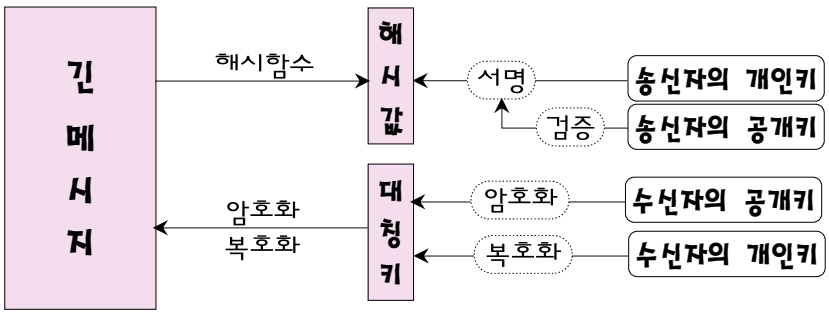
정보보호론	국가 전산 7급	2022년 10월 15일

♠ 필기합격인원/합격선(58명/77점) - 선발예정인원 48명 ♠

1. 송신자가 수신자에게 전달하는 세션키를 공개키 암호 방식을 이용하여 암호화할 때 사용되는 키는? [2022년 국가 7급]

① 송신자의 개인키 ② 송신자의 공개키
③ 수신자의 개인키 ④ 수신자의 공개키

♤ 하이브리드 암호시스템



• 메시지 암호화에 사용된 **대칭키(세션키)**는 **수신자의 공개키**로 암호한다.

정답 : ④

2. 다음의 정보보호와 관련된 원칙을 제시한 사람은? [2022년 국가 7급]

이 원칙은 공격자가 암호 알고리즘을 완전히 알고 있더라도 키가 없이는 복호화해 평문을 얻을 수 없어야 함을 의미하는 것으로, 암호 알고리즘의 안전성이 암호 알고리즘 설계 자체의 비밀성에 의존해서는 안 되고 키의 비밀성에 의존해야 함을 강조한다. 따라서 암호 알고리즘은 널리 공개해서 많은 암호학자의 검증을 거치는 과정을 통해 안전성을 인정받아야 한다.

---

① Rabin ② Hellman ③ Kerckhoffs ④ Koblitz

♤ 커크호프 원리(Kerckhoff's principle)

• **"암호시스템에서 키를 제외한 나머지는 모든 것이 공개되어도 안전해야 한다"**
• 현대 암호에서 **암호시스템의 안전성**은 Kerckhoff's principle에 기반한다.

정답 : ③

3. (가), (나)에 들어갈 용어를 바르게 연결한 것은? [2022년 국가 7급]

PGP 기법은 세션키로 메시지를 암호화하기 위해 [(가)] 알고리즘과
사용자 인증을 위한 전자서명에 이용하기 위해 [(나)] 알고리즘을 사용할 수 있다.

	(가)	(나)
①	IDEA	RSA
②	IDEA	DES
③	RSA	IDEA
④	RSA	AES

♤ PGP

(가) 세션키로 메시지 암호화는 대칭키 암호 알고리즘을 사용 : IDEA, DES, AES 등
(나) 사용자 인증을 위한 전자서명은 공개키 암호 알고리즘을 사용 : RSA

// PGP에서 사용되는 알고리즘

대칭키 알고리즘	AES, IDEA, Triple DES, Blowfish 등	메시지 기밀성
공개키 알고리즘	RSA, ElGamal, DSS, ECC, ECDSA 등	전자서명

정답 : ①

4. 쓰레기 처리장 또는 휴지통을 뒤져서 정보를 얻어내는 사회 공학적 공격 기법은? [2022년 국가 7급]

① Eavesdropping
② Shoulder Surfing
③ Dumpster Diving
④ Forensic Analysis

♤ **쓰레기통 다이빙(Dumpster diving)**

- 덤프스터 다이빙을 해석하면 **쓰레기 수거함**에 들어가서 쓸 만한 것을 가져간다는 말이다.
- 덤프스터 다이빙은 휴지통을 뒤져서 정보를 얻어내는 사회 공학적 공격 기법을 말한다.

- 이브즈드라핑(eavesdropping) : 엿듣기, 도청
- 숄더 서핑(shoulder surfing) : 어깨 너머로 개인의 기밀 데이터를 얻는 사회 공학적 공격
- 법의학적 분석(forensic analysis) : 범죄 조사와 관련된 증거를 검사하는 분석 도구 및 기법

정답 : ③

5. 접근제어(access control)에 대한 설명으로 옳지 않은 것은? [2022년 국가 7급]

① 임의적 접근제어(discretionary access control)는 정보 소유자가 정보의 보안 수준을 결정하고 그에 대한 접근제어까지 설정한다.

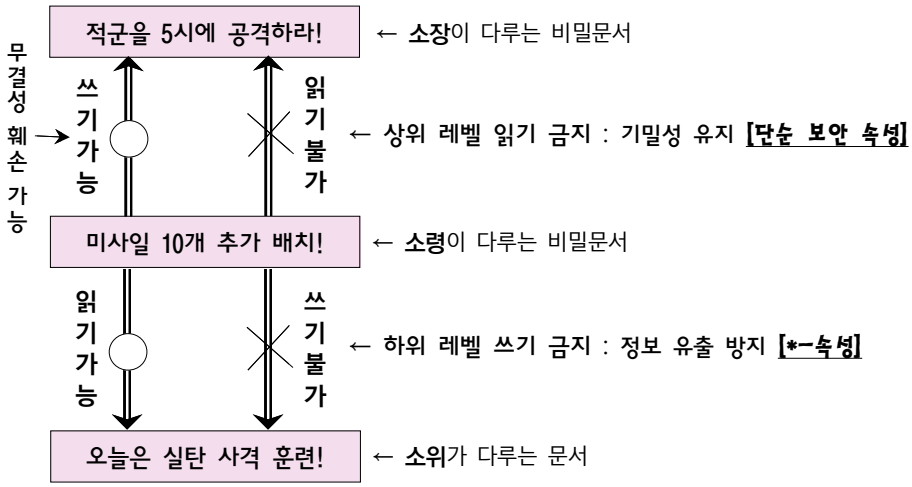
② BLP(Bell-LaPadula) 모델과 Biba 모델은 강제적 접근제어(mandatory access control) 모델에 해당한다.

③ 역할기반 접근제어(role-based access control)는 사람이 아닌 역할 또는 직책에 권한을 부여한다.

④ BLP 모델에서는 낮은 수준의 보안 권한을 가진 사람이 자신의 권한보다 높은 보안 수준의 문서에 쓸 수 없다.

♤ **접근제어 – BLP 모델**

- BLP 모델에서는 **낮은** 수준의 보안 권한을 가진 사람이 자신의 권한보다 **높은** 보안 수준의 문서에 **쓸 수 없다.(×) → 쓸 수 있다.**



정답 : ④

6. 윈도우 운영체제에서 컴퓨터의 MAC 주소를 출력하는 명령어는? [2022년 국가 7급]

① ping ② ipconfig/all ③ ifconfig ④ nslookup

♤ **ipconfig/all**

- IP주소, 서브넷마스크, MAC주소, 네트워크 상태 등을 확인 및 설정할 수 있다.

정답 : ②

7. 다음 /etc/passwd 파일 내용의 일부에서 사용자의 그룹 ID는? [2022년 국가 7급]

```
--------------------------------------------------
user05:x:1001:501:group05:/home/user05:/bin/bash
--------------------------------------------------
```

① x
② 1001
③ 501
④ group05

♤ /etc/passwd 파일

• user05:x:1001:501:group05:/home/user05:/bin/bash

↓보기 쉽도록 분리하면

①	②	③	④	⑤	⑥	⑦
user05	x	1001	**501**	group05	/home/user05	/bin/bash

개인정보	설 명
① 로그인 명	• 각 사용자 이름이다. 중복 불가 • login에 사용되는 이름이다. • 슈퍼유저는 통상적으로 root를 사용한다.
② 비밀번호	• 각 사용자의 비밀번호이다. 보통 알 수 없도록 변형한다. • 최소 6자 이상(영문자 2개 이상, 1개 이상의 수 또는 특수문자 포함) • /etc/passwd에는 비밀번호 위치에 문자 "**x**"가 기록된다.
③ 사용자 ID	• 사용자 ID(uid)는 0~65,535의 고유한 수이다. • 0은 슈퍼유저이다. • 관례적으로, 1~99는 잘 사용하지 않는다.
④ 그룹 ID	• 그룹 ID(gid)는 0~65,535의 고유한 수이다.(사용자 ID와 같다) • 관례적으로, 0~99는 잘 사용하지 않는다. • 그룹 ID는 각 사용자가 속하는 그룹의 고유번호이다. • 사용자 계정은 반드시 1개 이상의 그룹에 포함되어야 한다. • 등록시 그룹 번호를 지정하지 않으면, 디폴트로 1이 된다. • 그룹 번호 1은 "other" 그룹이다.
⑤ 설명	• 기타 사용자 정보이다. 보통 사용자 이름이다.
⑥ 홈 디렉터리	• 사용자의 절대경로 디렉터리 이름이다. • 단순히, cd를 입력하면 찾아가게 된다.
⑦ 로그인 셸	• 로그인 했을 때, 사용자가 사용하는 셸 프로그램 이름이다. • 이 필드가 빈칸이면, bin/sh로 간주된다. - 본 셸

정답 : ③

8. 다음은 블록 암호의 운영모드 중 하나를 표현하고 있다. 해당 운영모드에 대해 추론할 수 있는 설명으로 옳은 것은? (단, $i, j \geq 0$, $i \neq j$이다) [2022년 국가 7급]

P_i: 평문 블록	$C_i = P_i \oplus O_i$
C_i: 암호문 블록	$P_i = C_i \oplus O_i$
E_k: 암호화 함수(키 k 이용)	$O_i = E_K(I_i)$
IV: 초기벡터(initial vector)	$I_i = O_{i-1}$(단, $I_0 = IV$)

① C_i에 비트 오류가 발생하더라도 복호화된 P_j에 영향을 미치지 않는다.

② P_i와 P_j가 동일할 경우 C_i와 C_j가 같아지는 문제점이 존재한다.

③ 고속의 암복호화를 위해 별도의 전처리 없이 병렬처리가 가능하다.

④ 복호화에 사용되는 IV값은 암호화에 사용된 IV값과 다를 수 있다.

♤ **운영모드**

// 먼저, 암복호화 과정을 분석하면 다음과 같다.

i = 0	• $C_0 = P_0 \oplus O_0 = P_0 \oplus E_K(I_0) = P_0 \oplus E_K(IV)$ • $P_0 = C_0 \oplus O_0 = C_0 \oplus E_K(I_0) = C_0 \oplus E_K(IV)$
i = 1	• $C_1 = P_1 \oplus O_1 = P_1 \oplus E_K(I_1) = P_1 \oplus E_K(O_0) = P_1 \oplus E_K(E_K(I_0)) = P_1 \oplus E_K(E_K(IV))$ • $P_1 = C_1 \oplus O_1 = C_1 \oplus E_K(I_1) = C_1 \oplus E_K(O_0) = C_1 \oplus E_K(E_K(I_0)) = C_1 \oplus E_K(E_K(IV))$

• i=0이면 IV를 1번 암호한 것과 xor 연산한다.
• i=1이면 IV를 2번 암호한 것과 xor 연산한다.
• i=2이면 IV를 3번 암호한 것과 xor 연산한다.
• i=i이면 IV를 i+1번 암호한 것과 xor 연산한다.

① C_i에 비트 오류가 발생하더라도 복호화된 P_j에 영향을 미치지 않는다.(○)
→ C_i와 P_j는 서로 아무런 **연관성 없이 암복호화 처리**되므로($i \neq j$)

② P_i와 P_j가 동일할 경우 C_i와 C_j가 **같아지는 문제점이 존재**한다.(×)
→ **같아지는 문제점이 존재**하지 않는다. $i \neq j$이므로

③ 고속의 암복호화를 위해 별도의 전처리 없이 **병렬처리**가 **가능**하다.(×)
→ **병렬처리**가 불**가능**하다. 이전에 IV를 암호 처리한 것이 필요하므로

④ 복호화에 사용되는 IV값은 암호화에 사용된 IV값과 **다를 수 있다.**(×)
→ IV값과 **같아야 한다.** 다르면 정상적으로 암복호화가 될 수 없다.

정답 : ①

9. 개인정보 보호법령상 민감정보와 고유식별정보를 바르게 연결한 것은? [2022년 국가 7급]

① 유전자검사 등의 결과로 얻어진 유전정보 – 운전면허의 면허번호
② 정당의 가입정보 – 유전자검사 등의 결과로 얻어진 유전정보
③ 여권번호 – 외국인등록번호
④ 범죄경력자료 – 군번

♤ **민감정보와 고유식별정보**

개인정보 보호법 – 제23조(민감정보의 처리 제한)

① 개인정보처리자는 **사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활** 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 **"민감정보"**라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 〈개정 2016. 3. 29.〉

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다. 〈신설 2016. 3. 29.〉

개인정보 보호법 시행령 – 제19조(고유식별정보의 범위)

법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.
〈개정 2016. 9. 29., 2017. 6. 27., 2020. 8. 4.〉

1. 「주민등록법」 제7조의2제1항에 따른 **주민등록번호**
2. 「여권법」 제7조제1항제1호에 따른 **여권번호**
3. 「도로교통법」 제80조에 따른 운전면허의 **면허번호**
4. 「출입국관리법」 제31조제5항에 따른 **외국인등록번호**

정답 : ①

10. 개인정보보호위원회 고시에 따른 개인정보 영향평가 영역과 평가 분야를 짝지은 것으로 옳지 않은 것은? [2022년 국가 7급]

① 대상기관 개인정보보호 관리체계 – 개인정보 침해대응
② 대상시스템의 개인정보보호 관리체계 – 접근권한 관리
③ 개인정보처리 단계별 보호조치 – 이용 및 제공
④ 대상시스템의 기술적 보호조치 – 개인정보의 암호화

♤ **개인정보 영향평가의 평가영역 및 평가분야 (제9조~제11조 관련)**

평가 영역	평가 분야	세부 분야
I. 대상기관 개인정보보호 관리체계	1. 개인정보 보호 조직	개인정보보호책임자의 지정
		개인정보보호책임자 역할수행
	2. 개인정보 보호 계획	내부관리계획 수립
		개인정보보호 연간계획 수립
	3. 개인정보 침해대응	침해사고 신고 방법 안내
		유출사고 대응
	4. 정보주체권리보장	정보주체 권리보장 절차 수립
		정보주체 권리보장 방법 안내
II. 대상시스템의 개인정보보호 관리체계	5. 개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독
	6. 개인정보파일 관리	개인정보파일대장 관리
		개인정보파일 등록
	7. 개인정보처리방침	개인정보처리방침의 공개
		개인정보처리방침의 작성
III. 개인정보 처리단계별 보호조치	8. 수집	개인정보 수집의 적합성
		동의 받는 방법의 적절성
	9. 보유	보유기간 산정
	10.이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공시 안전성 확보
	11. 위탁	위탁사실 공개
		위탁 계약
		수탁사 관리·감독
	12. 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성

평가 영역	평가 분야	세부 분야
IV. 대상시스템의 기술적 보호조치	**13. 접근권한 관리**	계정 관리
		인증 관리
		권한 관리
	14. 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	15. 개인정보의 암호화	저장시 암호화
		전송시 암호화
	16. 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	17. 악성프로그램 등 방지	백신 설치 및 운영
		보안업데이트 적용
	18. 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	19. 개인정보의 파기	안전한 파기
	20. 기타 기술적 보호조치	개발 환경 통제
		개인정보처리화면 보안
		출력시 보호조치
	21.개인정보처리구역보호	보호구역지정
V. 특정 IT기술 활용시 개인정보 보호	22. CCTV	CCTV 설치시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치 및 관리에 대한 위탁
	23. RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	24. 바이오정보	원본정보 보관시 보호조치
	25. 위치정보	개인위치정보 수집 동의
		개인위치정보 제공시 안내사항

정답 : ②