



0. 요약 범위

2025년 2회 예상 실기 이론 문제 범위 요약

출제확률 : 100 : 100% ★ : 80% 🔥 : 50%

과목	예상 문제 수	예상 문제 범위
DB	4문제	100 SQL ★ 정규화 ★ 키 🔥 관계대수 🔥 요개논물
SW 개발	2문제	★ 테스트 커버리지 🔥 블랙박스 테스트 ★ 인터페이스 구현(기술, 표현, 웹, 보안)
SW 설계	2문제	★ 디자인 패턴 ★ 응집도, 결합도 🔥 UML ★ 메모리/프로세스 🔥 라우팅 프로토콜
네트워크/OS	2문제	🔥 네트워크 계층 프로토콜 🔥 데이터 링크 계층 프로토콜
보안/신기술	1문제	🔥 암호 알고리즘, 🔥 보안 기능
총		11문제

1. DB

1) SQL 100

상황	쿼리
데이터 추가	INSERT INTO 테이블(컬럼1, 컬럼2... 생략가능) VALUES (값1, 값2 ...);
데이터 삭제	DELETE FROM 테이블 WHERE 조건;
데이터 수정	UPDATE 테이블 SET 컬럼1 = 값1, 컬럼2 = 값2 WHERE 조건;
테이블 제거	DROP TABLE 테이블 RESTRICT; (다른 테이블이 참조하면 삭제 불가) DROP TABLE 테이블 CASCADE; (참조하는 테이블까지 삭제)
권한 회수	REVOKE 권한 ON 테이블 FROM 사용자;
뷰 생성	CREATE VIEW 뷰이름 AS SELECT 컬럼1, 컬럼2 ... FROM 테이블 WHERE 조건;
두개 컬럼 정렬	SELECT 컬럼1, 컬럼2 FROM 테이블 ORDER BY 컬럼1 DESC, 컬럼2 DESC; (컬럼1 먼저 정렬) SELECT 컬럼1, 컬럼2 FROM 테이블 ORDER BY 컬럼2 DESC, 컬럼1 DESC; (컬럼2 먼저 정렬)
인덱스 생성	CREATE INDEX 인덱스이름 ON 테이블(컬럼1, 컬럼2...);
범위 조회	SELECT 컬럼1, 컬럼2 ... FROM 테이블 WHERE 컬럼1 BETWEEN 1 AND 3; (1~3 사이) SELECT 컬럼1 컬럼2 ... FROM 테이블 WHERE 컬럼1 IN (1,2,3); (1,2,3 중 하나)
특정 문자로 시작하는 데이터 조회	SELECT 컬럼1 컬럼2 ... FROM 테이블 WHERE 컬럼1 LIKE '특정문자*';
특정 문자 앞에 딱 한글자만 있는 데이터 조회	SELECT 컬럼1 컬럼2 ... FROM 테이블 WHERE 컬럼1 LIKE '_특정문자*';
합계에 조건을 걸고 조회할 때	SELECT 컬럼2, SUM(컬럼1) AS 합계 FROM 테이블 WHERE 조건 GROUP BY 컬럼2 HAVING SUM(컬럼1) 조건;
NULL 값 데이터 조회	SELECT 컬럼1 컬럼2 ... FROM 테이블 WHERE 컬럼1 IS NULL;
테이블에 새로운 컬럼 추가	ALTER TABLE 테이블 ADD 컬럼이름 데이터타입;
데이터 개수 세기	SELECT COUNT(컬럼명) FROM 테이블 WHERE 조건; SELECT 컬럼1, 컬럼2 ... FROM 테이블 WHERE 컬럼1 IN (SELECT 컬럼명 FROM 다른테이블 WHERE 조건); (서브쿼리 값 중 컬럼1이 어느 하나라도 일치하면 반환)
서브쿼리 IN ALL ANY=SOME EXISTS	SELECT 컬럼1, 컬럼2 ... FROM 테이블 WHERE 컬럼1 > ALL (SELECT 컬럼명 FROM 다른테이블 WHERE 조건); (모든 서브쿼리 값 보다 컬럼1이 크면 반환) SELECT 컬럼1, 컬럼2 ... FROM 테이블 WHERE 컬럼1 > ANY (SELECT 컬럼명 FROM 다른테이블 WHERE 조건); (서브쿼리 값 중 컬럼1이 어느 하나보다 크면 반환) (ANY = SOME) SELECT 컬럼1, 컬럼2 ... FROM 테이블 WHERE EXISTS (SELECT 컬럼명 FROM 다른테이블 WHERE 조건); (서브쿼리 값 중 어느 하나라도 일치하는 튜플 반환)

쿼리	해석
SELECT COUNT(*) FROM 테이블 WHERE 조건1 AND 조건2 OR 조건3 조건3 인 튜플 갯수	[AND가 우선] (조건1 AND 조건2)이거나 조건3 인 튜플 갯수
SELECT COUNT(DISTINCT 컬럼1) FROM 테이블	컬럼1 값 중 중복 제외한 튜플 갯수

조인(JOIN) 종류 !

조인 종류	키워드
세타 조인 !	(JOIN)조건 만족하는 튜플만 반환
동등 조인 !	(=내부 조인, JOIN)세타조인에서 조건이 등호로 일치하는 튜플만 반환
자연 조인 !	(NATURAL JOIN)동등조인에서 조인에 참여한 중복 속성 제거
외부 조인	(LEFT/RIGHT/FULL OUTER JOIN)조건에 일치하지 않는 튜플도 반환
교차 조인	(CROSS JOIN) 모든 튜플 조합 반환

조인(JOIN) 예시

SELECT 테이블1.컬럼1, 테이블2.컬럼2...
FROM 테이블1 JOIN 테이블2
ON 테이블1.조인컬럼 = 테이블2.조인컬럼;
(단, NATURAL JOIN, CROSS JOIN은 ON을 사용하지 않음)

집합 연산자

연산자	설명
UNION !	중복 행 제거 합집합
UNION ALL	중복행 포함 합집합
INTERSECT	교집합
MINUS	차집합

스키마 종류 !

스키마 종류	키워드
외부스키마	사용자/개발자관점, 사용자뷰, 서브스키마
개념스키마	전체적인 뷰, 개체 간의 관계/제약 조건 등 정의
내부스키마	물리 저장장치 관점, 실제 저장될 레코드 형식 정의

2) 정규화 ★

정규형	조건
제1정규형 !	모든 속성 값 = 원자값(Atomic value)
제2정규형 !	부분 함수 종속 제거(완전 함수 종속 성립)
제3정규형 !	이행함수 종속 제거
BCNF !	모든 결정자가 후보키
제4정규형	다치 종속 제거
제5정규형	조인 종속 제거

함수 종속	설명
완전 함수 종속(Full)	기본키 전체에 대해서만 종속
부분 함수 종속(Partial)	기본키의 일부 속성에 종속
이행 함수 종속(Transitive)	A→B이고 B→C일때 A→C가 성립 ** A→B : 속성 A의 값이 속성 B의 값을 결정

반정규화

- 정규화된 테이블 구조를 의도적 통합, 분리, 중복 허용, 성능 최적화

3) 키(Key) ★

기대(후)슈 : 기본키 + 대체키 = 후보키 ⊂ 슈퍼키



키 종류	키워드
기본키	후보키 중 선택된 키, NOT NULL
대체키	후보키 중 나머지 선택되지 못한 키
후보키	유일성O, 최소성O, 튜플 구별하는데 기준이 되는 키
슈퍼키	유일성O, 최소성 X, 튜플 유일하게 식별
외래키	한 릴레이션의 컬럼이 다른 릴레이션의 기본키

4) 요개논물(데이터 모델) 🔥

데이터 모델 구성요소(3가지) !

구성 요소	핵심 개념	설명
구조	논리 데이터모델에서 표현	타입, 관계 정의
연산	데이터 처리 작업 명세	데이터 조작, 검색 방법(SELECT...)
제약조건	무결성 유지 위한 방법	논리적인 제약사항

요개논물(DB 설계 단계) !

단계	핵심 활동	주요 산출물
요구조건 분석	사용자 요구사항 수집 분석	요구조건 명세서
개념적 설계	현실 세계 개념적/추상적 표현	ER다이아그램
논리적 설계	목표 DBMS에 맞는 설계, 정규화	논리적 스키마
물리적 설계	특정 DBMS 고려	테이블 정의서

+ 구현 → 데이터베이스 구축 프로세스 순서(요개논물 + 구현) !

5) 관계대수/관계해석 🔥

관계대수		관계해석
절차적 언어		비절차적 언어(Codd 박사)
어떻게(HOW) 데이터 가져올것인지 명시		무엇을(WHAT) 원하는지 명시

관계대수 연산자

(1)일반 집합 연산자

연산자	기호	설명
합집합	U	중복 제외, 두 릴레이션 튜플 모두 반환
교집합	∩	두 릴레이션 공통 튜플 반환
차집합	-	왼쪽 릴레이션에 속하지만 오른쪽 릴레이션에 속하지 않는 튜플 반환
카티션 프로덕트	x	두 릴레이션의 튜플들을 순서쌍으로 조합하여 만들 수 있는 모든 튜플을 반환

(2)순수 관계 연산자 !

연산자	기호	설명
셀렉트 (Select)	σ(Sigma)	주어진 조건 만족하는 튜플 반환(수평)
프로젝트 (Project)	π(Pi)	주어진 조건 만족하는 열 반환(수직)
조인 (Join)	⋈	공통 속성 기준 결합
디비전 (Division)	÷	A÷B : B의 모든 튜플에 대해 관계를 맺고 있는 A의 튜플 반환

2. SW 개발

1) 테스트 커버리지(화이트박스 테스트) ★

커버리지 강도 - 구문 < 결정 < 조건 < 조건/결정 < MC/DC

커버리지 종류	영어	핵심 키워드
구문(문장)	Statement !	모든 명령문, 모든 문장 수행
결정(분기)	Decision/Branch !	모든 조건, 결정문
조건	Condition !	결정문 내 각 개별 조건식
조건/결정	Condition/Decision	조건 + 결정 모두 만족
MC/DC !	Modified Conditon/Decision !	개별 조건식의 독립적 영향

2) 블랙박스 테스트 🔥

블박 테스트 유형	영어	핵심 키워드
동등 분할 !	Equivalence Partitioning !	입력 데이터를 유효값/무효값 그룹핑
경계값 분석 !	Boundary Value Analysis	등가 분할 후 경계값 포함 테스트 설계
결정 테이블	Decision Table	논리적 조건과 그에 따른 행동 표로 정리
원인-결과그래프 !	Cause-Effect Graph	입력(원인)이 출력(결과)에 미치는 영향 그래프 표현, 테스트 선정
상태 전이	State Transition	상태 변화 기반 테스트 설계
오류 예측	Error Guessing	테스터의 경험과 직관, 오류가 발생 부분 예측
비교 테스트	Comparison Testing	여러 버전 또는 제품을 비교 테스트
페어와이즈 테스트	Pairwise Testing	모든 가능한 입력 값 조합 대신, 최소 테스트 케이스, 입력 값들의 모든 쌍(pair)을 테스트
분류 트리 테스트	Classification Tree	테스트 관련 요소를 트리 구조로 분석하고 테스트 케이스 도출
유스케이스 테스트	Use Case Testing	사용자의 시나리오(유스케이스)를 기반으로 테스트

3) 인터페이스 구현 ★

인터페이스 보안 프로토콜 !

(1)터널링(VPN)

프로토콜	동작 계층	키워드
PPTP	데이터 링크 계층	PPP 기초
L2F	데이터 링크 계층	시스코 개발, UDP 사용
L2TP !	데이터 링크 계층	L2F + PPTP, VPN에서 사용, 터널링
IPSec !	네트워크 계층	IP 패킷 단위 암호화, 강력한 보안 제공

(2)웹 트래픽 암호화

프로토콜	동작 계층	키워드
SSL/TLS	전송 계층	웹 통신 암호화 표준, HTTPS의 기반
S-HTTP	응용 계층	클라이언트 서버 간 메시지 단위 암호화
HTTPS	응용 계층	통신 채널 전체 암호화

인터페이스 통신 기술 !

통신 기술	키워드
AJAX !	일부 콘텐츠만 리로드, HTML만으로 어려운 작업 구현
Fetch API	Promise 기반, 비동기 코드 쉽게 관리, 브라우저 내장 API
웹소켓	양방향 실시간 통신, 서버 푸시 가능, 연결 계속 유지
GraphQL	API를 위한 쿼리 언어, 불필요한 데이터 전송 없음

인터페이스 데이터 표현 형식

데이터 표현 형식	키워드
JSON	사람이 읽기 쉬운, key-value 쌍, 주석 불가능
XML	태그(<>) 사용, 마크업 언어, 뛰어난 확장성
YAML	사람이 읽고 쓰기 편한, 들여쓰기, 주석 가능

웹 서비스 인터페이스

(1)클래식 웹 서비스 프로토콜


프로토콜	키워드
UDDI	검색 엔진
WSDL	XML 형식
SOAP	XML 메시지

(2)현대 웹 서비스 아키텍처 스타일

REST - 키워드 : HTTP 활용, 주로 JSON 사용

3. SW 설계

1) 디자인 패턴 ★

생성패턴-싱글빌드프업	패턴	핵심 키워드
	싱글톤(Singleton) !	객체 하나만 생성, 어디서든 참조
	팩토리 메서드 !	상위 클래스 - 인터페이스만 정의 (Factory Method)
	빌더(Builder)	조립 + 분리
	프로토타입(Prototype)	복제
	앱스트랙트 팩토리 !	조합을 만드는 인터페이스(API) 제공, Kit이라고 불림.

구조패턴 -어댑터프 브플킴

패턴	핵심 키워드
어댑터(Adapter) !	서로 다른 인터페이스 연결
데코레이터(Decorator)	기능 추가 + 확장
퍼사드(Facade)	단순 인터페이스, 오류 단위 확인
프록시(Proxy) !	객체의 대리자가 대신 처리
브리지(Bridge) !	기능 클래스-구현 클래스 연결, 추상 계층 분리
플라이웨이트(Flyweight)	가상 인스턴스/ 가상화
컴포지트(Composite)	트리구조, 복합 객체 = 단일 객체

행위패턴 ! - 전용 중방이상 매커택템

패턴	핵심 키워드
전략(Stratgy)	알고리즘군
옵저버(Observer) !	한 객체 바뀌면 의존하는 다른 객체에 연락 가고 자동 갱신
중재자(Mediator)	통신 빈도수 낮음
방문자(Visitor) !	메서드가 각 클래스 돌아다님, 새로운 기능(연산)만 따로 추가할때 사용
이터레이터(Iterator) !	컬렉션 내 모든 요소 순차 탐색, Cursor
상태(State)	원시코드 수정 취소, 상태 캡슐화
메멘토(Memento)	복구, Undo 기능, 객체 정보 저장
커맨드(Command)	재사용성, 기능 캡슐화
책임 연쇄 (Chain of responsibility)	하드코딩(기능 처리 연결 변경 불가) → 연결 변경 가능하게 디자인, 2개 이상 객체
템플릿 메서드 (Template Method)	상위 클래스 - 추상 메서드(기능의 골격) 하위 클래스 - 세부처리 구체화

2) 응집도, 결합도 ★

응집도 - 모듈 내부의 요소들이 얼마나 밀접하게 관련되어 있는지

결합도 - 모듈과 모듈 간의 상호 의존 정도

응집도(cohesion)	키워드
기능적 (Functional cohesion) !	모든 기능 단일 목적 위해 수행
순차적 (Sequential cohesion) !	이전 출력을 다음 입력으로 사용
통신적(교환적)(Communicational cohesion) !	동일한 입력 출력 사용
절차적 (Procedural cohesion) !	입출력간 연관성X, but 순서에 따라 수행
시간적 (Temporal cohesion)	특정 시간에 처리
논리적 (Logical cohesion)	논리적 유사하지만 실제로는 다른 기능
우연적 (Accidental cohesion)	모듈 내부 요소 연관 없음

결합도(coupling)	키워드
내용 (Content coupling) !	모듈 내부 변수
공통 (Common coupling) !	전역 변수 참조 갱신
외부 (External coupling)	외부 데이터 사용
제어 (Control coupling) !	제어 신호(요소)를 이용하여 통신
스탬프 (Stamp coupling) !	자료구조(배열, 객체, 구조 등) 전달
자료 (Data coupling)	파라미터 통해서 전달

3) UML 다이어그램



베네딕트 컴배비치 + 시커스톤

정적 다이어그램	핵심 키워드
클래스 다이어그램	속성, 메서드 포함, 클래스간 관계 표현
객체 다이어그램	객체 모델링, 인스턴스
컴포넌트 다이어그램	구현단계 인터페이스/의존관계
배치 다이어그램	물리적 위치
복합체 다이어그램	내부 구조
패키지 다이어그램	폴더 모양, 유스케이스 요소 그룹화
동적 다이어그램	핵심 키워드
유스케이스 다이어그램	사용자 관점 표현
시퀀스 다이어그램	객체 메시지 + 흐름
커뮤니케이션 다이어그램	객체 메시지 연관관계
상태 다이어그램	럼바우 동적 모델링 + 상태변화
활동 다이어그램	어떤 기능 수행
타이밍 다이어그램	시간제약 명시적

클래스 다이어그램 관계

(1) 강약 마름모 (2) 강약 화살표 (3) 강약 속 빈 화살표

관계	모양	키워드
포함(복합)(Composition)	강한 마름모 ◆ (속 찬)	영구적
집합(Aggregation)	약한 마름모 ◇ (속 빈)	포함되어 있는 관계
연관(Association)	강한 화살표 → (실선)	서로 관련(연결)
의존(Dependency)	약한 화살표 → (점선)	짧은 시간 동안 연관 유지
일반화(Generalization)	강한 속 빈 화살표 -> (실선)	일반적인지 구체적인지
실체화(Realization)	약한 속 빈 화살표 -> (점선)	기능으로 그룹화, 자식 클래스 추상메서드

4. 네트워크/OS

1) 메모리 교체/프로세스 스케줄

메모리 페이지 교체 알고리즘

(1) FIFO - 가장 먼저 들어온 페이지를 가장 먼저 내보냄

3개 프레임, 페이지 참조 순서: 2, 3, 2, 1, 5, 2, 4 일때, Page Fault 몇번?

참조	2	3	2	1	5	2	4
1 프레임	2	3	3	1	5	2	4
2 프레임		2	2	3	1	5	2
3 프레임				2	3	1	5
Page Fault	V	V		V	V	V	V

답 : 6

(2) LRU - 가장 오랫동안 참조되지 않은 페이지를 내보냄

3개 프레임, 페이지 참조 순서: 2, 3, 2, 1, 5, 2, 4 일때, Page Fault 몇번?

참조	2	3	2	1	5	2	4
1 프레임	2	3	2	1	5	2	4
2 프레임		2	3	2	1	5	2
3 프레임			3	2	1	5	
Page Fault	V	V		V	V	V	V

답 : 5

(3) LFU - 참조 횟수가 가장 적은 페이지를 내보냄

3개 프레임, 페이지 참조 순서: 2, 3, 2, 1, 5, 2, 4 일때, Page Fault 몇번?

참조	2	3	2	1	5	2	4
1 프레임	2	3	3	1	5	2	4
2 프레임		2	2	3	1	5	2
3 프레임			3	2	1	5	
Page Fault	V	V		V	V	V	V

답 : 5

프로세스 스케줄링 알고리즘

비선점형 - 한 프로세스가 CPU를 할당받으면 해당 프로세스 종료까지 CPU 할당 유지
선점형 - 현재 실행 중인 프로세스를 중단시키고 다른 프로세스에 CPU를 강제 할당 가능

비선점형 스케줄링		선점형 스케줄링	
종류	설명	종류	설명
FIFO	도착 순서대로 할당	Round Robin(RR)	FIFO + 시간 지정 (같은 시간 할당)
SJF	실행 시간 짧은 프로세스에 할당	SRT	선점형 SJF
HRN	SJF + 대기 시간 고려		
기한부	마감시간 임박한 프로세스 먼저		
우선순위	우선순위에 따라 할당		

[공통 문제] 다음과 같이 프로세스들이 준비 큐에 도착했을 때

프로세스	도착 시간	실행 시간
P1	0	3
P2	1	1
P3	2	4
P4	3	2

[문제 1] SJF 스케줄링을 사용할 경우 평균 대기 시간과 평균 반환 시간

프로세스	0	1	2	3	4	5	6	7	8	9	10
P1	O	V	V	V							
P2		O	X	X	V						
P3			O	X	X	X	X	V	V	V	V
P4				O	X	V	V				

평균 대기 시간 : (0 + 2 + 4 + 1)/4 = 1.75

평균 반환 시간 : (3 + 3 + 8 + 3)/4 = 4.25 (반환시간 = 대기시간 + 실행시간)

[문제 2] SRT 스케줄링을 사용할 경우 평균 대기 시간과 평균 반환 시간

프로세스	0	1	2	3	4	5	6	7	8	9	10
P1	O	V	X	V	V						
P2		O	V								
P3			O	X	X	X	X	V	V	V	V
P4				O	X	V	V				

평균 대기 시간 : (1 + 0 + 4 + 1)/4 = 1.5

평균 반환 시간 : (4 + 1 + 8 + 3)/4 = 4 (반환시간 = 대기시간 + 실행시간)

[문제 3] RR 스케줄링(시간 할당량 = 2)을 사용할 경우 평균 대기 시간과 평균 반환 시간

프로세스	0	1	2	3	4	5	6	7	8	9	10
P1	O	V	V	X	X	X	X	X	V		
P2		O	X	V							
P3			O	X	V	V	X	X	X	V	V
P4				O	X	X	V	V			

평균 대기 시간 : (5 + 1 + 4 + 2)/4 = 3

평균 반환 시간 : (8 + 2 + 8 + 4)/4 = 5.5 (반환시간 = 대기시간 + 실행시간)

2) 네트워크 계층 프로토콜

! 역할 : 데이터 전송 최적 경로 제공

프로토콜	핵심 키워드
IP	데이터그램의 주소 지정 및 경로 설정
ARP	논리 주소(IP) → 물리 주소(MAC)로 변환
RARP	물리 주소(MAC) → 논리 주소(IP)로 변환
ICMP	오류 정보 전송, Ping-of-Death에서 사용
IGMP	멀티캐스트 그룹 관리
라우팅 프로토콜	아래 참고 RIP, OSPF, BGP
NAT	사실 IP 주소 → 공인 IP 주소 변환, IPv4주소 부족 해결

3) 라우팅 프로토콜

정적 라우팅	동적 라우팅	경로 계산, 동적 경로 변경
고정된 경로 사용		
내부 라우팅 프로토콜(IGP)	외부 라우팅 프로토콜(EGP)	
동일한 AS 내	서로 다른 AS간	
프로토콜 알고리즘	키워드	프로토콜 알고리즘
RIP	거리 벡터(벨만-포드)	홉 수 제한
OSPF	링크 상태(다익스트라)	큰 네트워크, AS를 지역으로 나눔
BGP	경로 벡터	초기 전체 라우팅 테이블 교환, 이후 변경사항만 교환
		** AS : 자율시스템(네트워크 영역)

4) 데이터 링크 계층 프로토콜

! 역할 : 노드 사이 데이터 전송 및 오류 수정

프로토콜	핵심 키워드
HDLC	비트(Bit) 지향 프로토콜, 데이터 흐름 제어/오류 보정 가능한 비트 열 삽입 다음 장 참고
ATM	비동기식 시분할 다중화 방식 패킷형 전송 기술 (필요할때, 시간을 나눠서, 여러 사용자가, 전송)
PPP(Point to Point)	두 노드 직접 연결시 사용
프레임 릴레이(Frame Relay)	중계(Relay)/다중화 기능만 수행, 고속 데이터 전송

HDLC 프레임 !

프레임	제어부 시작	키워드
I(정보) 프레임	0	데이터 전달 역할
S(감시/감독) 프레임	10	오류/흐름 제어 역할
U(비번호) 프레임	11	링크 동작모드 설정 역할

HDLC 동작모드 !

동작 모드	키워드
정규 응답 모드(NRM)	보조국(종국)은 폴 메시지 수신한 경우에만 송신
비동기 응답 모드(ARM)	포인트 투 포인트 불균형 링크에서 사용, 호환국(주국 + 보조국)끼리 허가 없이 전송 가능
비동기 균형 모드(ABM)	포인트 투 포인트 균형 링크에서 사용, 종국은 주국의 허가없이 송신 가능,

데이터링크 오류제어

FEC !		BEC !	
오류를 스스로 수정		오류 발생 시 송신 측에 재전송 요구	
종류	키워드	종류	키워드
해밍 코드(Hamming)	1비트 수정 가능	패리티검사(Parity)	패리티 비트
상승 코드	여러 비트 수정 가능	CRC(순환 잉여 검사)	다항식 토대 오류검사
! 해밍코드, 패리티검사, CRC		ARQ(자동반복 요청)	재전송 기반 오류제어
		블록합 검사	2차원 패리티 검사

5. 보안/신기술

1) 암호 알고리즘 🔥

대칭키 암호 알고리즘

대칭키 ! - 암호화키=복호화키, 비밀키 전달 필요, 암호화/복호화 빠름

알고리즘	키워드
DES !	IBM 개발, 블록 64비트
AES !	DES 성능문제 극복, 블록 128비트
SEED	KISA 개발, 한국 최초 표준
IDEA !	초기 블록 암호화 알고리즘
Skipjack !	전화기와 같이 음성 암호화에 주로 사용

비대칭키 암호 알고리즘

비대칭키 ! - 공개키/개인키 존재

알고리즘	키워드
디피-헬만	최초의 공개키 알고리즘
RSA	소인수분해 기반
ECC	RSA 대안, 타원곡선 이산 로그 기반, 짧은 키

해시 암호 알고리즘

해시 함수 ! - 임의의 길이를 갖는 데이터를 고정된 길이로 바꾸는 단방향 함수

알고리즘	키워드
MD5	무결성 검사에 사용, R.Rivest 개발
SHA-1	160비트, NSA(1995)
SHA-2(256/384/512)	256/384/512비트, AES 대응, NSA(2001)

2) 보안 기능 🔥

서버 접근 통제 !

접근 통제 방식	키워드
DAC(임의적)	신분/식별자 기반, 사용자가 다른 사용자 자신의 판단따라 권한 허용
MAC(강제적)	규칙 기반, 객체 포함 허용 등급, 주체 접근 권한 근거
RBAC(역할기반)	중앙 관리자, 역할에 기초

3A !

어쨌든 인증! 어떠한 권한 부여? Authen(tication) 어떤 인증 Author(ization) 권한 부여

AAA	키워드
Authentication(인증)	접근시도 가입자 식별 및 인증
Authorization(권한 부여)	어떤 수준의 권한 허용
Accounting(계정 관리)	리소스 사용 정보 수집 관리

인증기술

기술	키워드
SSO !	커버로스 사용, 한번 인증 → 여러 컴퓨터 자원 이용 가능
커버로스(Kerberos)	티켓 기반, 대칭키 암호화 기반
OAuth !	비밀번호 제공하지 않고 웹사이트 접근 권한 부여 가능

🔥보안/신기술 과목은 초압축 이론 요약 PDF에서는 매우 일부만 다루고 있습니다. 중요도가 낮지만 출제범위가 넓은 보안/신기술 과목은 kimjaahyun.com에서 확인하세요.

🔥목차를 보며 복습해봅시다([3]= 3가지)

1. DB	- 생성패턴 - 싹팩빌프업 - 구조패턴 - 어데퍼프 브플컴 - 행위패턴 - 전용 중방이상 매커택템
1) SQL	2) 응집도, 결함도 - 웨리 - 조인 종류[5] - 집합 연산자[4] - 스키마 종류[3]
2) 정규화	3) UML 다이어그램 - 정규형(1,2,3,BCNF,4,5) - 함수종속[3] - 반정규화
3) 키	- 베네틱트 컴배비치 + 시커스톤 - 클객컴배복패, 유시커상탈타 - 클래스 다이어그램 관계 (1)강약 마름모[2] (2)강약 화살표[2] (3)강약 속 빈 화살표[2]
4) 요개논물 (데이터모델)	4. 네트워크/OS 1) 메모리 교체/프로세스 스케줄 - 메모리 페이지 교체 알고리즘 (1)FIFO (2)LRU (3)LFU - 프로세스 스케줄링 알고리즘 (1)비선점형[5] (2)선점형[2]
5) 관계대수/관계해석	2) 네트워크 계층 프로토콜[7] 3) 라우팅 프로토콜 4) 데이터 링크 계층 프로토콜[4] - HDLC 프레임[4] - HDLC 동작모드[3] - 데이터링크 오류제어(FEC[2],BEC[4])
1)일반 집합 연산자[4] (2)순수 관계 연산자[4]	5. 보안/신기술 1) 암호 알고리즘 - 대칭키 암호 알고리즘[5] - 비대칭키 암호 알고리즘[3] - 해시 암호 알고리즘[3]
2. SW개발	2) 보안 기능 - 서버 접근 통제[3] - 3A - 인증기술[3]
1) 테스트커버리지(화이트박스 테스트)[5]	
2) 블랙박스 테스트[10]	
3) 인터페이스 구현	
- 인터페이스 보안 프로토콜	
(1) 터널링 VPN[4] (2) 웹트래픽 암호화[3] - 인터페이스 통신 기술[4] - 인터페이스 데이터 표현 형식[3] - 웹 서비스 인터페이스	
(1)클래식 웹 서비스 프로토콜[4] (2)현대 웹 서비스 아키텍처 스타일[1]	
3. SW 설계	
1) 디자인 패턴	

🔥초압축 이론 요약 PDF는

아래와 같이 과목별로 맞춰야할 문제수를 맞추기 위한 범위를 커버하고 있습니다.

과목	예상 문제 수	맞춰야할 문제 수
DB	4문제	3문제
SW 개발	2문제	1문제
SW 설계	2문제	2문제
네트워크/OS	2문제	1문제
보안/신기술	1문제	0문제
총	11문제	7문제

🔥중, 하 난이도의 코딩 문제를 풀 수 있다면 현재 범위를 공부했을 때 합격할 수 있습니다. (2025년 1회 기준 중,하 난이도의 코딩문제는 9문제 중 5문제)

? 초압축 이론 요약 PDF 내용을 숙지했습니다! 다음엔 무엇을 할까요?

🔥중, 하 난이도의 코딩 문제를 확실하게 풀 수 있도록 C언어, 자바, 파이썬 핵심 기초 문제를 다시 한번 푸는 것을 권장합니다.

? 이론을 조금 더 확실하게 준비하고 싶습니다. 무엇을 공부할까요?

🔥kimjaahyun.com → 정처기 실기 공부법 [이론편]을 확인하면 각 과목별로 출제확률 20%(🔥)에 해당하는 범위가 있습니다. 해당 범위를 추가로 공부하세요.

🔥합격을 응원합니다!