i-PIN으로 본인확인 결과를 이용한다.
④ O — i-PIN은 본인확인기관이 신청자의 신원을 확인한 후 발급한다.

오답 포인트

③은 i-PIN의 도입 목적을 정반대로 서술한 선지이다. i-PIN은 주민등록번호가 여러 웹사이트에 흩어져 저장되는 위험을 줄이기 위한 수단이지, 주민등록번호를 개별 웹사이트에 저장하게 하는 수단이 아니다.

다시 나오면 이렇게 판단

개별 웹사이트가 주민등록번호를 직접 수집·저장한다는 설명은 i-PIN의 핵심 취지와 반대이므로 틀린 것으로 판단한다. 발급 주체는 본인확인기관이고, 노출 시에는 폐지 후 새로 발급받을 수 있다는 점도 함께 확인한다.

암기 포인트

i-PIN은 '주민등록번호 대신 사용, 본인확인기관 발급, 개별 웹사이트에는 주민등록번호 미저장'으로 정리한다.

NoteBase

문 17. 다음 설명에 해당하는 것으로 가장 적절한 것은?

· 시스템에 설치되어 그 존재의 흔적을 최대한 숨기면서 공격자가 언제든지 시스템에 관리자 권한으로 접근할 수 있도록 비밀통로를 지속적으로 유지 시켜 주는 프로그램 집합이다.
· 프로세스/스레드 감추기, 프로세스 보안 설정 변경 및 제거, 파일/폴더 감추기, 레지스트리/서비스 감추기 등의 기능을 가진다.

① 쿠키(cookie)
② 루트킷(rootkit)
③ 스파이웨어(spyware)
④ 블록체인(blockchain)

정답 2번

출제 포인트

시스템 내부에서 자신의 존재와 악성 활동을 숨기고 공격자의 관리자 권한 접근을 지속시키는 루트킷의 특징을 구별하는 문제이다.

핵심 개념

루트킷은 시스템에 침투한 뒤 프로세스·파일·레지스트리·서비스 등을 감추고 공격자의 특권 접근을 유지하도록 하는 악성 도구의 집합이다. 핵심 키워드는 '흔적 은폐'와 '관리자 권한 접근 유지'이다.
쿠키는 웹사이트 이용 정보를 저장하는 작은 데이터이고, 스파이웨어는 사용자 정보를 몰래 수집하는 악성 프로그램이며, 블록체인은 거래 기록을 여러 참여자가 분산하여 저장·검증하는 기술이다.

선지별 해설

① X — 쿠키는 웹사이트가 로그인 상태나 이용 설정 등을 기억하기 위해 브라우저에 저장하는 데이터이다. '쿠키'라는 표현이 틀렸으며, 제시문처럼 흔적을 숨기고 관리자 권한 접근을 유지하는 것은 루트킷이다.
② O — 루트킷은 프로세스·스레드·파일·폴더·레지스트리·서비스 등을 은폐하고 공격자가 높은 권한으로 다시 접근할 수 있게 한다. 제시문의 두 핵심 특징과 일치한다.
③ X — 스파이웨어는 사용자의 활동이나 개인정보를 몰래 수집하여 외부로 전달하는 데 초점이 있다. '스파이웨어'라는 표현이 틀렸으며, 은폐 기능과 관리자 권한 접근의 지속적 유지를 중심으로 하는 것은 루트킷이다.
④ X — 블록체인은 기록을 여러 참여자에게 분산 저장하고 합의에 따라 검증하는 기술이다. '블록체인'이라는 표현이 틀렸으며, 제시된 악성 프로그램 집합은 루트킷이다.

NoteBase

오답 포인트

악성 프로그램이라는 넓은 범주만 보고 스파이웨어를 고르기 쉽다. 그러나 제시문의 '프로세스·파일·레지스트리 등을 감춤'과 '관리자 권한 접근을 지속적으로 유지'라는 표현은 정보 수집이 중심인 스파이웨어가 아니라 루트킷을 가리킨다.

다시 나오면 이렇게 판단

정보를 몰래 수집하면 스파이웨어, 시스템 구성요소와 자신의 흔적을 숨기면서 특권 접근을 유지하면 루트킷으로 판단한다.

암기 포인트

루트킷은 '은폐 + 관리자 권한 접근 유지'이다.

NoteBase

문 18. 국내에서 개발한 암호 알고리즘에 관한 설명으로 가장 적절하지 않은 것은?

① ARIA(Academy Research Institute Agency)는 ISPN 구조의 128bits 블록 암호로 키의 길이에 따라 ARIA-128, ARIA-192, ARIA-256으로 구분한다.

② HIGHT(HIGh security and light weigHT)는 비교적 간단한 연산으로 빠른 암호화 복호화 기능을 제공하며 32bits, 64bits, 128bits 블록 크기를 가진 블록 암호 알고리즘이다.

③ LEA(Lightweight Encryption Algorithm)는 128bits 경량 블록 암호 알고리즘으로 스마트폰 보안, 사물인터넷(IoT) 등 저전력 암호화에 널리 사용된다.

④ SEED는 암호전문가들이 개발한 알고리즘으로 2005년 국제표준화 기구인 ISO/IEC 및 IETF에서 국제 블록 암호 알고리즘 표준으로 제정되었다.

정답 2번

출제 포인트

국산 블록 암호인 ARIA, HIGHT, LEA, SEED의 블록 크기와 키 길이를 구분하는 문제이다.

핵심 개념

블록 크기는 한 번에 암호화하는 평문의 단위이고, 키 길이는 암호화에 사용하는 비밀키의 길이이다. ARIA와 LEA는 128비트 블록에 128·192·256비트 키를 사용하고, HIGHT는 64비트 블록에 128비트 키를 사용한다. SEED는 128비트 블록과 128비트 키를 사용한다.

선지별 해설

① O — ARIA는 ISPN 구조의 128비트 블록 암호이며, 키 길이에 따라 ARIA-128, ARIA-192, ARIA-256으로 구분한다.
② X — 틀린 표현은 '32비트, 64비트, 128비트 블록 크기'이다. HIGHT의 블록 크기는 64비트로 고정되고 키 길이는 128비트이다. 32비트·64비트·128비트를 서로 다른 블록 크기로 지원하는 알고리즘이 아니다.
③ O — LEA는 128비트 블록을 사용하는 경량 블록 암호로, 단순한 산술·논리 연산을 중심으로 구현되어 모바일 기기나 사물인터넷과 같은 저전력 환경에 적합하다.
④ O — SEED는 국내 암호 전문가들이 개발한 128비트 블록 암호이며, 2005년에 ISO/IEC 국제표준에 포함되고 IETF 문서로도 규격화되었다.

오답 포인트

②는 HIGHT와 관련된 숫자 32, 64, 128을 나열하여 모두 블록 크기인 것처럼 보이게 한다. HIGHT에서 64비트는 블록 크기이고 128비트는 키 길이이며, 32는 블록 크기 종류가 아니다.

NoteBase

다시 나오면 이렇게 판단

국산 블록 암호 문제에서는 먼저 블록 크기와 키 길이를 분리해 확인한다. HIGHT는 '64비트 블록·128비트 키'로 고정하여 판단하고, ARIA와 LEA는 '128비트 블록·128/192/256비트 키'로 구분한다.

암기 포인트

HIGHT는 64블록·128키, ARIA와 LEA는 128블록·세 가지 키, SEED는 128블록·128키이다.

NoteBase

문 19. 다음은 암호 알고리즘의 키 쌍 생성 과정이다. 위의 키 쌍 생성 과정을 적용한 암호 알고리즘으로 가장 적절한 것은?

- 공개키 : E, N
- 개인키 : D, N
- 최소공배수(LCM, Least Common Multiple)
- 최대공약수(GCD, Greatest Common Division)

단계 1 : N을 구한다.
의사난수 생성기로 p와 q를 구한다. (p와 q는 소수) N = p × q
단계 2 : L을 구한다.
L = LCM(p-1, q-1) (L은 p-1과 q-1의 최소공배수)
단계 3 : E를 구한다.
1 < E < L GCD(E, L) = 1
단계 4 : D를 구한다.
1 < D < L E × D mod L = 1

① ECC

② RSA

③ ElGamal

④ Diffie-Hellman

정답 2번

출제 포인트

서로 다른 두 소수 p, q로 $N = pq$를 만들고, $L = \text{lcm}(p-1, q-1)$에 대하여 E D ≡ 1 ±od L이 되도록 공개 지수 E와 개인 지수 D를 정하는 과정은 RSA의 키 생성 절차이다.

NoteBase

선지별 해설

① X
ECC는 타원곡선 위의 점과 스칼라 곱을 이용해 키를 생성한다. 선지의 'ECC'가 틀렸으며, 제시된 절차에 해당하는 알고리즘은 RSA이다.

② O
RSA는 두 소수 p, q의 곱 N을 법으로 사용하고, $L = \mathrm{lcm}(p-1, q-1)$과 서로소인 E를 선택한 뒤 D를 E의 모듈러 역원으로 정한다. 따라서 공개키는 (E, N), 개인키는 (D, N)이 된다.

③ X
ElGamal은 유한군의 이산로그 문제를 바탕으로 개인키 x와 공개키 $y = g^x$를 생성한다. 선지의 'ElGamal'이 틀렸으며, 두 소수의 곱과 서로 역원인 지수 E, D를 사용하는 것은 RSA이다.

④ X
Diffie-Hellman은 각 참여자가 비밀 지수를 정하고 g^a, g^b 같은 공개값을 교환해 공통 비밀 g^{ab}를 만드는 키 합의 방식이다. 선지의 'Diffie-Hellman'이 틀렸으며, 제시된 공개키·개인키 생성 절차는 RSA이다.

오답 포인트

공개키 암호와 관련된 알고리즘 이름만 보고 고르면 혼동하기 쉽다. 이 문항의 결정적 단서는 $N = pq$, $L = \mathrm{lcm}(p-1, q-1)$, $\gcd(E, L) = 1$, E D ≡ 1 ±od L이라는 네 조건이다.

다시 나오면 이렇게 판단

두 소수의 곱으로 법 N을 만들고 공개 지수와 개인 지수를 모듈러 역원 관계로 정하면 RSA로 판단한다. 타원곡선의 점 연산이면 ECC, 생성원 거듭제곱과 이산로그 구조이면 ElGamal이나 Diffie-Hellman을 검토한다.

암기 포인트

RSA는 '두 소수의 곱 N + 서로 역원인 공개·개인 지수 E, D'로 기억한다.

NoteBase

문 20. 다음은 암호 알고리즘의 키 쌍 생성 과정이다. 다음과 같이 값과 식이 주어질 때 위의 암호 알고리즘의 키 쌍 생성 과정에 따라 평문 M을 암호화한다. 암호문 C의 값으로 옳은 것은?

- 공개키 : E, N
- 개인키 : D, N
- 최소공배수(LCM, Least Common Multiple)
- 최대공약수(GCD, Greatest Common Division)

단계 1 : N을 구한다.
의사난수 생성기로 p와 q를 구한다. (p와 q는 소수) $N = p \times q$
단계 2 : L을 구한다.
$L = LCM(p-1, q-1)$ (L은 p-1과 q-1의 최소공배수)
단계 3 : E를 구한다.
$1 < E < L$ $GCD(E, L) = 1$
단계 4 : D를 구한다.
$1 < D < L$ $E \times D \bmod L = 1$

p=3, q=11, E=7, 평문 M=4, 암호문 C = ?

① 13

② 14

③ 15

④ 16

정답 4번

출제 포인트

RSA에서 공개키 E, N을 구한 뒤 암호화식 C=M^E N으로 암호문을 계산하는 문제이다.

조건 정리

주어진 값: $p = 3, q = 11, E = 7, M = 4$

구해야 할 값: 암호문 C

먼저 $N = pq = 3 \times 11 = 33$을 구한다. 또한 $L = \text{LCM}(p-1, q-1) = \text{LCM}(2, 10) = 10$이고

$\gcd(7, 10) = 1$이므로 $E = 7$은 공개 지수 조건을 만족한다.

NoteBase

사용할 공식

RSA 암호화식은 C=M^E N이다. 평문을 공개 지수만큼 거듭제곱한 뒤 공개 모듈러스 N으로 나눈 나머지가 암호문이므로 이 공식을 사용한다.

계산 과정

$N = 3 \times 11 = 33$이다.
$4^2 = 16$이고, 4^4=256≡25±od33이다.
따라서 4^7=4^4×4^2×4≡25×16×4=1600≡16±od33이다.
그러므로 암호문은 $C = 16$이다.

선지 판단

① X — 13은 4^7을 33으로 나눈 나머지가 아니다. 틀린 값 13은 올바르게는 16이다.
② X — 14는 모듈러 거듭제곱 결과와 일치하지 않는다. 틀린 값 14는 올바르게는 16이다.
③ X — 15는 160033의 값이 아니다. 틀린 값 15는 올바르게는 16이다.
④ O — 4^7≡16±od33이므로 암호문 C는 16이다.

오답 포인트

공개 지수 $E = 7$을 암호문 자체로 보거나 4×7처럼 단순 곱셈하는 것이 함정이다. RSA 암호화는 곱셈이 아니라 거듭제곱 후 N으로 나눈 나머지를 구하는 연산이다.

다시 나오면 이렇게 판단

RSA 계산에서는 먼저 $N = pq$를 구하고, 공개키의 지수 E를 사용하여 M^E N을 계산한다. 큰 거듭제곱은 제곱을 반복하면서 매 단계 나머지를 줄이면 된다.

암기 포인트

RSA 암호화는 공개키로 C=M^E N, 복호화는 개인키로 M=C^D N이다.

NoteBase