ICT의 가치를 이끄는 사람들!!!

127회

정보관리기술사 기출풀이 4교시

T 02.724.1831 E kpcitpe@kpc.or.kr H www.kpc.or.kr C cafe.naver.com/kpcitpe

국가기술자격 기술사 시험문제

정보처리기술사 제 127 회 제 4 교시

분야	정보처리	종목	정보관리기술사	수험번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. 최근 여러 기업에서 MSA(Micro Service Architecture) 도입이 활발하게 이루어지고 있다. MSA 에 대한 아래의 사항을 설명하시오.
   가. MSA 개념 및 특징과 구현시 지켜야 할 원칙
   나. 모놀리스 아키텍처(Monolith Architecture)와 MSA 비교
   다. MSA 구현을 위한 서비스 메쉬(Service Mesh)

2. 데이터 커머스(Data Commerce)의 중요성이 점차 증대되고 있다. 데이터 커머스에 대한 아래의 사항을 설명하시오.
   가. 개념과 주요 기술
   나. 특징
   다. 활용 분야

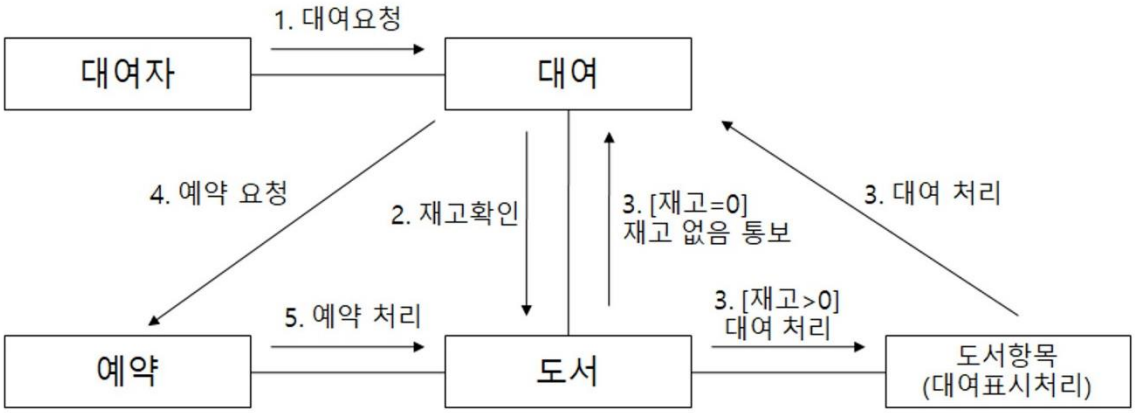
3. 데이터베이스 샤딩(Sharding)에 대한 아래의 사항을 설명하시오.
   가. 샤딩의 개념 및 분할방법
   나. 샤딩과 파티셔닝(Partitioning)의 차이점
   다. 샤딩 적용 시 고려사항

4. 최근 데이터 산업 발전을 위하여 "데이터 산업진흥 및 이용촉진에 관한 기본법"(약칭: 데이터산업법)을 제정하였다. 이 법의 목적 및 주요 내용과 기대 효과에 대하여 설명하시오.

5. UML 2.0 의 순차 다이어그램(Sequence Diagram)에 대한 아래의 사항을 작성하시오.
   가. 순차 다이어그램의 목적과 작성순서, 구성요소별 표기법

구성요소	Frame, Object, Lifelines, Activation Box, Messages, Guard

나. 아래의 도서예약시스템의 협력 다이어그램(Collaboration Diagram)을 순차 다이어그램으로 변환

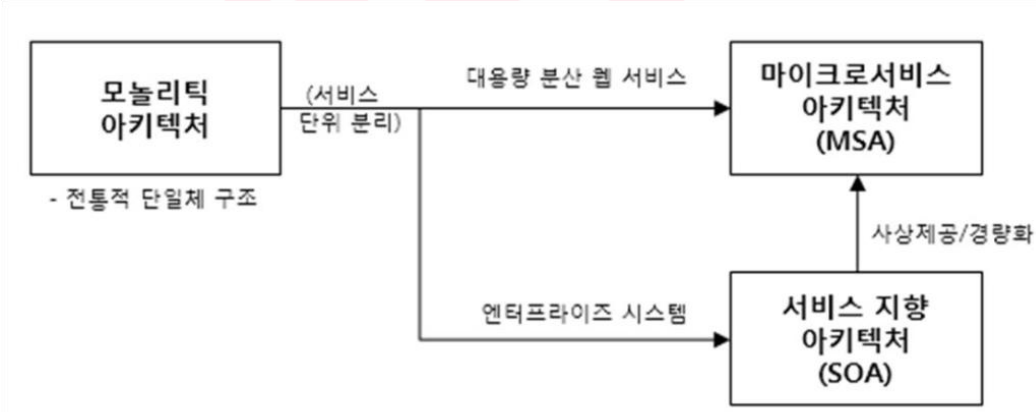


6. 블록(Block) 암호 모드에 대한 아래의 사항을 설명하시오.
   가. ECB(Elctronic CodeBook) 모드
   나. CBC(Cipher Block Chaining) 모드
   다. CFB(Cipher FeedBack) 모드
   라. OFB(Output FeedBack) 모드

문 제	1. 최근여러 기업에서 MSA(Micro Service Architecture) 도입이 활발하게 이루어지고 있다. MSA 에 대한 아래의 사항을 설명하시오 가. MSA 개념 및 특징과 구현시 지켜야 할 원칙 나. 모놀리스 아키텍처 (Monolith Architecture)와 MSA 비교 다. MSA 구현을 위한 서비스 매쉬 (Service Mesh)
출 제 영 역	소프트웨어공학 / 난 이 도 ★★★☆☆
출 제 배 경	- MSA 도입 확산에 따른 개념과 구현 위한 지식 확인
출 제 빈 도	117 회 정보관리 1 교시, 120 회 정보관리 2 교시, 120 회 컴시응 1 교시
참 고 자 료	- 스프링으로 하는 마이크로서비스 구축(소프트웨어 아키텍처) (매그너스 라슨 저, 박규태 역)
Keyword	- SOA 사상, 기능단위 분리, 분산 거버넌스, 분산 DB, DB 오너십, 변화대응, Loosely Coupled, 자율성의 원칙, 회복성의 원칙, 투명성의 원칙, 자동화의 원칙
풀 이	서현석(123 회 정보관리기술사)

1. MSA 개념 및 특징과 구현시 지켜야 할 원칙

1) SOA 사상에 근거를 두는 MSA 개념 및 특징

구분	설 명	
개념도		
개념	- 서비스/애플리케이션을 기능단위로 분할하고 이들의 조립으로 애플리케이션을 제공하는 아키텍처	
특징	● SOA 사상	- SOA 사상에 근간을 두고 대용량 분산 웹 서비스에 맞는 구조로 경량화
	● 기능단위 분리	- Loosely Coupled, 영향 최소화, 독립적 배포 가능한 기능단위 분리
	● 분산 거버넌스	- 기능/서비스에 따라 최적의 환경, 자원 할당, 개발언어 선택 및 적용 가능
	● 분산 DB	- 각 기능 서버마다 각기 다른 종류의 DB 와 데이터 소유 가능
	● DB 오너십	- 자신이 소유하지 않은 데이터에 접근할 때 데이터를 소유한 서비스가 제공한 인터페이스를 통해서만 접근
	● 변화대응	- 각 기능 / 서비스 별 작은 규모의 조직 구성 변화에 빠르게 대응 가능

- 독립적 배포 가능한 기능들의 조합으로 어플리케이션 설계로 변경과 확장에 유연함

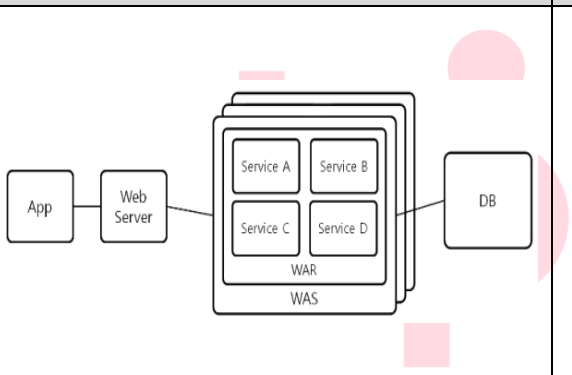
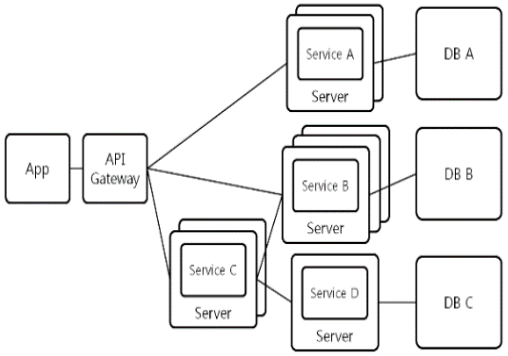
2) MSA 구현시 지켜야 할 원칙

원칙	내용
자율성의 원칙	- 낮은 결합력으로 여러팀에 의해 동시/**독립적으로 배포 가능**, 신속 변화대응과 독립적 배포로 애플리케이션 또는 인프라의 장애는 시스템의 일부에만 영향으로 빅뱅 출시가 아닌 점진적으로 변화 가능해야 함
회복성의 원칙	- 가능한 비동기 처리를 하고 적절한 회로 차단기와 타임아웃을 사용한 설계로 장애 발생 때 확산이나 전파를 차단하고 **빠르게 회복** 가능해야 함
투명성의 원칙	- 여러 팀이 개발한 여러 서비스에 의존하고 상호작용하기 때문에 **서비스의 위치, 장애, 병행처리** 시 시스템이 어느 지점에서나 **투명하고 관찰 가능**해야 함
자동화의 원칙	- 프로비저닝을 통한 **인프라 구성의 자동화**를 도입하고 서비스간 일관된 인프라를 구성해, 복잡한 아키텍처 관리 비용을 감소해야 함

- MSA 는 SOA 사상을 근간으로 모놀리식 애플리케이션보다 개별적으로 쉽게 개발하고 추론 **가능**

2. 모놀리스 아키텍처 (Monolith Architecture)와 MSA 비교

1) 모놀리스 아키텍처와 MSA 구성도 비교

비교 항목	모놀리스 아키텍처	MSA
구성도		
특징	- 하나의 서버에 모든 비즈니스 로직이 포함되어 있는 아키텍처	- 여러개의 독립된 기능들을 조합하여 서비스를 제공하는 아키텍처

- 단일 아키텍처 모놀리스에서 대용량 분산 서비스하는 MSA 로 발전

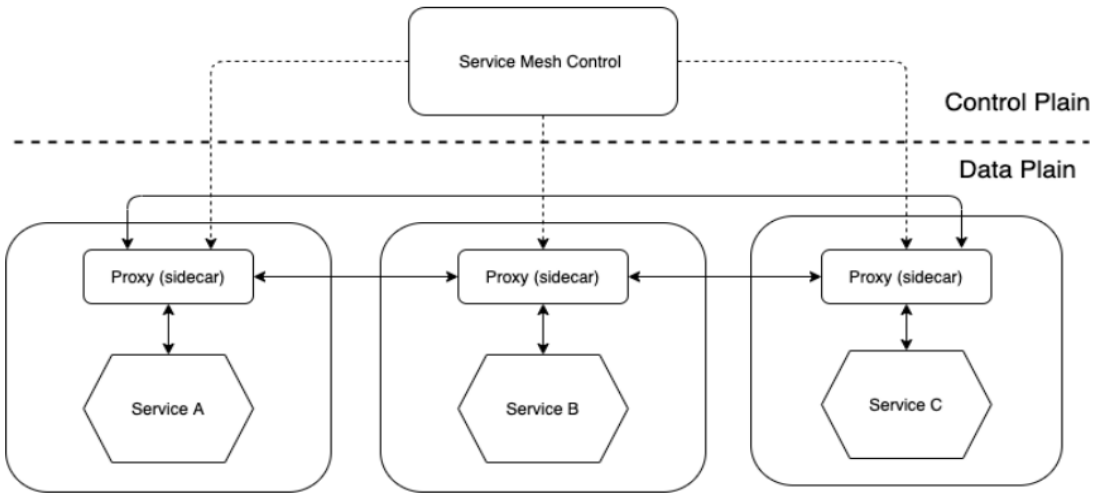
2) 모놀리스 아키텍처와 MSA 상세 비교

비교 항목	모놀리스 아키텍처	MSA
배포	- 전체 배포, 단 하나의 변경에 전체 시스템 다시 빌드 및 배포	- 기능 단위 독립적 빌드 및 배포
DB	- 하나의 데이터베이스 사용	- 서비스/서버 별 각각 다른 종류의 DB 사용
결합력	- 서비스별 모듈별 높은 결합력	- 서비스별 낮은 결합력
변경	- 작은 변경에 전체 모듈 영향	- 변경 영향도 낮음, 유지보수 용이
확장	- 부분 확장 어려움	- 부분 확장 용이
개발 독립	- 선택된 하나의 개발 언어에 의존적	- 서비스별 특성 따라 다양한 개발 언어 사용

- 모놀리스 아키텍처는 하나의 애플리케이션으로 구현, MSA 는 여러 개의 작은 애플리케이션으로 구현하여 조합
- 시스템이 커질 수록 서비스가 많아지고, 서비스간의 연결이 복잡해져 장애 추적이 어렵고 장애 전파로 이어지는 문제를 인프라 측면에서 해결하기 위해 서비스 매쉬를 구성

3. MSA 구현을 위한 서비스 매쉬

1) 서비스 매쉬 개념 및 개념도

구분	내용
개념	- 서비스 간의 통신을 제어하고 표시하고 관리할 수 있도록 하는데 특화된 마이크로 서비스를 위한 인프라 계층
개념도	

- 서비스를 직접 호출하는 것이 아닌 Proxy 간 호출하는 구조

2) 서비스 매쉬 구성요소

구분	상세 구분	설 명
Control Plane	● Configuration Store	- Data Plane 의 Proxy 설정 값들을 저장하고, Proxy 들에 설정 값을 전달하는 역할
Data Plane	● Circuit Breaker	- 호출되는 서비스가 응답이 없을때 Proxy 에서 이 연결을 끊어 장애 전파 차단
	● Networking	- L4/L7 레벨 접근 제어 정책, Routing 및 Load Balancing 설정
	● Dynamic App Configuration	- 서비스 별 필요한 환경 설정 값 과 데이터를 저장 공유
	● Dynamic Service Discovery	- 서비스를 호출할 때 서비스의 위치 (IP 주소와 포트)를 제공하는 기능

- Data Plane 에서 프록시를 통해 모든 네트워크 통신을 조정하고 제어 "끝"

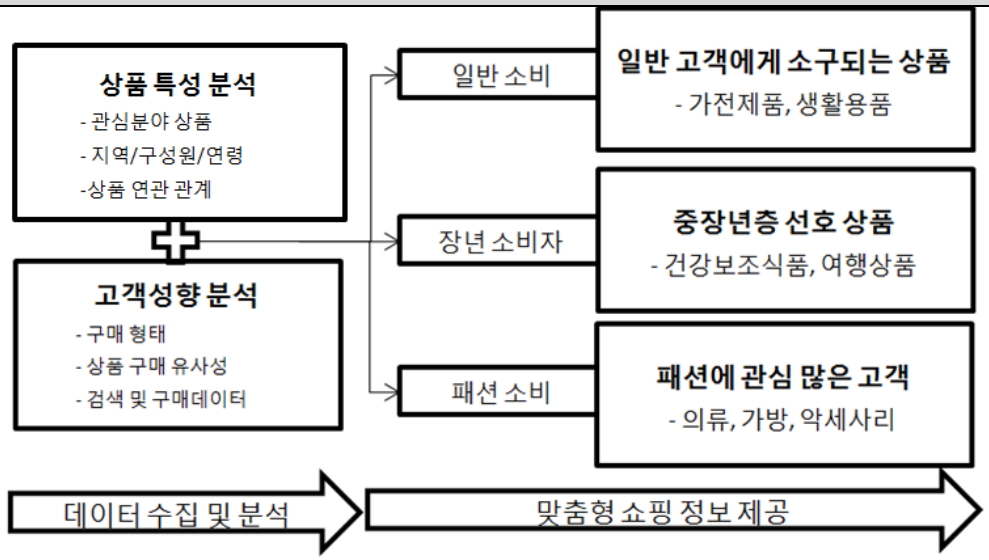
기출풀이 의견

1. 문제의 물어본 것에 집중해서 풍부하게 작성하고, 3단락에 서비스 메쉬는 MSA와 어떤 관계가 있는지 짚어주고 작성하시면 다른 분들과 차별화될 것입니다. 마지막 4 단락은 MSA와 SOA와 비교, 서비스 매쉬와 API Gateway와 관계 또는 Saga패턴 등 추가로 제시하시면 고득점 기대됩니다

문 제	2. 데이터 커머스(Data Commerce)의 중요성이 점차 증대되고 있다. 데이터 커머스 대한 아래의 사항을 설명하시오 가. 개념과 주요 기술 나. 특징 다. 활용 분야
출 제 영 역	디지털 서비스 / 난 이 도 ★★★☆☆
출 제 배 경	- 빅데이터를 활용 고객 타게팅 및 맞춤형 커머서스 시장 확대에 따른 현황 및 지식 확인
출 제 빈 도	미출제
참 고 자 료	- 주간기술동향 1995 호 - T 커머스 방송 서비스 기술동향 - 161206-KISA-2017 년 인터넷 10 대 이슈전망 - 데이터 커머스(D-Commerce)
K e y w o r d	- 빅데이터 수집/처리/저장, 연관분석, 상관 분석, 통계 분석, 오피니언 마이닝, 텍스트 마이닝
풀 이	서현석(123 회 정보관리기술사)

1. 데이터 커머스의 개념과 주요 기술

1) 빅데이터 기반 맞춤형 커머스, 데이터 커머스의 개념

구분	설 명
개념도	
정의	- 빅데이터 분석 기술을 기반으로 소비자와 상품 데이터를 분석해 소비자와 상품을 연결, 맞춤형 쇼핑 정보를 제공하는 커머스 서비스

- 소비자 맞춤형 서비스 제공 위해 빅데이터 기술과 분석기술이 필요

2) 데이터 커머스의 주요기술

기술 구분	주요 기술	설 명
빅데이터 기술	● 수집 기술	- 다양한 형태로 발생되는 소비자, 구매 , 판매 데이터를 수집 - ETL, Sqoop, Flume
	● 처리 기술	- 다양한 형태의 소비자 소비 데이터, 판매 데이터 분산 처리 기술 - Hadoop, YARN, MapReduce, Spark, Storm

	● 저장 기술	- 수집된 데이터를 정형, 비정형 데이터로 저장 및 공유 - RDB, HDFS, NoSQL
탐색적 데이터 분석 기술	● 연관분석	- 소비자 구매 데이터 발생 빈도에 따라 상품간 연관 관계를 찾아 추천 - Apriori, 지지도, 신뢰도, 향상도
	● 상관 분석	- 소비자/판매자, 소비자/제품 등 두 변수간 어떤 상관 관계를 찾아 추천 - 분산, 공분산, 산관계수
	● 통계 분석	- 소비 패턴, 소비자 제품 옵션 선택 등 관측한 현상의 특징 또는 경험을 분석 - R
마이닝 기술	● 오피니언 마이닝	- 텍스트로 표현되는 소비자의 행동과 감성을 분석해 쇼핑에 대한 인사이트를 제공 - crawling, word2vec, 텍스트 마이닝, 긍정/부정평가
	● 텍스트 마이닝	- 텍스트 데이터로부터 패턴이나 관계를 찾아내 고객 타게팅을 강화하고 커머스에 활용할 수 있는 의미 있는 정보를 찾아내는 기법

- AI 기술을 융합으로 관심 및 의도 패턴을 식별하여 오디언스 타겟팅을 강화하고 예측 모델을 생성하여 상품 추천 및 입찰을 향상시킬 수 있음

2. 데이터 커머스의 특징

1) ICT 기술 등장에 따른 데이터 커머스 특징

특징	설 명
산업 변화 특징	 출처 : KT 경제경영연구소
배경	- ICT 기술 발전으로 정보과잉 환경에서 소비자들은 극심한 구매 결정장애와 저가 상품에 대한 신뢰성 문제로 커머스에 시간과 비용은 과거보다 증가, 데이터 기반 맞춤형 커머스 등장

- 빅데이터 기술과 AI 기술로 데이터에 기반한 맞춤형 커머스는 더욱 정교해지고 있음

2) 데이터 커머스 특징

특징	설 명
고객 맞춤형 서비스	- 수집 생성된 개인별 데이터를 분석해 개별 고객 맞춤형 쇼핑 서비스 제공
개인 감성 분석	- 빅데이터 분석을 통해 인공지능이 개인이 원하는 취향을 찾아 맞춤형으로 제공
빅데이터 활용	- 다양한 유형의 개인별 데이터를 수집 분석하여 커머스에 활용
중계 플랫폼	- 소비자 맞춤형 상품 추천하고 판매자를 연결, 구매 중계

- 금융(핀테크), O2O, 홈쇼핑 등 다양한 분야에서 데이터 커머스 활용 가능

3. 디지털 커머스 활용 분야

분야 구분	활용 분야	활용 설명
금융	● 핀테크	- 소비자 검색 기록을 바탕으로 최저가 추천 및 이벤트 알림
	● 신용카드	- 소비 위치, 최근 상품 구매 이력에 따라 다음 구매할 상품을 예측하고 추천
O2O	● 배달앱	- 소비자 최근 검색기록, 위치에 따라 맛집을 추천하거나 날씨, 계절에 따른 구매이력을 바탕으로 주변 음식점 추천
	● 키오스크	- 키오스크를 통해 많은 사람들이 주문하는 상품, 서비스를 추천
광고	● 관심도 분석	- 특정 대상이 어떤 상품을 구매하려는 의도를 파악하고, 어떤 광고가 높은 관심을 얻을 수 있을지 분석
	● 영향 식별	- 광고에 가장 큰 영향을 미치는 카테고리, 카피라이트, 도메인 등 식별
애플리케이션	● 쇼핑 큐레이션 앱	- 이용자 데이터를 기반으로 관심 상품을 찾아주고, 맞춤형 서비스를 제공하는 모바일 앱
홈쇼핑	● T 커머스	- 데이터를 활용한 커머스 방송 - 시청자 데이터를 분석해 소비자 타깃 구분 동시간, 동일채널에 가구별로 맞춤형 쇼핑 방송을 송출

- 데이터 분석을 통해 맞춤형 상품 제공 및 구매를 유도하는데 필요한 모든 분야에 활용 가능

"끝"

기출풀이 의견

2. 1단락 개념 작성 후 주요기술은 알고 계신 기술들을 잘 그룹핑해 상세하게 작성하고, 2단락 특징은 2가지 측면으로 "가.", "나."로 구분해 풍부하게 작성하시는 것이 좋습니다. 또한 3단락 활용 분야는 되도록 다양한 산업분야를 토대로 작성하시면 다른분들과 차별화될 것으로 예상됩니다. 마지막으로 4단락에 활용 시 고려 사항으로 개인정보 보호, 보호된 정보 활용 가치 등 언급해주시면 고득점 받으실 것이라고 예상됩니다.

문 제	3. 데이터베이스 샤딩(Sharding)에 대한 아래의 사항을 설명하시오. 가. 샤딩의 개념 및 분할방법 나. 샤딩과 파티셔닝(Partitioning)의 차이점 다. 샤딩 적용 시 고려사항		
출 제 영 역	데이터베이스	난 이 도	★★★☆☆
출 제 배 경	- 4차산업혁명 관련 빅데이터 처리 등 효율적인 대용량 데이터 처리에 대한 기술적 방법 대두로 이해 대한 확인		
출 제 빈 도	- 1회(102회 정보관리 1교시)		
참 고 자 료	- DB 분산처리 기법 '샤딩'을 신중하게 수용해야할 이유(CIO Korea)		
K e y w o r d	- 수평분할, 수직분할, Vertical Partitioning, Range based Partitioning, Key or Hash based Partitioning, Directory based Partitioning		
풀 이	서현석(123회 정보관리기술사)		

1. 샤드키 기준으로 분리, 샤딩의 개념 및 분할 방법

1) 샤딩의 개념

구분	내용	
정의	- 물리적으로 다른 데이터베이스에 데이터를 수평 분할 방식으로 분산 저장하고 조회하는 기법	
특징	● **데이터베이스 위치 추상화**	- 어플리케이션 서버에서 물리적으로 데이터베이스의 위치를 알 필요 없음
	● **데이터베이스 신뢰 및 성능개선**	- 샤드에서 데이터 조회가 실패하더라도 다른 샤드에서 데이터 서비스 제공 가능

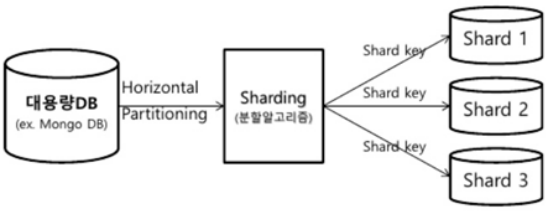
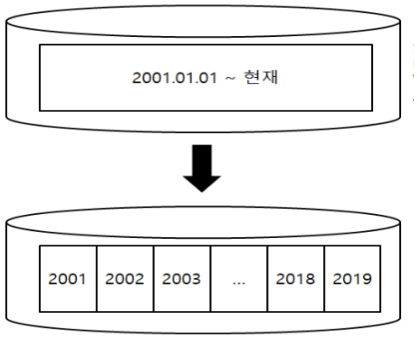
2) 샤딩의 분할 방법

분할방법	정의	특징
Vertical Partitioning	- 테이블 별로 서버를 분할하는 방식	- 구현이 간단, 전체 시스템에 큰 변화가 필요 없음
Range based Partitioning	- 하나의 feature 나 table 이 점점 거대해지는 경우 서버를 분리하는 방식	- 데이터를 분할하는 방법이 예측 가능해야 함
Key or Hash Based Partitioning	- 엔티티를 해쉬 함수에 넣어서 나오는 값을 이용해서 서버를 정하는 방식	- 해쉬결과 데이터가 균등하게 분포되도록 해쉬함수를 정하는 것이 중요
Directory Based Partitioning	- 파티셔닝 매커니즘을 제공하는 추상화된 서비스를 만드는 방식	- 데이터베이스 엑세스와는 떨어져 있는 샤드키를 Look-UP 할 수 있으면 됨

- 샤딩은 수평분할 방식을 이용하며 파티셔닝은 수평 분할 뿐만 아니라 수직 분할도 가능

2. 샤딩과 파티셔닝의 차이점

1) 개념 측면에서의 차이점

구분	샤딩	파티셔닝
정의	- 각각의 개별 파티션을 수평분할 방식을 사용하여 저장하는 기술	- 퍼포먼스, 가용성, 정비용이성 등의 목적을 위해 논리적인 엔티티들을 다른 물리적인 엔티티들로 나누는 기술
개념도		

2) 구성 측면에서의 차이점

구분	샤딩	파티셔닝
분할방식	- 수평 분할	- 수평, 수직 분할
키 여부	- 샤드 키 저장	- 키 없음
증설 방안	- Scale Up	- Scale out
데이터양	- 데이터 추가(샤드)	- 원본 데이터 분할
분할 데이터 저장위치	- 별도 서버 분리 저장	- 동일 서버 저장

- 샤딩 적용시 어플리케이션 연계 및 데이터베이스 구성 측면에서 트랜잭션, 파티셔닝, 조인 등을 고려하여 구성해야 함

3. 샤딩 적용 시 고려 사항

구분	고려사항	설명
어플리케이션 연계 측면	● **Global Transaction 사용 고려**	- Shared DB 간 Global Transaction 사용하여 트랜잭션 가능
	● **Sharding-DB 간 조인 고려**	- Sharding-DB 간에 조인이 불가능 하기에 처음부터 역정규화도 고려해야 함
	● **Global Unique key 고려**	- DBMS 에서 제공하는 Auto-Increment 를 사용하면 key 가 중복될 수 있기 때문에 Application 레벨에서 Guide 생성 해야 함
데이터베이스 구성 측면	● **서비스 정지 없이 Scale-up 가능 고려**	- 데이터베이스 서비스의 정지 없이 Scale-up 증설이 가능해야 함
	● **Shard 해쉬 함수 설계 고려**	- 성능 향상 및 파티셔닝을 위한 해쉬 함수 설계가 중요함

	● 작은 Table 단위 구성	- Table 단위를 가능한 작게 구성해야 함

- Vertical, Range 기반, Key or hash 기반, Directory 기반에 따른 샤딩 활용 사례 확인

4. 샤딩 활용 사례

구분	활용사례
Vertical Partitioning	- 사용자 프로필 정보용 서버, 사용자 친구 리스트 서버, 사용자 컨텐츠 서버 등을 분할하여 활용
Range based Partitioning	- 데이터가 많은 경우 지역, 일정, 위치 등 영역별로 데이터를 분리하여 활용
Key or Hash Based Partitioning	- 해쉬함수 이용 처리 속도 및 성능 향상을 우선시하는 경우 활용
Directory Based Partitioning	- DB 와 Cache 를 적절히 조합하여 활용 가능

- 샤딩 적용시 고려 사항으로 사드를 관리하기 위한 툴을 구축해야 하며, 다른 방안으로 데이터를 분할할 수 있는지에 대한 고려를 수행해야 함
- 샤딩이 필요해지는 이전 시점에 샤딩을 적용해야 하며, 샤딩 키에 대한 신중하게 선택 필요

"끝"

기출풀이 의견

3. 팩트가 있는 문제 이므로 샤딩 기술에 대한 명확한 답안을 작성해야 합니다. 샤딩과 파티셔닝의 차이점에서는 수평, 수직 분할 같은 명확한 차이점에 대해서 작성해야 합니다. 4단락에서는 샤딩의 활용 사례나 문제점에 대한 해결 방안을 기입하시면 답안이 풍성해질 것 입니다.

문 제	4. 최근 데이터 산업 발전을 위하여 "데이터 산업진흥 및 이용촉진에 관한 기본법"(약칭:데이터산업법)을 제정하였다. 이 법의 목적 및 주요 내용과 기대효과에 대하여 설명하시오.		
출 제 영 역	디지털서비스	난 이 도	★★★★☆
출 제 배 경	- 데이터 경제를 통한 경제 활성화 및 데이터 산업 육성을 위한 데이터 기본법 제정		
출 제 빈 도	미출제		
참 고 자 료	- 과학기술정보통신부 보도자료(데이터 산업 전반, 본격 육성한다! 데이터 경제를 활짝 여는 '데이터 기본법' 제정") - 데이터산업법의 의미와 주요쟁점(KISO 저널)		
Keyword	- 데이터 경제, 데이터 컨트롤 타워, 데이터 전문기업, 데이터 거래사, 국가데이터정책위원회		
풀 이	서현석(123회 정보관리기술사)		

1. 데이터 경제 창출, 데이터산업법의 정의 및 목적

1) 데이터산업법 정의

- 과학기술정보통신부에서 데이터 산업 발전 기반을 조성하고, 국가데이터정책위원회, 데이터 거래사 등을 통해 데이터 경제를 활성화하기 위해 제정된 법

2) 데이터산업법 목적

분류	주요 목적	설 명
국가경제 측면	● 데이터 경제 시대 주도권 확보	- 데이터 중요성이 부각되고 있는 상황 - 경제, 사회 전반에서 창출되는 데이터 활용의 중요성 부각
	● 4차 산업 경쟁력 확보	- 데이터와의 융합하는 인공지능, 5G 이동통신, 빅 데이터 등 데이터 활용 정책 추진
국가정책 측면	● 공공 부문 데이터 관련 기본법제 강화	- 기존 공공데이터의 제공 및 이용 활성화에 관한 법률, 데이터 기반 행정 활성화에 관한 법률로는 데이터 활용 위한 법적 근거 부족
	● 데이터 댐 정책 활성화	- 디지털 뉴딜 정책을 범국가적 프로젝트로 추진, 데이터 댐 중심으로 데이터 생산, 수집, 가공

- 국가 전체의 데이터 지휘본부(컨트롤 타워) 확립, 데이터 거래분석 제공 사업자 등 데이터 전문기업 체계적 육성, 데이터 경제 시대 혁신의 촉진자로서 데이터 거래사 양성, 데이터 자산가치와 권리가 보장되는 시장 조성 등의 주요 내용 포함

2. 데이터산업법 주요 내용

법조항	구분	주요내용
제 1 조, 제 2 조	● 목적•정의 규정	- 법의 목적을 데이터로부터 경제적 가치를 창출 - 데이터 산업 발전의 기반을 조성 - 국민 생활 향상 국가경제 발전에 이바지하는 것으로 규정, 데이터 등 관련 용어 정의
제 4 조	● 데이터산업 진흥	- 정부는 데이터 생산, 거래 및 활용 촉진, 기반 조성

	기본계획 수립	- 3 년마다 데이터 산업 진흥 기본 계획 수립
제 6 조	● **국가데이터 정책 위원회**	- 공공민간 데이터 정책을 총괄하는 기구를 설치 - 기본계획 수립, 데이터 생산, 거래 및 활용 관련 정책 개선 사항 - 데이터 산업 진흥 관련 계획 총괄•조정 심의
제 12 조	● **데이터 자산 보호**	- 인적 물적으로 상당한 투자와 노력으로 생성한 경제적 가치를 지니는 데이터를 보호
제 14 조, 제 20 조	● **데이터 가치 평가 지원, 품질관리**	- 데이터 가치 평가 기법 및 가치평가 체계 - 품질 인증 기준 등의 마련과 관련 업무 전담한 가치 평가 기관과 품질인증 기관 등 지정 추진
제 16 조	● **데이터 사업자 신고**	- 데이터 거래 사업자, 데이터 분석제공 사업자 등 과기정통부에 신고 - 신고 사업자에 대해 필요한 재정적, 기술적 지원할 수 있음
제 23 조	● **데이터 거래사 양성지원**	- 데이터 거래에 관한 전문지식이 있는 사람은 과기정통부 장관에 데이터 거래사로 등록할 수 있음 - 과기정통부는 데이터 거래사에게 데이터 거래업무의 수행에 필요한 정보제공 및 교육을 제공
제 24 조, 제 31 조	● **창업지원, 중소기업자 특별지원**	- 데이터 기반 산업 활성화 및 기업의 데이터 관련 역량 강화, 사업화 등 지원 - 데이터 각종 지원시책 시행 시 중소기업자 우선 고려 및 데이터 거래, 가공 등 필요 비용 일부 지원
제 25 조	● **전문인력 양성**	- 과기정통부 장관 및 행정안전부 장관은 데이터 전문인력 양성을 위한 시책 마련 - 과기정통부 장관은 전문인력 양성기관 지정 및 지원
제 34 조	● **데이터분쟁 조정 위원회 설치**	- 데이터의 생산, 거래 및 활용에 관한 분쟁을 조정하기 위한 데이터분쟁조정위원회 설치

- 데이터 컨트롤타워 확립과 데이터 전문기업 체계적 육성, 데이터 거래사 양성으로 인한 데이터산업법 기대효과 발생

3. 데이터산업법 기대 효과

구분	기대효과	설명
데이터 정책 측면	● **국민과 기업의 정책에 대한 예측성과 신뢰성 향상 기대**	- 국가 전체의 데이터 지휘본부(컨트롤 타워) 확립, 국가 전체의 지휘본부 확립, 중장기적 범부처 정책 수립은 국민과 기업의 정책에 대한 예측성과 신뢰성 향상
	● **데이터 생산, 거래, 활용 관련 분쟁조정위원회 조정 기대**	- 데이터의 정당한 가치를 평가하고, 이러한 가치를 가지는 데이터의 무단 취득, 사용공개 등의 방지 - 데이터 자산 관련 분쟁시 소송전 분쟁조정위에서 조정 신청 가능
데이터	● **데이터 전문기업 체계적 육성**	- 데이터 전문기업 체계적 육성에 따른 데이터

활성화 측면	기대	산업기반 조성에 기여 효과
	● 데이터 거래사 양성 기대	- 전문지식을 바탕으로 데이터 거래에 관한 상담, 중개, 알선 등을 수행 - 데이터 거래사 등록제 운영과 함께 교육 등 필요한 지원 제공 예정

- 향후 데이터산업법의 지속 발전을 위한 개정 방안으로 국가 주도 진흥에서 민간 주도 진흥으로 패러다임을 바꾸고, 국가 데이터 정책위원회는 국가 데이터 규제 개혁위원회로 변경하여 각종 데이터 규정에 대한 해소 필요

"끝"

기출풀이 의견

4. 법 관련 팩트가 명확한 문제 이므로 내용을 정확히 모르는 경우에는 선택하시면 안됩니다. 데이터 산업법에 대해 주요 내용을 숙지하고 있다면 숙지된 내용을 명확히 작성하고 목적 및 기대효과는 주요내용을 기반으로 작성하셔도 충분히 좋은 답안이 될 거라고 생각됩니다.

문 제	5. UML 2.0 의 순차 다이어그램(Sequence Diagram)에 대한 아래의 사항을 작성하시오. 가. 순차 다이어그램의 목적과 작성순서, 구성요소별 표기법 (구성요소: Frame, Object, Lifelines, Activation Box, Messages, Guard) 나. 아래의 도서예약시스템의 협력 다이어그램(Collaboration Diagram)을 순차 다이어그램으로 변환		
출 제 영 역	소프트웨어공학	난 이 도	★★☆☆☆
출 제 배 경	- 객체 지향 설계를 위한 시퀀스 다이어그램에 대한 이해 확인		
출 제 빈 도	UML 은 빈출. 순차 다이어그램 2 회 출제(관리 – 126 회, 86 회)		
참 고 자 료	- UML 사이트(https://www.uml-diagrams.org) - 객체지향 설계 및 구현(저자 김철진, 조은숙, 배동희)		
K e y w o r d	- Interaction, 순차, 시간, 통신, 관계, 협력, 상호작용, 유즈케이스, 클래스 다이어그램, 타이밍 다이어그램, Combined Fragment		
풀 이	서현석(123 회 정보관리기술사)		

1. 구성요소간 상호 작용 표현, 상호작용 다이어그램의 개요

구분	설 명	
정의	- 객체들 간에 주고받는 메시지를 통해 상호작용을 명세하고 유스케이스를 수행하기 위해 객체들 간의 상호작용을 표현하는 다이어그램	
유형	● **Sequence**	- 객체들 간의 상호작용을 발생 순서에 초점을 둔 다이어그램
	● **Communication**	- 객체들 간의 상호작용 연결에 초점을 둔 다이어그램
	● **Interaction Overview**	- Sequence 와 Activity Diagram 의 결합 형태의 다이어그램
	● **Timing**	- 객체들간의 상호작용을 시간 제약에 초점을 둔 다이어그램

- Communication Diagram 은 UML 1.0 의 협력(Collaboration) 다이어그램 계통으로 순차 다이어그램과 메시지 순서 연결은 동일하나 관계와 시간 측면의 차이점 존재

2. 순차 다이어 그램의 목적과 작성순서, 구성요소별 표기법 설명

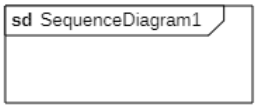
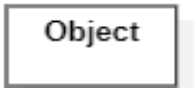
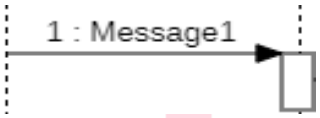
1) 순차 다이어그램의 목적과 작성순서

구분	설 명	
정의	- 시스템이 실행시 생성되고 소멸되는 객체를 표기하고 객체들 사이에 주고받는 메시지를 시간의 발생 순서에 중점을 둔 다이어그램	
목적	● **순서 초점 표현**	- 어떤 결과를 만들어내는 이벤트 시퀀스 정의
	● **오퍼레이션 정의**	- 시스템의 논리적 해석 통해 객체가 지니게 되는 동작 정의
	● **시스템 흐름 시각화**	- 개발자, 업무 담당자 모두에게 동작 흐름을 설명
	● **요구사항 명세**	- 시스템 구현에 필요한 요구사항들을 기록하는 문서로서 사용
작성순서	① **액터 파악**	- 유스케이스 정의서 및 다이어그램 분석하여 액터를 파악

	② 객체 파악	- 유스케이스 정의서 분석으로 참여 객체 파악
	③ 액터 및 객체 나열	- 액터와 참여 객체를 순차 다이어그램의 수평 축에 나열
	④ 메시지 정의	- 객체간의 메시지를 시간의 순차에 맞춰 정의

- UML1.X 대비 in-line 가드에 대한 부족 부분을 UML 2.0 에서는 Combined fragment 등으로 보완 가능

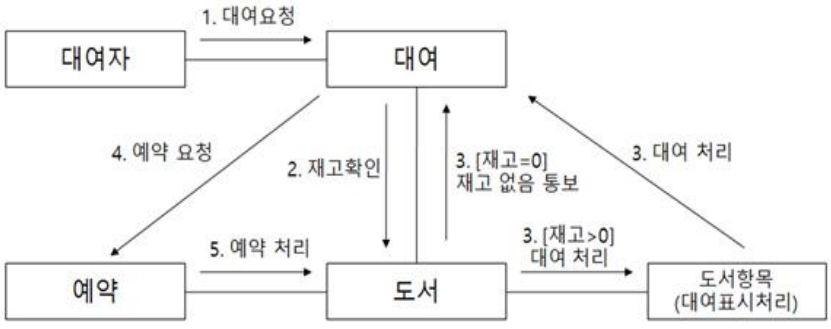
2) 순차 다이어그램의 구성 요소별 표기법

구성요소	표기법	설명
Frame		- 다이어그램의 전체 또는 일부를 묶어 표현 - sd, dep, act, pkg, uc 등
Object		- 메시지 교환에 참여하는 객체 - 시스템 행위자 또는 시스템 내의 유효한 객체
Lifelines		- 객체가 시스템상 실행 여부를 표현하는 기준선 - 메시지 전달 시 생명선에 활성 막대가 생성
Activation Box		- 객체가 시스템에 존재함을 의미 - Box 의 길이는 해당 메소드의 실행 소요 시간
Messages		- 객체간의 전달되는 메시지 - 동기/비동기/Self 메시지 형태 존재
Guard		- 대괄호를 이용하여 조건을 명시하는 방법 - In-line 별 조건의 메시지 흐름 표현

- 시퀀스 다이어그램은 유스케이스 다이어그램, 클래스 다이어그램 등 정적 모델링 수행 후 작성
- 협력 다이어그램과 순차 다이어그램은 행위에 대한 메시지 순서 표현과 시각화 표현이라는 공통점 존재

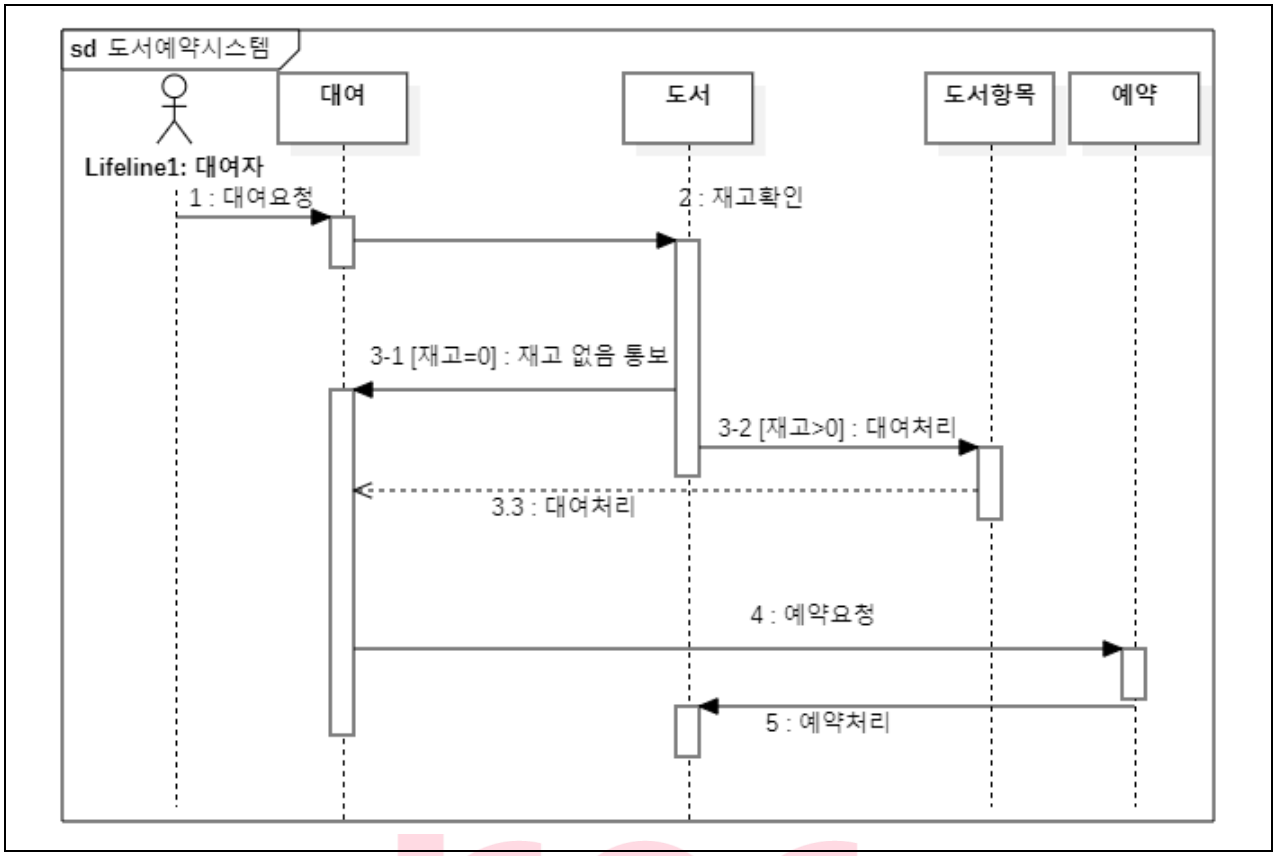
3. 도서예약시스템의 협력 다이어그램(Collaboration Diagram)을 순차 다이어그램으로 변환

1) 도서예약시스템 협력 다이어그램 분석

구분	설명	
협력 다이어그램		
분석사항	● 액터 파악	- 대여자가 액터로서 대여라는 시스템을 호출
	● 객체 파악	- 대여, 예약, 도서, 도서항목(대여표시처리)
	● 객체 배치	- 대여자 -> 대여 -> 도서 -> 도서항목(대여표시처리) -> 예약
	● 메시지 정의	- 1~5 번의 순차적 메시지 흐름 확인, 3 번 Guard 명시 확인

- 3 번 메시지는 In-line 조건으로 도서 재고 존재 여부 따라 대여처리 또는 예약 관련 메시지가 순차적으로 진행

2) 순차 다이어그램의 변환 결과



- 순차 다이어그램 작성 시 긴 시나리오는 분할하고 메시지 순서에 따라 좌에서 우, 위에서 아래로 작성 필요

4. 순차 프로그램 작성시 유의사항

구분	유의사항	설 명
객체 및 메시지 순서	● 액터와 객체 나열 순서	- 액터 우선, 객체는 메시지 겹침 최소화
	● 메시지 작성 순서	- 발생 순서 기준으로 위에서 아래, 좌에서 우로 작성
객체 배치 및 연결	● 객체 메모리 존재 확인	- 소멸 오브젝트 인한 메모리 부족 발생 가능성 점검
	● 객체 이해 명확성	- 수신 객체 동작 명확히 파악 후 메시지 전달

- 다이어그램 작성시 참여하지 않는 객체는 제외하고 1 개의 다이어그램은 1 개의 시나리오에서만 작성
- 순차, 통신 다이어그램은 유즈케이스 다이어그램 이후 활용 가능하며 클래스 다이어그램 등과 연계 작성하여 메시지 순서와 객체 등의 명확화 및 가시화가 가능

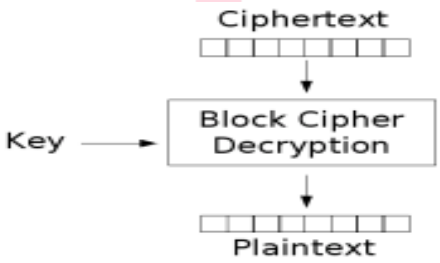
"끝"

기출풀이 의견

5. UML은 빈출 문제로서 이번 문제인 시퀀스 다이어그램은 언제든지 출제 가능하니, 간단한 다이어그램은 작성 가능하도록 학습 필요합니다. 메시지의 순서라는 협력 다이어그램(UML2.0 통신 다이어그램)과는 서로 간 변환이 가능하니 이점을 간글에 추가하시면 차별화가 가능할 것 같습니다.

문 제	**6. 블록(Block) 암호 모드에 대한 아래의 사항을 설명하시오.** **가. ECB(Electronic CodeBook) 모드** **나. CBC(Cipher Block Chaining) 모드** **다. CFB(Cipher FeedBack) 모드** **라. OFB(Output FeedBack) 모드**
출 제 영 역	보안 / 난 이 도 ★☆☆☆☆
출 제 배 경	- 블록 암호화 운용 모드에 대한 이해 확인
출 제 빈 도	미출제
참 고 자 료	- 현대 암호학(저자 원동호) - 위키 백과(https://ko.wikipedia.org/wiki/블록_암호_운용_방식)
K e y w o r d	- IV, 패딩, 블록간 영향, 스트림 암호, AES, DES, Feistel, SPN, 전치, 대체, CTR, PCBC
풀 이	서현석(123 회 정보관리기술사)

1. 대칭키 암호화 방식, 블록 암호화(Block Chipher)의 개요

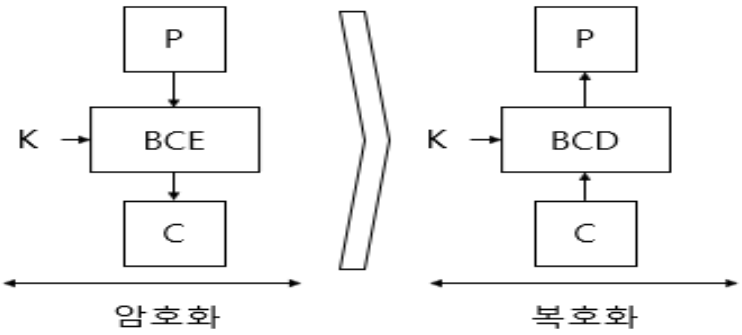
구분	설 명	
정의		- 평문을 일정한 블록 단위로 나누어 각 블록마다 암호화 과정을 수행하여 고정된 크기의 블록 단위 암호문을 생성하는 암호화 방식
활용 원리	● **혼돈**	- 비선형 함수. 암호문과 키 사이 관계 숨김
	● **확산**	- 선형 함수. 전치와 치환 통해 암호문과 평문과의 관계 숨김
구조별 알고리즘	● **Feistel 구조**	- DES, TDES, SEED, LOKI, CAST, Blowfish, MISTY, RC5, RC6
	● **SPN 구조**	- IDEA, AES, ARIA, SHARK, SAFER, Square, Rijndael, Serpent
운용 모드	● **평문 암호 방식**	- ECB, CBC, PCBC(Propagating CBC)
	● **키스트림 암호 방식**	- CFB, OFB, CTR(CounTeR)

- 블록 암호화 운용 모드 동작시 초기 암호화를 위한 초기화 벡터 및 복호화 처리 위한 패딩 등을 활용
- ECB 는 가장 단순한 암호 방식이며, CBC 는 암호화 연쇄처리로 CTR 과 함께 사용 권장되는 운영 모드

2. ECB(Electronic CodeBook) 모드와 CBC(Cipher Block Chaining) 모드 설명

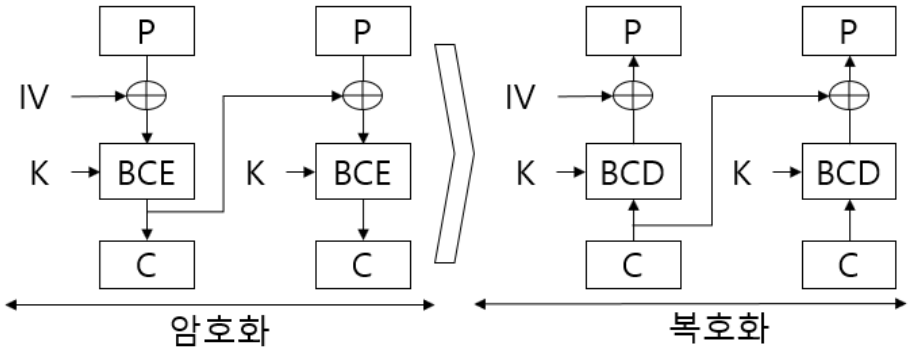
1) ECB(Electronic CodeBook) 모드 설명

구분	설 명
정의	- 암호화하려는 평문을 여러 블록으로 나누고 블록 단위를 비밀키로 암호화하여 오류 전파 방지 및 병렬 처리 등이 가능한 암호 모드

암/복호화 매커니즘	 - P : Plain text, C : Cipher text, K : Key - BCE : Block Cipher Encryption, BCD : Block Cipher Decryption	
특징	● 오류 미전파	- 블록 단위별 암호화로 다음 블록으로 오류 전파 없음
	● 병렬 처리 가능	- 동일 키와 암호화 방식 구성으로 암/복호화 병렬 수행 가능
	● 패딩 필요	- 암호문은 블록의 배수가 되어 복호화 후 패딩 필요
	● 반복 공격 취약	- 평문 블록의 내용 동일시 암호 블록도 동일. 반복 공격 가능

- ECB 모드는 Brute-Force Attack, Dictionary Attack, 재생공격 등이 가능하여 미사용 권장

2) CBC(Cipher Block Chaining) 모드 설명

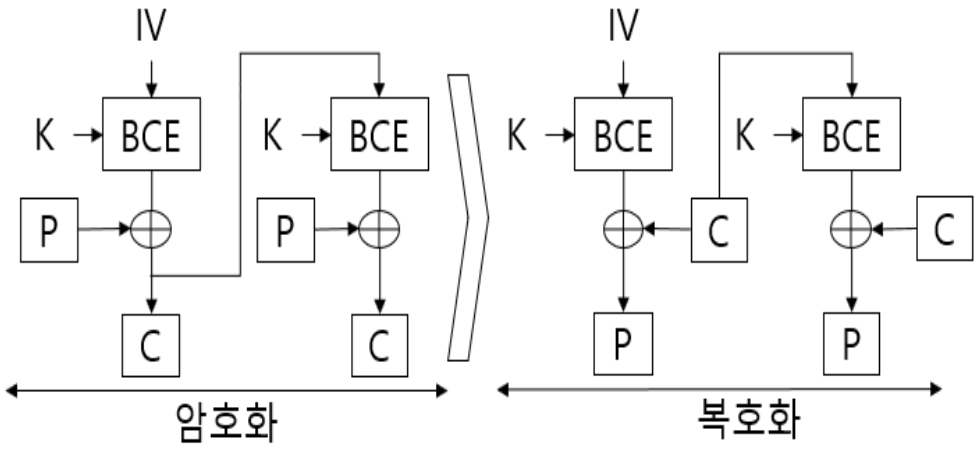
구분	설 명	
정의	- 첫 블록은 초기화 벡터로 암호화하고, 이후 각 블록은 이전 암호문 결과와 XOR 연산을 순차적으로 반복하는 암호 모드	
암/복호화 매커니즘		
특징	● 초기 IV 변경	- IV 가 같으면 초기 출력 결과가 동일 특성 이용한 공격 가능
	● 복호화 병렬 처리	- 복호화시 블록 암호화 후 이전 암호화블록과 XOR 로 복구 가능
	● 블록간 오류 전파	- 암호문 손상 후 복호화시 해당 평문과 다음 평문 블록에 영향
	● 암호화 순차 진행	- 이전 암호문은 다음 암호문에 영향으로 순차 수행 필요 - 암호화시에는 병렬 처리 불가

- CFB, OFB 암호 모드는 평문의 직접 암호화 대신 IV 를 블록 암호화 후 암호문을 생성하는 방식

3. CFB(Cipher FeedBack) 모드와 OFB(Output FeedBack) 모드 설명

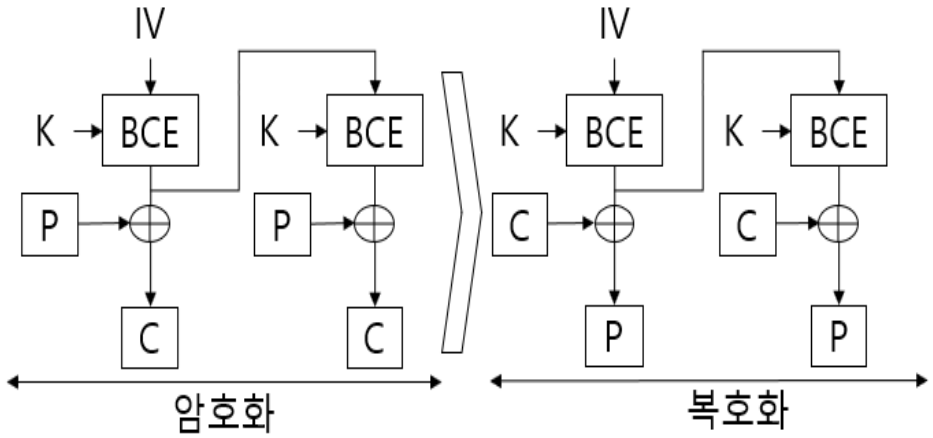
1) CFB(Cipher FeedBack) 모드 설명

구분	설 명
정의	- 초기화 벡터(IV)를 블록암호화 후 평문 블록과 XOR 연산으로 암호문 블록을 생성하고, 생성된 암호문을 다음 블록의 IV 로 사용하는 암호모드

암/복호화 매커니즘		
특징	● **Bit 단위 암호화**	- 키 스트림 활용으로 평문 블록의 데이터를 1bit 단위 암호화 가능
	● **패딩 불필요**	- 평문이 아닌 IV 의 암호화 처리로 복호화시 패딩 불필요
	● **오류 영향 전파**	- 암호문 블록 손상시 복호화 중 해당 평문과 다음 평문블록 영향
	● **재전송 공격 취약**	- 전송된 암호 블록의 임의 부분 변경시, 평문 내용 변경 전송 가능

- CFB 모드에서는 재전송공격에 취약하므로 매번 다른 값의 IV 사용하거나, 미사용 권장

2) OFB(Output FeedBack) 모드 설명

구분	설 명
정의	- 초기화 벡터(IV)를 블록 암호화해서 생성한 키스트림 값을 평문 블록과 XOR 연산하여 암호문 블록을 생성하는 암호 모드
암/복호화 매커니즘	

특징	● **암/복호 동일**	- XOR 명령 대칭으로 암호화와 암호 해제 방식 동일
	● **사전 준비 가능**	- 키스트림 값을 미리 생성 가능하여 암호화 및 XOR 연산속도 향상
	● **병렬 처리 불가**	- 암/복호화시 키스트림 영향으로 병렬 처리 불가능
	● **오류 영향 최소화**	- 암호문 블록 오류 발생시 대응하는 평문 블록에만 영향

- CFB 는 자기동기 스트림 암호 변환, OFB 는 동기식 스트림 암호로 블록암호를 변환
- CTR 모드는 OFB 모드와 동일한 스트림 암호 일종이나 입력 값에 대한 차이 존재

4. OFB(Output FeedBack) 모드와 CTR(CounTeR) 모드의 비교

비교항목	CTR(CounTeR)	OFB(Output FeedBack)
입력 값	- 카운터 값을 암호화로 입력	- IV 암호화 출력을 입력

병렬 처리	- 난수 사용으로 암/복호 병렬 처리 가능	- 키스트림 사전 생성만 가능
키스트림 반복	- 키스트림 값의 동일 생성 없음	- 키스트림 동일 값 생성시, 이후 값 동일
기밀성	- 복호화시 1 비트 단위 반전 가능하여 통신 오류와 기밀성의 동일 성질 보유	

- OFB 와 CTR 모드는 스트림 암호 특성의 동일 구조 형태이나, OFB 는 동일 스트림 값에 대한 공격 가능
- OFB 의 재전송 공격 대응 위해 비표(Nonce)와 Counter 기반 연속적 난수를 생성하는 CTR 모드 사용 권장

"끝"

기출풀이 의견

6. 블록 암호 운영 모드는 많은 분들이 알고 계신 토픽으로, 작성시에는 각 모드별 복호화까지 작성하시는 것을 고려해보시고 각 운영 모드별 장/단점을 정확히 제시하시면 고득점 기대됩니다. 또한 MAC, RSA, 복합암호화 등 타 암호화와의 연계하여 간글 제시하신다면 다른 분과 차별화될 것으로 예상됩니다.