정보보호론	국가 전산 7급	2024년 10월 12일

♠ 합격선/필기합격인원(90점/47명) - 선발예정인원 35명 ♠

1. 다음에서 설명하는 디지털 포렌식의 기본 원칙은? [2024년 국가 7급]

> 증거는 절차를 통해 삭제 또는 손상된 파일이 복구되는 과정을 거칠 수 있다. 이 증거를 법정에 제출하려면 같은 환경에서 같은 결과가 나와야 한다.

① 재현의 원칙
② 신속성의 원칙
③ 무결성의 원칙
④ 연계보관성의 원칙

♤ **디지털 포렌식 기본 원칙**

① 정당성의 원칙
모든 증거는 **적법한 절차**를 거쳐서 획득되어야 한다.

② 신속성의 원칙
컴퓨터 내부의 **정보 획득은 신속**하게 이루어져야 한다.**(휘발성 정보 수집 등을 위해)**

③ 연계보관성의 원칙
수집, 이동, 분석, 검토, 보관, 법정 제출의 각 단계에서 **증거를 명확하게 관리**
이를 만족하려면 증거를 전달하고 전달받는 데 관여한 담당자와 책임자를 명시해야 한다.

④ 무결성의 원칙
획득된 정보는 **위변조**되지 않았음을 입증할 수 있어야 한다.

⑤ 재현의 원칙
증거자료는 **같은 환경에서 같은 결과**가 나오도록 재현이 가능해야 한다.
동일한 조건에서 현장 검증을 실시하면, 피해 당시와 동일한 결과가 나와야 한다.

디지털 포렌식	• 디지털 포렌식은 정보기기에 저장된 디지털 자료를 근거로 사법기관에 전자 증거물을 제출하기 위해 증거 수집, 분석, 보고서 작업 등을 처리하는 일련의 작업이다. • 과거에 얻기 어려웠던 증거들을 제공해주는 획기적인 방법이다.

정답 : ①

2. RSA 공개키 암호에서 공개키를 (n=11×13, e=7)로 설정하였을 때, 공개키에 대응하는 개인키 d값은? [2024년 국가 7급]

① 41
② 87
③ 97
④ 103

♤ RSA 암호

① 먼저, 서로 다른 임의의 두 소수를 선택한다.
p = **11**, q = **13**

② n = p × q를 구한다.
n = p × q = 11 × 13 = **143**

③ n의 오일러 파이 함수 $\Phi(n)$ = (p−1)(q−1)을 구한다.
$\Phi(n)$ = Φ(**143**) = (p−1)(q−1) = (11−1)(13−1) = **120**

④ **1 < e < Φ(n)**인 정수 중에서 **Φ(n)**과 **서로소**인 임의의 수 **e**를 선택한다.
→ 즉, **1 < e < 120**인 정수 중에서 **120**과 **서로소**인 임의의 수 **e**를 선택한다.
→ 이를 어렵게 표현하면, Z_{120}^{*}에서 임의의 수 **e**를 선택한다.
→ 문제에서 **e = 7**이 선택되었다.**(e는 공개키)**

⑤ d와 e를 곱하여 $\Phi(n)$으로 나눈 **나머지가 1**이 되는 **d**를 구한다.
(d × e) mod $\Phi(n)$ = **1**
(d × **7**) mod 120 = **1**
↓**개인키 d = 103** ←←←←←←←←←← **정답**
(**103** × **7**) mod 120 = **1**
721 mod 120 = **1**

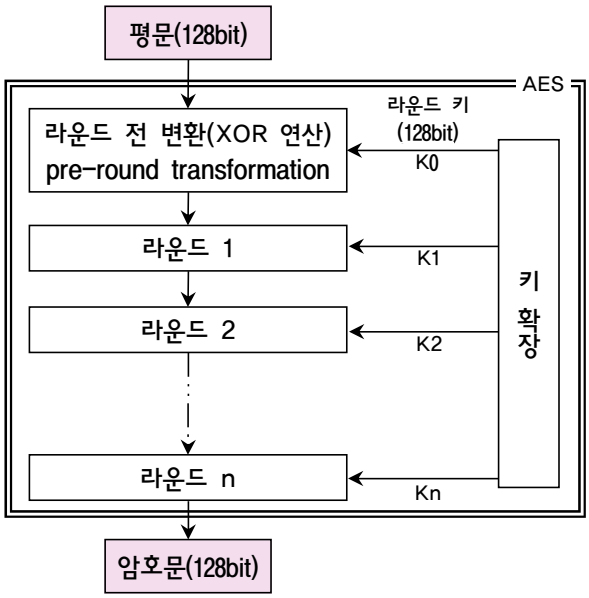
⑥ 최종적으로 생성된 키 관계는 다음과 같다.
• 공개키 **(e, n) = (7, 143)**
• 개인키 **(d, n) = (103, 143)**

정답 : ④

3. AES의 암호화 과정에서 마지막 라운드에 포함되지 않는 연산은? [2024년 국가 7급]

① SubBytes
② ShiftRows
③ MixColumns
④ AddRoundKey

♤ AES 암호



종류	암호키	라운드	라운드 키 수
AES-128	128bit	10	11
AES-192	192bit	12	13
AES-256	256bit	14	15

• AES는 각 라운드에서 사용할 **라운드 키**를 생성하기 위해 **키 확장** 과정을 거친다.
• **라운드 키**는 **암호키(128bit)**를 이용하여, **키 확장** 과정을 통해 생성된다.

// AES 라운드 함수

AES 암호 알고리즘은 안전성을 위해 각 라운드는 다음 **4가지 단계의 변환**을 적용한다.

① **바이트 치환(substitute byte)**	S-box 표를 이용하여 바이트 단위로 블록 교환**(대치)**
② **행 이동(shift row)**	P-box, 단순히 행과 행을 이동**(전치)**
③ **열 혼합(mix column)**	행렬 곱셈 연산(행렬을 사용하여 열의 각 바이트를 **대치**)
④ **라운드 키 더하기(add round key)**	확장된 키의 일부와 현재 블록을 XOR 연산**(대치)**

• **각 라운드**는 **마지막**을 **제외**하고 **4개의 변환**을 사용한다.
• 암호의 **마지막 라운드**는 MixColumns을 제외한 **3의 변환**을 사용한다.

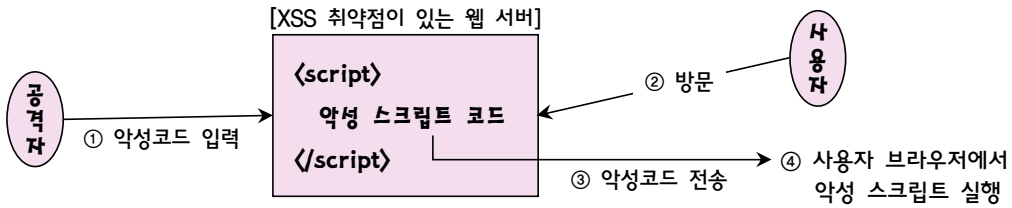
정답 : ③

4. 다음 설명에 해당하는 공격 기법은? [2024년 국가 7급]

브라우저로 전달되는 데이터에 악성 스크립트가 포함되어 사용자의 브라우저에서 실행되면서 해킹이 수행된다. 일반적인 공격 목적은 웹 사용자의 정보를 추출하는 것이다.

① XSS(Cross Site Scripting)
② 리버스 텔넷(Reverse Telnet)
③ 디렉터리 리스팅(Directory Listing)
④ SQL(Structured Query Language) Injection

♤ XSS(Cross Site Scripting) 공격



- 공격자가 XSS 취약점이 있는 웹 서버에 공격용 스크립트를 입력시켜 놓으면,
- 방문자가 악성 스크립트가 삽입된 페이지를 읽는 순간 방문자의 브라우저를 공격하는 방식
- 유명 **온라인 게시판**, 웹 기반 이메일 및 사용자 프로필 등에 악성 스크립트를 포함하면,
- 다른 방문자들이 해당 페이지를 읽어보는 즉시 악성 스크립트가 브라우저에서 실행된다.

// 예 : 쿠키값을 보여주는 스크립트
〈script〉
alert(document.cookie) → 이 부분에 공격용 악성코드를 포함시킬 수 있다.
〈/script〉

정답 : ①

5. 리눅스 시스템 명령어와 기능의 설명 중 옳지 않은 것은? [2024년 국가 7급]

① mv – 파일의 이름 변경과 이동
② chmod – 파일의 사용 권한 변경
③ rm – 파일 및 디렉터리 목록 보기
④ umask – 생성하는 디렉터리의 기본 권한 설정

♤ **리눅스 시스템 명령어**

- rm은 'Remove'의 약자
- rm은 파일 또는 디렉터리를 삭제하는 명령어이다.

정답 : ③

6. 윈도 명령 프롬프트 창에서 명령어 (가)를 실행한 화면의 일부이다. 이에 대한 설명으로 옳지 않은 것은? (단, 게이트웨이의 IP 주소는 172.21.70.1이고, 공격자의 IP 주소는 172.21.70.227이다) [2024년 국가 7급]

C: \ Users \ windows> (가)		
Interface: 172.21.70.180 --- 0xb		
Internet Address	Physical Address	Type
172.21.70.1	18-67-e0-4d-40-5c	dynamic
172.21.70.2	00-0c-db-58-27-2d	dynamic
172.21.70.227	18-67-e0-4d-40-5c	dynamic
172.21.70.253	00-0e-5e-fc-16-c4	dynamic

① 명령어 (가)는 arp -a이다.
② 게이트웨이의 ARP 테이블을 보여주는 화면이다.
③ 공격 대상의 IP 주소는 172.21.70.180임을 나타낸다.
④ 게이트웨이의 MAC 주소와 공격자의 MAC 주소가 같은 상태이다.

♤ **arp -a : arp 테이블의 모든 항목을 출력**

- 먼저, 주어진 문제는 **ARP 스푸핑 공격**에 대한 질문이다.
- 해서, 게이트웨이의 MAC 주소와 공격자의 MAC 주소가 같은 상태이다.

C: \ Users \ windows> arp -a			← **공격 대상 컴퓨터**
Interface: 172.21.70.180 --- 0xb			← **공격 대상의 IP 주소**
Internet Address	Physical Address	Type	
172.21.70.1	18-67-e0-4d-40-5c	dynamic	← **게이트웨이**
172.21.70.2	00-0c-db-58-27-2d	dynamic	
172.21.70.227	18-67-e0-4d-40-5c	dynamic	← **공격자**
172.21.70.253	00-0e-5e-fc-16-c4	dynamic	

- ARP 스푸핑은 공격자가 자신이 게이트웨이라고 **속이는 것**이다.
- ARP 스푸핑은 공격 대상 컴퓨터의 모든 정보를 **도청**할 수 있다.

- **게이트웨이의 ARP 테이블**을 보여주는 화면이다.(×)
  → **공격 대상 컴퓨터의 ARP 테이블**을 보여주는 화면이다.
- ARP 스푸핑을 수행하려면 **공격 대상 컴퓨터**의 **ARP 테이블**을 **확인**해야 함(arp-a)
- [0xb]는 네트워크 접속기(adapter)를 나타낸다.

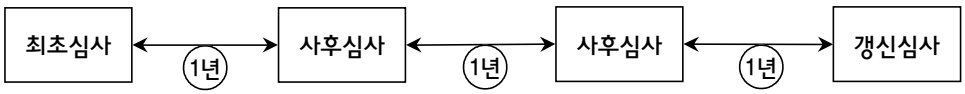
정답 : ②

7. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 규정하고 있는 인증에 대한 설명으로 옳지 않은 것은? [2024년 국가 7급]

① 인증심사의 종류는 예비심사, 최초심사, 사후심사, 갱신심사가 있다.
② 정보보호 관리체계 인증은 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 것이다.
③ 정보보호 및 개인정보보호 관리체계 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리 단계별 요구사항의 세 부분으로 구성되어 있다.
④ 최초심사를 통해 인증을 취득하면 3년의 유효기간이 부여되며, 유효기간 중 매년 1회 이상 사후심사를 신청하여야 한다.

♤ ISMS-P 심사 종류

• **인증심사**의 종류는 **예비심사**, 최초심사, 사후심사, 갱신심사가 있다.**(×)**
→ **인증심사**의 종류는 최초심사, 사후심사, 갱신심사가 있다.(**예비심사**는 없음)



정답 : ①

8. 블록암호 운영모드 중 암호화 과정에서 초기벡터(IV)를 사용하지 않는 것은? [2024년 국가 7급]

① CFB(Cipher Feedback)
② OFB(Output Feedback)
③ ECB(Electronic Codebook)
④ CBC(Cipher Block Chaining)

♤ 운영모드

모드	유형(type)	초기 벡터	오류전파	암호 병행처리	복호 병행처리	덧붙이기
ECB	**블록 암호**	불필요(none)	No	가능	가능	**사용**
CBC	**블록 암호**	필요(yes)	**Yes**	**불가**	가능	**사용**
CFB	**비동기** 스트림 암호	필요(yes)	**Yes**	**불가**	가능	미사용
OFB	동기 스트림 암호	필요(yes)	No	**불가**	**불가**	미사용
CTR	동기 스트림 암호	필요-카운터	No	가능	가능	미사용

• ECB는 초기벡터(IV)를 사용하지 않는다.

정답 : ③

9. TLS(Transport Layer Security) 1.3 프로토콜에 대한 설명으로 옳은 것만을 모두 고르면? (단, 세션 재개(resumption)와 PSK(Pre-Shared Key) 방식은 고려하지 않는다) [2024년 국가 7급]

> ㄱ. Handshake 프로토콜 이전에 클라이언트와 서버가 사용할 암호 알고리즘을 결정한다.
> ㄴ. Handshake 프로토콜에서 서버를 인증하려면 클라이언트는 서버의 인증서를 이용한다.
> ㄷ. Record 프로토콜에서 사용할 대칭키는 Handshake 프로토콜의 키교환으로부터 생성된다.
> ㄹ. Record 프로토콜에서 메시지 단편화, 암호화, 메시지인증코드 추가 등이 수행된다.

① ㄱ, ㄹ　　② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄹ　　④ ㄴ, ㄷ, ㄹ

♤ TLS

ㄱ. Handshake **프로토콜 이전**에 클라이언트와 서버가 사용할 암호 알고리즘을 결정한다.(×)
→ Handshake **프로토콜에서** 클라이언트와 서버가 사용할 암호 알고리즘을 협상한다.

정답 : ④

10. 다음과 같은 특성을 갖추고 있는 보안 모델은? [2024년 국가 7급]

> ○ 최초의 수학적 모델이다.
> ○ 강제적 접근통제 방식으로 접근을 통제하며, 시스템 내부에 있는 정보의 기밀성을 보호한다.
> ○ 주체는 주체보다 같거나 낮은 보안 수준의 객체만 읽을 수 있고, 주체보다 같거나 높은 보안 수준의 객체만 쓸 수 있다.

① 비바(Biba) 모델　　② 만리장성(Chinese Wall) 모델
③ 클락 - 윌슨(Clark-Wilson) 모델　　④ 벨 - 라파듈라(Bell-LaPadula) 모델

♤ **보안 모델**

BLP 모델	• 1973년, 미국의 Bell과 Lapadula가 개발한 **최초의 수학적 모델**이다. • 정보의 불법적 변조보다는 **기밀성 유지**에만 중점을 두고 있다. • 보안 등급을 이용한 **강제적** 보안 정책에 의한 접근통제 모델이다. • 상위레벨 읽기금지 정책(No-read-up policy, NRU) : [단순 보안 속성] • 하위레벨 쓰기금지 정책(No-write-down policy, NWD) : [*-속성]

정답 : ④