제127회 정보관리기술사 해설집

2022.04.16

국가기술자격 기술사 시험문제

기술사 제 127 회 제 4 교시(시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명 하십시오. (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 매쉬(Service Mesh)

2. 데이터 커머스(Data Commerce)의 중요성이 점차 증대되고 있다. 데이터 커머스에 대한 아래의 사항을 설명하시오.

   가. 개념과 주요기술

   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 이용에 관한 촉진법"(약칭:데이터산업법)을 제정하였다. 이 법의 목적 및 주요 내용과 기대효과에 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(Electronic CodeBook) 모드

나. CBC(Cipher Block Chaining) 모드

다. CFB(Cipher FeedBack) 모드

라. OFB(Output FeedBack)

01	MSA(Micro Service Architecture)		
문제	최근 여러 기업에서 MSA(Micro Service Architecture) 도입이 활발하게 이루어지고 있다. MSA에 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)		
도메인	소프트웨어 공학	난이도	하 (상/중/하)
키워드	구현원칙, Control plain, Data plain		
출제배경	MSA 확산에 따른 개념 확인		
참고문헌	ITPE 120회 기출문제 풀이집 / ITPE 10회 모의고사		
해설자	안응원 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

I. MSA 개념 및 특징과 구현시 지켜야 할 원칙

가. MSA의 개념 및 특징

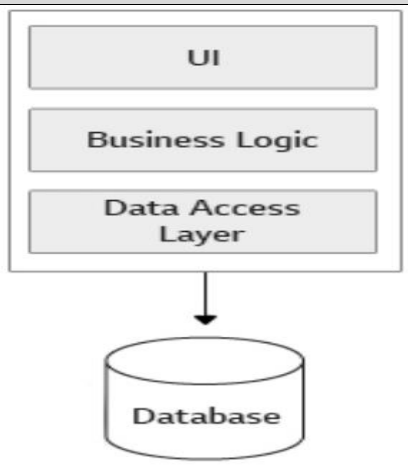
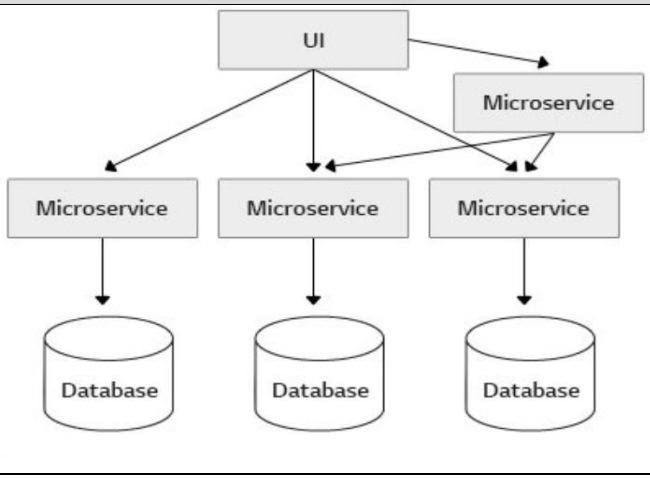
구분	설명	
개념	- 데이터에서부터 비즈니스 로직까지 독립적으로 상호 컴포넌트간의 의존성이 없이 개발된 컴포넌트로 REST API와 같은 표준 인터페이스로 그 기능을 외부로 제공하기 위한 서비스 아키텍처	
특징	경량화	- 하나의 비즈니스 범위에 맞추어 생성되어 하나의 기능만 수행
	다양한 아키텍처	- 서로 다른 서비스는 서로 다른 언어로 개발 가능
	컴포넌트 구성	- 서비스에 의한 컴포넌트로 구성
	진화적 디자인	- 능동적 변화에 대응 가능한 설계 원칙

나. MSA 구현시 원칙

원칙	설명
Strong Module Boundaries (명확한 모듈 경계)	- 시스템 변경 사항이 발생하면, 변경할 특정 도메인 내 마이크로서비스 단위만 이해하고 처리
Independent Deployment (독립적 배포)	- Loose Coupling이나 High Cohesion와 같은 의존성 관계를 고려하여 시스템을 설계, 구축함으로, 각각의 마이크로서비스를 독립적으로 배포하는 것을 용이
Technology Diversity (기술 다양성)	- 마이크로서비스의 독립성이 강화되면서, 마이크로서비스 내의 기술 선택이 자유로움

II. 모놀리스 아키텍처(Monolith Architecture)와 MSA 비교

가. 모놀리스와 마이크로서비스 아키텍처의 개념도

모놀리스 아키텍처	마이크로서비스 아키텍처
	

※ 그림출처 : IT Insight - 최신 IT 를 만나다(LG CNS)

- 마이크로서비스 아키텍처의 등장으로 이전까지의 단일 아키텍처를 모놀리스라고 분류

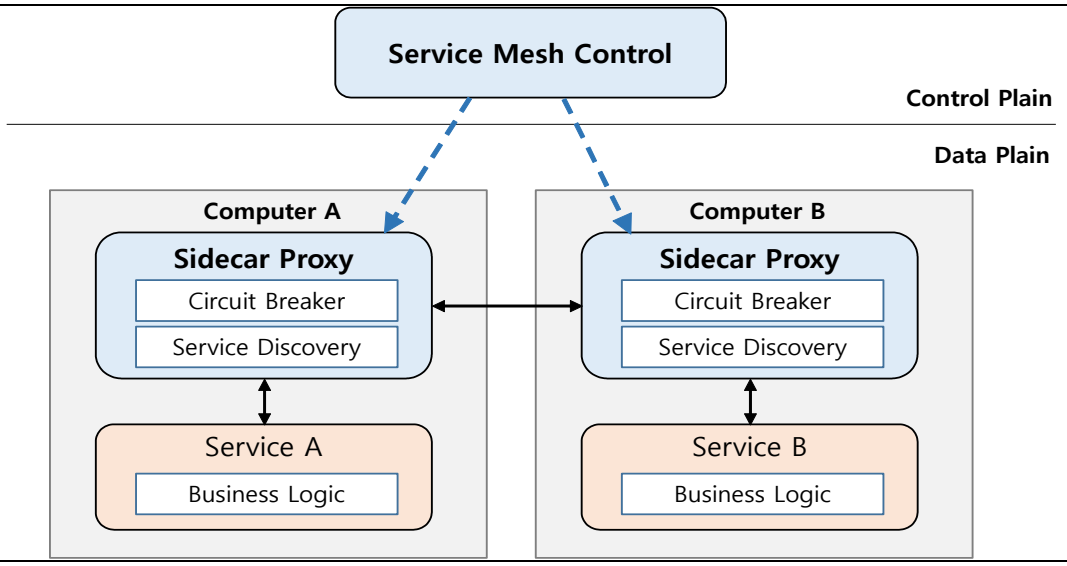
나. 모놀리스와 마이크로서비스 아키텍처 개념의 상세 비교

항 목	모놀리스 아키텍처	마이크로서비스 아키텍처
개념	하나의 서비스 또는 애플리케이션이 하나의 아키텍처로 구현된 방법	하나의 큰 애플리케이션을 여러 개의 작은 애플리케이션으로 구현하여 조합하는 방법
목적	전체 어플리케이션을 하나의 통합된 패키지로 개발, 배포	어플리케이션을 개별서비스 단위로 개발, 배포
개발	배포, 테스트, 표준화된 방식으로 관리 용이	- 서비스 단위의 신속한 개발, 확장 용이
특징	- 서비스 복잡도, 규모 증가에 따른 문제점 증가 - 배포 시간의 증가 - 부분적 스케일 아웃의 어려움 - 안정성의 감소	- 특정 서비스의 오류가 다른 서비스에 영향을 주지 않음 - 서비스 별 다른 언어로 개발 가능 - 분산시스템에 따른 추가적인 복잡도 증가

- 전체의 서비스를 포함하는지, 최소한의 서비스만 포함하는지의 여부로 구분가능

III. MSA 구현을 위한 서비스 매쉬(Service Mesh)

가. 서비스 매쉬의 정의 및 아키텍처

구분	설 명
정의	- 서비스 앞 단에 경량화된 프록시를 배치하여 서비스 간의 통신을 제어하는 아키텍처 패턴(Architecture Pattern)
아키텍처	

나. 서비스 매쉬의 주요 기술요소

구분	기술요소	설명
아키텍처	- Control Plane	- 중앙 집중화된 컨트롤러(Controller)에서 프록시(Proxy) 설정 정보 통제 - 컴포넌트(Component)의 관리 및 모니터링(Monitoring) 수행
	- Data Plane	- 트래픽(Traffic)을 설정에 따라 프록시를 통해 전달
컴포넌트	- Sidecar Proxy	- 어플리케이션 컨테이너(Container)와 별도로 추가적 사이드카 컨테이너 배포 - 실제 서비스와 병렬로 구성하여 프록시 호출
	- Service Discovery	- 서비스 시작 시 컨트롤러에 게시 - 트래픽 규칙과 구성을 프록시에 배포
	- Circuit Breaker	- Destination Rule을 정의하여 연결 및 이상 감지 - 마이크로서비스의 Resiliency 제공
비즈니스	- Business Logic	- 마이크로서비스에서 수행되는 비즈니스 기능 및 데이터 입출력

- 마이크로서비스(MicroServices)에는 비즈니스 로직(Business Logic)을 중심으로 남게 되어 경량화 구현 가능

IV. 서비스메시와 API Gateway의 비교

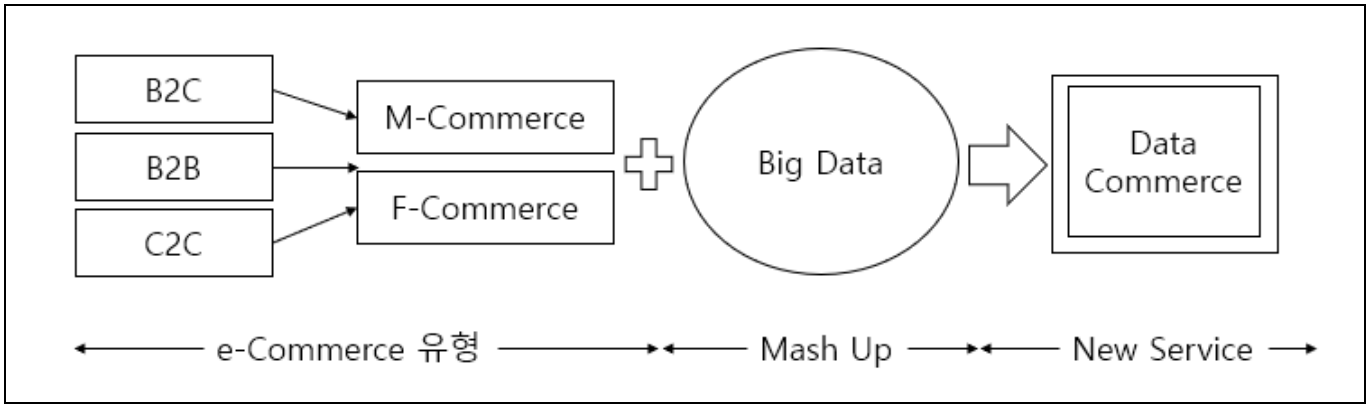
비교	서비스메시	API Gateway
특징	- 분산형 아키텍처 - 개별서비스 통신 제어	- 중앙집중형 아키텍처 - 내부 서비스 제어 및 보호
네트워크구성	- 서비스 내 Sidecar 구성 (Internal)	- 독립적인 API Gateway 구성 (External)
라우팅단위	- 요청 서비스	- 요청 서버
서비스호출	- Sidecar Proxy Pattern 사용 - 호출자 코드 내 공급자 주소 및 Failover 코드 삽입	- Gateway Proxy pattern 사용 - 단일 엔드포인트(Endpoint) 제공
서비스분배	- Service Registry 서비스 목록 수신 - Sidecar에서 로드밸런싱 알고리즘 수행	- 로드밸런싱(Load Balancing) 구성요소에 요청하여 Redirect
결함허용	- 개별 서비스에 한정	- API Gateway 장애 시 전체 서비스 영향 (SPOF, Single Point Of Failure)

- API Gateway 가 구현 편의성 측면에서 유리하나 단일 접점제공(SPOF)으로 장애발생 시 영향범위가 넓으므로 기업의 아키텍처(Architecture) 요구사항을 종합적으로 고려하여 적합한 방식 선택

"끝"

02	데이터 커머스(Data Commerce)		
문제	데이터 커머스(Data Commerce)의 중요성이 점차 증대되고 있다. 데이터 커머스에 대한 아래의 사항을 설명하시오. 가. 개념과 주요기술 나. 특징 다. 활용 분야		
도메인	IT 경영전략	난이도	중(상/중/하)
키워드	빅데이터, 연관분석, 상관분석, 군집분석, 추천시스템		
출제배경	빅데이터 확산으로 인한 e-Commerce 의 발전 동향 확인		
참고문헌	2017년 ICT(Information Communication Technology) 10대 이슈 키워드		
해설자	안응원 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

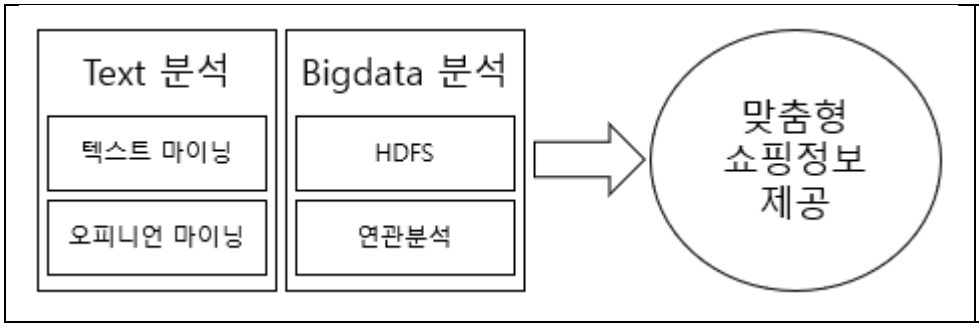
I. e-Commerce 시장의 진화, 데이터 커머스의 등장배경



- 다양한 commerce의 등장 및 빅데이터의 확산으로 인해 데이터 분석 기술 기반의 Data Commerce 등장

II. Data Commerce의 개념 및 특징

가. Data Commerce의 개념



- 데이터 분석 기술을 기반으로 소비자와 상품 데이터를 분석해 맞춤형 쇼핑 정보를 제공하는 커머스

나 Data Commerce의 특징

특징	설명
맞춤형 정보	데이터 분석을 통한 개인별 맞춤형 상품 추천
중계 플랫폼	기업과 소비자간의 중계 역할 수행
빅데이터 활용	다양한 채널에서의 데이터를 이용한 새로운 형태의 Commerce

III. Data Commerce의 주요기술 및 활용분야

가. Data Commerce의 주요기술

구분	주요기술	설명
마이닝	텍스트 마이닝	대규모의 문서(text)에서 의미있는 정보를 추출
	오피니언 마이닝	웹 사이트와 소셜 미디어에서 특정 주제에 대한 여론이나 정보글을 수집하고 분석해 결과를 도출하는 빅데이터 처리 기술
	웹 마이닝	인터넷을 이용하는 과정에서 생성되는 웹 로그(web log) 정보나 검색어로부터 유용한 정보를 추출하는 웹 대상의 데이터 마이닝
빅데이터 기술	Hadoop	빅데이터 활용을 가능하게 만든 빅데이터 플랫폼
	NoSQL	전통적인 관계형 데이터베이스 RDBMS와 다르게 설계된 비관계형 데이터베이스
	연관분석	룰기반의 모델로 상품과 상품사이에 어떤 연관이 있는지 찾아내는 알고리즘
	상관분석	두 변수 간에 어떤 선형적 관계를 갖고 있는 지를 분석하는 방법

- 다양한 빅데이터 분석 기술 및 AI기술 접목을 통해 정확도 높은 분석 가능

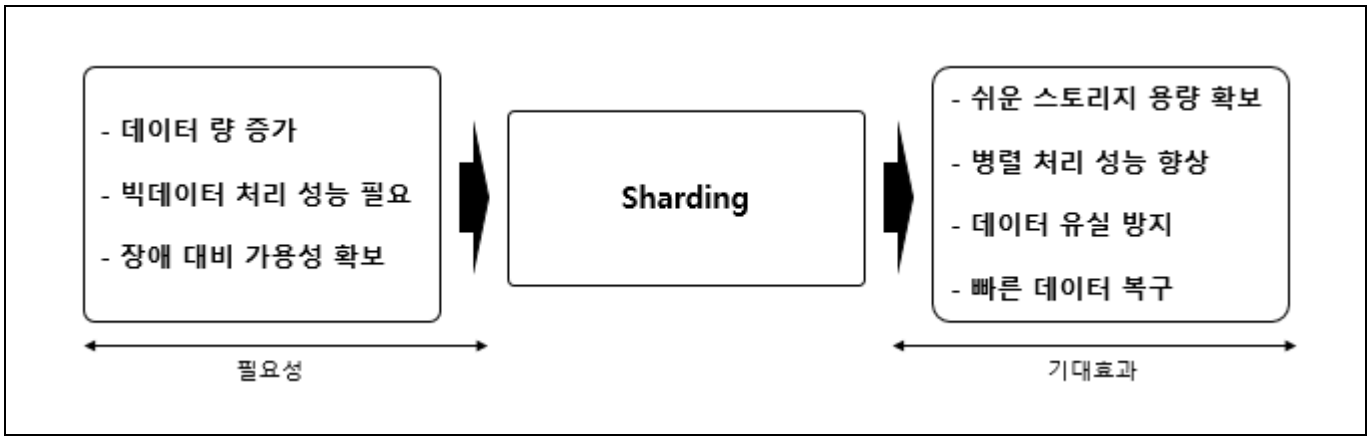
나. Data Commerce의 활용분야

활용분야	설명
포털 사이트의 쇼핑 서비스	다년간 누적된 검색 데이터 및 이용자의 데이터를 분석해 다양한 쇼핑 정보를 제공
쇼핑 큐레이션 앱	이용자 데이터를 기반으로 맞춤형 정보를 제공하는 모바일 앱
T 커머스	방송 시청가구 데이터를 기반으로 타깃을 구분하여 동시간, 동일채널에서 가구별로 다른 쇼핑 방송을 송출하는 방식

끝"

03	샤딩(Sharding)		
문제	데이터베이스 샤딩(Sharding)에 대한 아래의 사항을 설명하시오. 가. 샤딩의 개념 및 분할방법 나. 샤딩과 파티셔닝(Partitioning)의 차이점 다. 샤딩 적용 시 고려사항		
도메인	데이터베이스	난이도	상 (상/중/하)
키워드	샤드, 수평분할, Vertical Partitioning, Range based Partitioning, Key or Hash Based Partitioning, Directory Based Partitioning		
출제배경	데이터베이스 확장성 증가에 따른 주요 기술은 샤딩에 대한 이해 확인		
참고문헌	ITPE 서브노트 https://itwiki.kr/w/데이터베이스_샤드		
해설자	정상반 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 대용량 데이터 증가로 인한 효율적 관리, 샤딩(Sharding)의 필요성



- 기업은 점점 빅데이터 저장 및 처리를 필요로 하여 데이터 분산 저장을 지원하며 신속한 증설이 가능한 샤딩(Sharding)이 점점 주목받고 있음

II. 다수의 데이터베이스 분산 저장, 샤딩(Sharding)의 개념 및 분할방법

가. 샤딩(Sharding)의 개념, 특징 및 구성요소

구분	주요 내용	
개념	- DBMS 레벨에서 데이터를 나누는 것이 아니고 물리적으로 다른 데이터베이스에 데이터를 샤드(Shard)라고 부르는 각각의 개별 파티션으로 수평 분할 방식으로 분산 저장하고 조회하는 기법	
특징	성능개선	- 큰 데이터를 압축, 개별테이블은 각 샤드에서 더 빠른 작업 지원
	신뢰성 개선	- 한 샤드가 실패하더라도 다른 샤드는 데이터 서비스를 제공
	위치 추상화	- 어플리케이션 서버에서 어떤 데이터가 어떤 데이터베이스에 위치해 있는지 알 필요가 없음
구성요소	Shard DB	- 분할된 테이블과 데이터를 포함하고 있으며, 실제로 사용자 요청을 처리하는 데이터베이스

	shard metadata	- CUBRID SHARD의 동작을 위한 설정 정보. 요청된 질의를 분석하여 실제 질의를 수행할 shard DB를 선택하기 위한 정보 및 세션을 생성하기 위한 정보를 포함
	shard key	- (column)sharding된 테이블에서 shard를 선택하기 위한 식별자로 사용되는 칼럼
	shard key data	- 질의 중 shard를 식별하기 위한 힌트에 해당하는 shard key의 값
	shard ID	- shard DB를 식별하기 위한 식별자
	proxy	- 사용자 질의에 포함된 힌트를 해석하고, 해석된 힌트와 shard metadata를 이용하여 실제 질의 처리할 shard DB로 요청을 전달 역할을 하는 CUBRID 미들웨어 프로세스

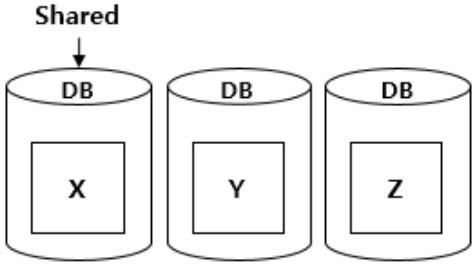
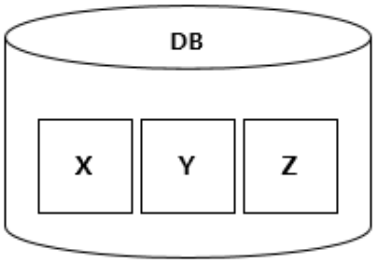
나. 샤딩의 분할방법

방법	설명	사례/특징
Vertical Partitioning	-테이블 별로 서버를 분할하는 방식 -구현 간단. 전체 시스템에 큰 변화 필요 없음. 각 서버 데이터 거대해지면 추가 샤딩 필요	-사용자 프로필정보용 서버, 사용자 친구리스트용 서버, 사용자가 만든 콘텐츠용 서버 등으로 분할하는 방식
Range based Partitioning	-하나의 feature나 table이 점점 거대해지는 경우 서버를 분리하는 방식 -데이터를 분할하는 방법이 예측 가능해야 함	-사용자가 많은 경우 사용자의 지역정보를 이용해서 user 별로 서버를 분리하거나, 일정데이터라면 연도별로 분리, 거래정보라면 우편번호를 이용하는 방식
Key or Hash Based Partitioning	-엔티티를 해쉬 함수에 넣어서 나오는 값을 이용해서 서버를 정하는 방식 -해쉬 결과 데이터가 균등하게 분포되도록 해쉬 함수를 정하는 게 중요	-예) 사용자ID가 숫자일 경우 나머지연산을 이용하는 방법
Directory Based Partitioning	-파티셔닝 메커니즘을 제공하는 추상화된 서비스를 생성	-샤드키를 look-up 할 수 있으면 되므로, 구현은 DB와 캐쉬를 적절히 조합해서 만들 수 있음

- 샤드 간 조인이 안되는 제한사항이 있으며, 전역적인 Unique Key는 응용(App)에서 생성할 필요가 있음.

III. 샤딩과 파티셔닝(Partitioning)의 차이점

가 샤딩과 파티셔닝 개념적 차이점

구분	샤딩	파티셔닝
개념도		
개념	- 데이터를 여러 데이터베이스 인스턴스로 분할	- 하나의 데이터베이스 인스턴스에 데이터(테이

	하는 기법	블)를 분할하는 기법

나. 샤딩과 파티셔닝 상세 차이점

구분	샤딩	파티셔닝
분할 방식	- 수평 분할	- 수평 분할 / 수직 분할
관리	- Master Node 관리	- 별도 Master node 없음
분할 데이터 저장위치	- 별도 서버로 분리 저장	- 동일서버에 저장
키	- Shared Key 저장	- 별도 Key 없음
증설	- Scale out 통한 DB 증설	- Scale up을 통한 DB 증설
조인	- Join 연산 사용할 수 없음	- Join 연산 사용 가능

- 샤딩과 파티셔닝의 가장 큰 차이점은 분할된 데이터의 저장 공간 위치임.

IV. 샤딩 적용 시 고려사항

구분	가이드라인	주요 내용
DB 설계 가이드라인	데이터 재분배	서비스 정지 없이 scale-up 할 수 있어야 함
	조인	Sharding-DB 간에 조인이 불가능 하기에 처음부터 역정규화도 고려해야 함
	파티션	샤드 해쉬 함수 설계가 중요
	데이터는 작게	Table의 단위를 가능한 작게 만들어야 함
응용 설계 가이드라인	트랜잭션	Global Transaction을 사용하면 shard DB간의 트랜잭션도 가능
	Global Unique Key	DBMS에서 제공하는 auto-increment를 사용하면 key가 중복될 수 있기 때문에, 어플리케이션 레벨에서 GUID를 생성해야 함

"끝"

04	데이터산업법		
문제	최근 데이터 산업 발전을 위하여 "데이터 산업진흥 및 이용에 관한 촉진법"(약칭:데이터산업법)을 제정하였다. 이 법의 목적 및 주요 내용과 기대효과에 대하여 설명하시오.		
도메인	데이터베이스	난이도	상 (상/중/하)
키워드	데이터산업법, 데이터3법, 개인정보보호법, 데이터거래소, 데이터 댐, 디지털 뉴딜		
출제배경	'데이터 산업진흥 및 이용촉진에 관한 기본법'(이하 '데이터 기본법') 의결에 대한 문제 출제 예상		
참고문헌	ITPE Final Round 데이터 경제를 활짝 여는 '데이터 기본법' 제정 _ 과기정통부 2021.10.12(화) 보도자료		
해설자	정상반 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 데이터 산업의 육성, 데이터산업법의 개요 및 목적

가. 데이터 산업법의 개념

- 4차 산업혁명의 핵심인 데이터경제 전환에 적극 대응하고, 데이터의 생산, 유통, 활용을 촉진하기 위한 법제
- 데이터 산업발전 기반 조성 및 데이터 경제 활성화를 위한 **'데이터 산업진흥 및 이용촉진에 관한 기본법'**

나. 데이터 산업법의 목적

- 데이터의 생산, 거래 및 활용 촉진에 관하여 필요한 사항을 정함으로써 데이터로부터 경제적 가치를 창출하고 데이터산업 발전의 기반을 조성하여 국민생활의 향상과 국민경제의 발전에 이바지함을 목적으로 함
- 데이터 산업진흥 및 이용촉진에 관한 기본법, 제1장제1조(목적)

II. . 데이터산업법의 주요 내용

가. 데이터산업법의 주요 내용

구분	주요내용	설명
산업 발전 관점	국가 전체의 데이터 컨트롤 타워 확립	- 국가 데이터 정책위원회 신설 - 신속한 의사 결정과 투자 기여
	데이터 전문기업 체계적 육성	- 데이터 거래·분석제공 사업자 신고제 도입 - 데이터 산업기반 조성 기여
데이터 거래 관점	데이터 거래사 양성	- 안전한 데이터 거래를 지원할 '데이터 거래사' 양성 - 데이터 거래에 관한 상담·중개·알선 등 수행
	데이터 자산가치와 권리가 보장되는 시장 조성	- 데이터 가치평가·자산보호·분쟁보호 위원회 등 도입 - 데이터의 정당한 가치 평가 및 무단 취득·사용·공개 방지

나. 데이터산업법의 상세 내용

구분	법조항	설명

1. 목적/정의 규정	제1조, 2조	- 법의 목적을 데이터로부터 경제적 가치를 창출하고 데이터 산업 발전의 기반을 조성하여 국민 생활의 향상과 국가 경제 발전에 이바지하는 것으로 규정하고, 데이터 등 관련 용 어 정의
2. 데이터 산업 진흥 기본계획 수립	제4조	- 정부는 데이터 생산, 거래 및 활용을 촉진하고 데이터산업의 기반을 조성하기 위하여 3 년마다 데이터 산업 진흥 기본계획을 수립
3. 국가 데이터 정책위원회	제6조	- 공공·민간 데이터 정책을 총괄하는 기구를 설치(국무총리 위원장)하고, △ 기본계획 수립, △데이터 생산, 거래 및 활용 관련 정책·제도개선 사항, △ 데이터 산업 진흥관련 계획 총 괄·조정 심의
4. 데이터 자산 보호	제12조	- 인적 물적으로 상당한 투자와 노력으로 생성한 경제적 가치를 지니는 데이터('데이터 자산')를 보호 ※ 무단으로 취득·사용·공개, 타인에게 제공하는 행위, 정당한 권한 없이 데이터자산에 적용한 기술적 보호조치 제거 등 금지
5. 데이터 가치평가 지원 품질 관리	제14조, 20조	- 데이터 가치평가 기법 및 가치평가 체계, 품질인증 대상 및 품질인증 기준 등의 마련과 관련 업무를 전담할 가치평가 기관과 품질인증 기관 등 지정 추진
6. 데이터 사업자 신고	제16조	- 데이터 거래사업자, 데이터 분석제공 사업자 등은 과기정통 부에 신고하여야 하며 과기정통부 및 관계 중앙행정기관은 신고한 사업자에 대하여 필요한 재정적·기술적 지원 등을 할 수 있음
7. 데이터거래사 양성지원	제23조	- 데이터 거래에 관한 전문지식이 있는 사람은 과기정통부 장 관에 데이터 거래사로 등록할 수 있으며, 과기정통부는 데이 터 거래사에게 데이터 거래업무의 수행에 필요한 정보제공 및 교육을 제공
8. 창업지원, 중소기업자 특별지원	제24조, 31조	- 데이터 기반 산업 활성화 및 기업의 데이터 관련 역량 강 화, 사업화 등 지원, 데이터 각종 지원시책 시행 시 중소기업 자 우선 고려 및 데이터 거래·가공 등 필요 비용 일부 지 원
9. 전문인력 양성	제25조	- 과기정통부 장관 및 행정안전부 장관은 데이터 전문인력 양 성을 위한 시책 마련, 과기정통부 장관은 전문인력 양성기관 지정 및 지원
10. 데이터분쟁 조정위원회 설치	제34조	- 데이터의 생산, 거래 및 활용에 관한 분쟁을 조정하기 위한 데이터분쟁조정위원회 설치

- 데이터발전법을 통해서 법적, 제도적 지원을 통한 데이터 산업 발전에 기대

III. 데이터산업법의 기대효과

가. 데이터 기본법의 정책, 산업측면 기대 효과

구분	기대효과	설명
정책측면	예측성과 신뢰성 향상	- 국민과 기업의 거버넌스, 정책 수립 시 예측 가능하고 신뢰할 수 있는 전략 수립에 기여

	신속한 의사결정, 투자 기여	- 국가적인 측면에서의 정책, 방향성에 대한 의사결정 기여 및 기업 투자 활성화에 기여
산업 활성화 측면	체계적인 다양한 사업자 육성	- 데이터 거래, 분석제공 사업자 신고제 도입으로 개별 사업자의 상황에 따른 종합적인 지원 육성 가능
	데이터 산업기반 조성 기여	- 데이터 관련 분야의 창업, 중소기업에 대해 역량강화, 컨설팅과 사업화 등을 지원으로 산업 활성화

- 정책, 산업 활성화 측면 외 제도, 시장측면에서의 기대 효과 존재

나. 데이터 기본법의 제도, 시장형성 측면 기대 효과

구분	기대효과	설명
제도측면	데이터 관련한 신규 일자리 창출	- 전문지식을 바탕으로 한 '데이터 거래사' 양성으로 데이터 산업 생태계의 새로운 일자리 창출 기대
	전문지식 함유한 인재 육성	- '데이터 거래사 등록제' 운영으로 직간접적으로 교육등의 필요한 자원 제공으로 인재 지속적 양성 기대
시장형성 측면	정당한 권리 보호, 공정시장 환경 조성	- 데이터 가치평가, 자산보호, 분쟁조정 위원회등을 도입하여 지속적으로 데이터 산업 시장 환경 조성
	데이터에 대한 시장에서의 가치 확보	- 무분별한 데이터 수집, 이용등을 방지, 데이터 자체의 시장에서 정당한 가치 평가 기대

- 데이터산업법 제정과 더불어 같이 시행될 산업디지털법은 데이터 생산, 활용을 촉진하고 데이터산업의 진흥을 목표로 한다는 점에서는 유사하지만 세부사항에서 차이 발생

IV. 데이터산업법과 산업디지털법 비교

구분	데이터산업법	산업디지털법
데이터 개념 (데이터, 산업데이터)	- 다양한 부가가치 창출을 위해 광 또는 전자적 방식으로 처리될 수 있는 자료 또는 정보	- 제품 또는 서비스의 개발·생산·유통·소비 등 활동과정에서 생성 또는 활용되는 것으로써 광 또는 전자적 방식으로 처리될 수 있는 모든 종류의 자료 또는 정보
정책추진체계	- 총리 소속 국가데이터정책위원회 (간사 과기정통부, 행정안전부)	- 산업부 소속 산업디지털전환위원회
데이터의 법적보호	- 데이터생산자의 데이터 자산에 대한 부정 사용 금지	- 산업데이터를 생성한 자는 해당 산업데이터를 활용해 사용·수익할 권리
신고의무	- 데이터거래사업자, 데이터분석제공사업자 신고	- 산업 디지털 전환 지원 전문회사 신고
특유사항	- 데이터 안심구역, 데이터 가치 평가, 데이터 거래사	- 디지털 전환 선도사업 규제 개선

"끝"

05	순차 다이어그램		
문제	UML 2.0의 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		
도메인	소프트웨어공학	난이도	상 (상/중/하)
키워드	시간 순서, 유즈케이스, 모델링, 속성, 상호 작용		
출제배경	상호 작용 분석 및 유즈케이스 표현을 위해 활용 되고 있는 순차 다이어그램 관련 지식 점검		
참고문헌	ITPE 기술사회 서브노트		
해설자	서경석 기술사(제119회 정보관리기술사 / akslemf@naver.com)		

I. 시간의 흐름에 따라 표현하는 순차 다이어그램의 개요

가. 순차 다이어그램의 정의

- 객체를 정의하고 한 Usecase내에 포함된 객체 간의 상호작용을 시간 순서로 표현하는 동적 다이어그램

나. 순차 다이어그램의 특징

특징	설명
시간순서	- Use Case 시나리오를 시간과 순서에 따라 묘사 및 도식화
관계성 제외	- 객체들 간의 관계성은 표현하지 않음
명시성	- 복잡한 시나리오나 실시간 명세 표현, 메시지의 명시적인 순서를 나타내기에 효과적

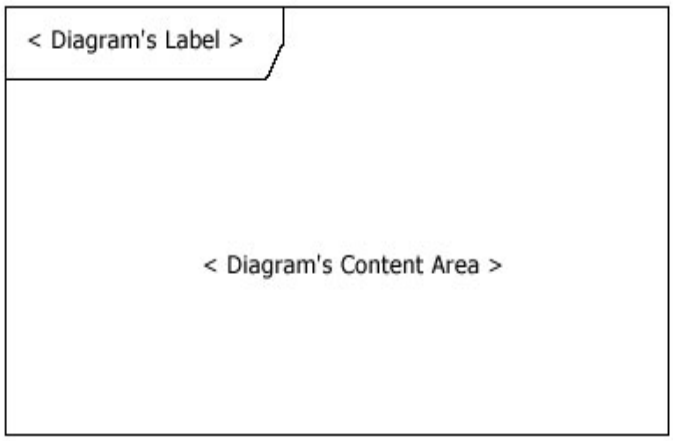
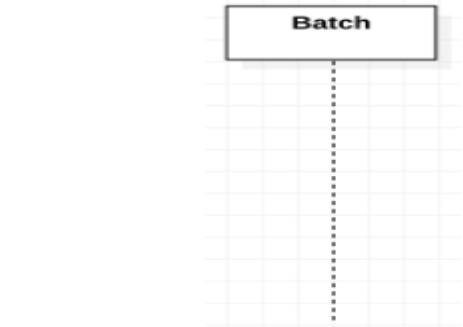
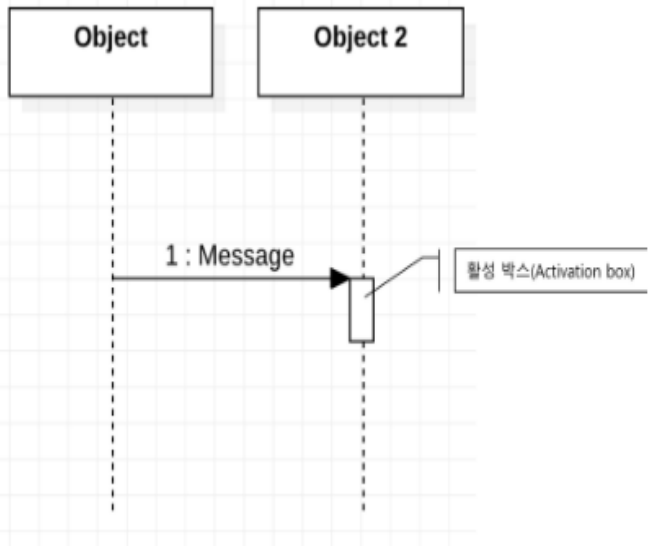
II. 순차 다이어그램의 목적과 작성순서, 구성 요소별 표기법

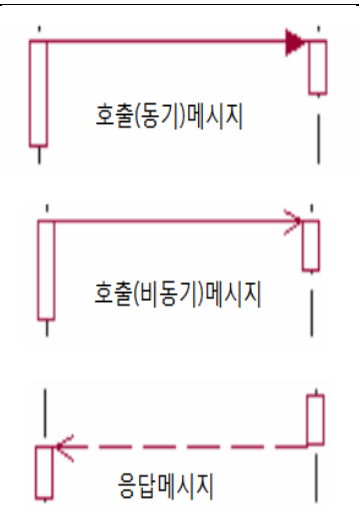
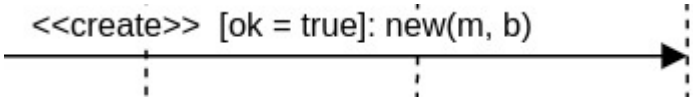
가. 순차 다이어그램의 목적과 작성순서

구분		설명
목적	- 모델링	- 객체간 동적 상호 작용을 시간적 개념을 중점으로 표현
	- 속성 정의	- 객체들이 가져야 하는 오퍼레이션과 속성을 정의
	- 유즈케이스 상세화	- 유즈케이스에 필요한 객체가 등장, 객체간 메시지 표현
	- 상호작용 확인	- 유즈케이스 상세화를 통한 이벤트 간 상호 작용 시각화
	- 프로그래밍 사양 정의	- 일부 케이스 도구 순차 다이어그램 기반 프로그램 생성 지원
작성 순서	- 대상 선정	- 유즈케이스 다이어그램을 이용하여 유즈케이스 정의서 분석
	- 액터 파악	- 유즈케이스 액터 파악 및 순차 다이어그램에 위치
	- 객체 선정	- 유즈케이스 실현을 위해 객체 지정 및 순차 다이어그램 위치
	- 메시지 정의	- 유즈케이스 실현 위해 필요한 객체간 메시지 정의
	- 추가 정의	- 처리를 위해 필요하지만 정의 되지 않은 객체 추가 정의

- 유즈케이스 다이어그램 활용 통한 유즈케이스 분석 후 시간에 맞춰 순차 다이어그램 작성 진행

나. 순차 다이어그램의 구성 요소별 표기법

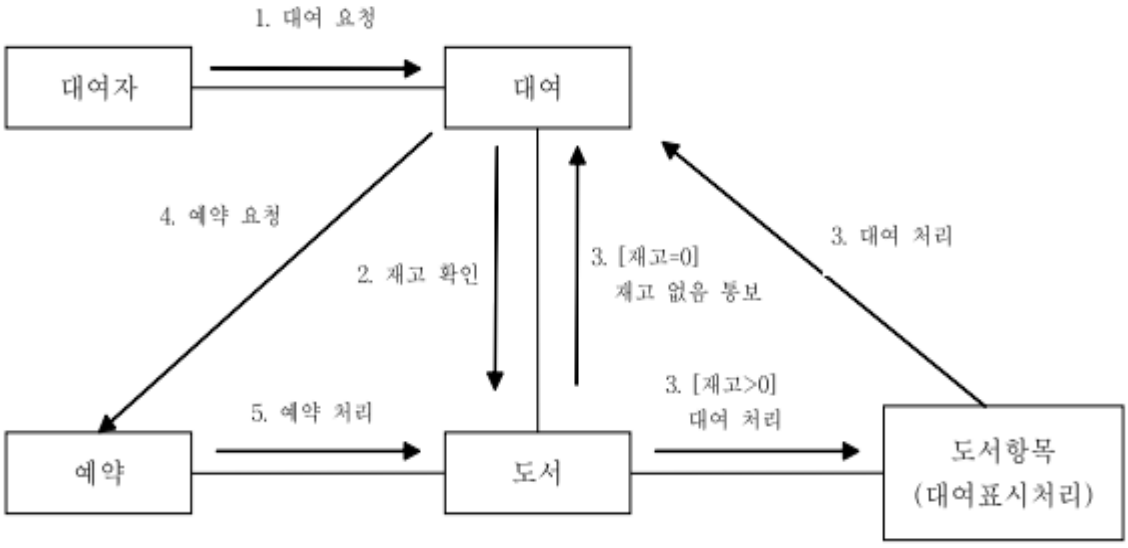
구분	표기법	설명
Frame		- 프레임 엘리먼트는 다이어그램의 레이블을 위한 지정된 장소를 제공하고, 다이어그램의 그래픽 영역을 제공 - 다이어그램의 레이블은 프레임의 "네임박스(namebox)"라고 부르게 될 왼쪽 코너의 상단 위치
Object		- 가장 윗부분에 표현, 왼쪽에서 오른쪽으로 객체들을 나열
Lifelines		- 모델링 되는 시퀀스에 개입된 역할 또는 개별 인스턴스
Activation Box		- 객체 라이프라인 상단 표현 박스 - 객체의 호출 용도 - 객체의 특정 메소드 실행 또는 정보처리가 실행 되고 있거나 다른 객체의 메소드가 종료되기를 기다리는 것을 표시

Messages		- 서로 다른 객체 간 상호 작용 혹은 의사 소통 통신 정의 요소 - 하나의 객체 라이프라인으로부터 다른 객체 라이프라인까지 선+화살표로 표시
Guard		- 단일 메시지에 대해서 조건을 명시 하기 위한 표기법 - 메시지의 Text의 앞쪽에 []로 감싼 후 조건을 명시 - 표기법 사례는 ok = true일 때 수행

- Frame 좌측 상단 Name box에 레이블 입력 후 Object, Lifeline, Activation box, Message, Guard 표기

III. 도서예약시스템의 협력 다이어그램을 순차 다이어그램으로 변환

가. 도서예약시스템 협력 다이어그램 분석

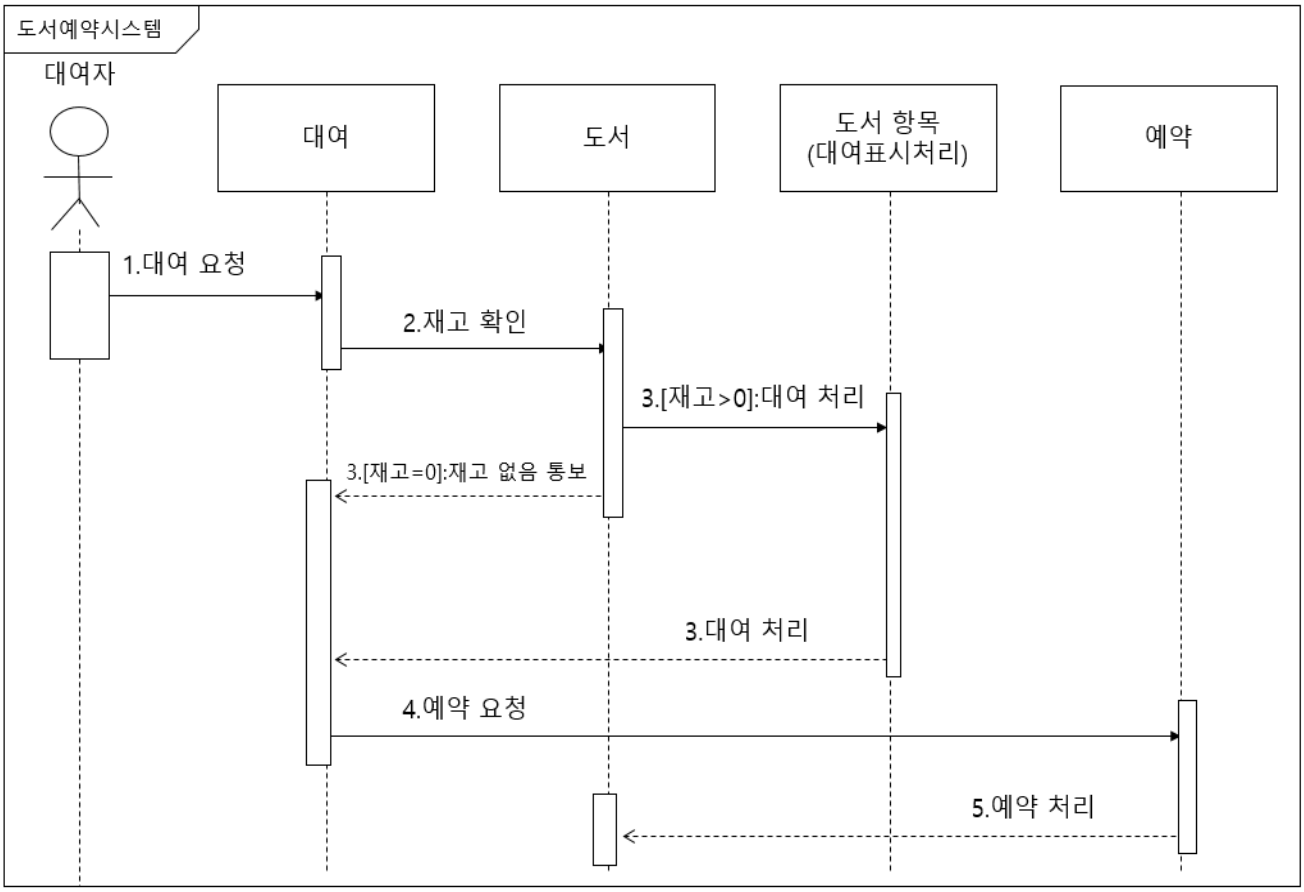
구분	세부	설명
협력 다이어그램		
분석	- 유즈케이스 분석	1. 대여 요청, 2. 재고 확인 3-1. [재고=0] 재고 없음 통보 3-1-1. 예약 요청 시 예약 처리 3-2. [재고>0] 대여표시처리 3-2-1. 대여 처리

	- 액터 파악	- 대여자
	- 객체 선정	- 대여, 예약, 도서, 도서항목
	- 메시지 정의	- 대여 요청, 재고 확인, 재고 없음, 대여 처리, 예약 요청, 예약 처리
	- 추가 정의	- 주어진 조건에 대한 분석 결과 추가 정의는 불필요

- 순차 다이어그램 작성 순서에 맞춰 협력 다이어그램 분석 후 변환 진행

나. 도서예약시스템 순차 다이어그램 변환

순차 다이어그램

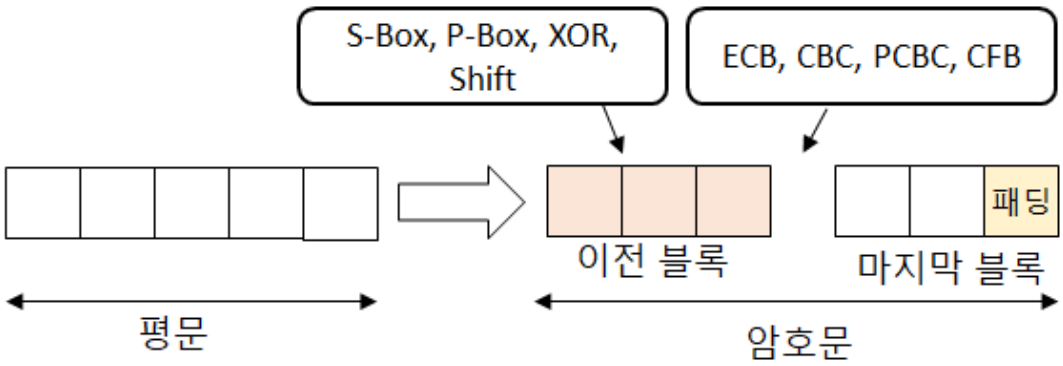


- 도서예약시스템 구성 시 기본적으로 모든 응답은 동기식으로 처리하도록 구성
- 재고 확인, 예약 요청 부분에 동기식 처리 후 즉시 응답 메시지 전송
- 순차 다이어그램 작성 순서에 맞춰 협력 다이어그램 분석 수행
- 유즈케이스 대여, 재고확인, 재고없음통보, 대여처리, 예약요청, 예약처리에 대해 순차 다이어그램 작성

"끝"

06	블록 암호 모드		
문제	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		
도메인	보안	난이도	중 (상/중/하)
키워드	ECB, CBC, CFB, OFB		
출제배경	대칭키 기반 암호화 방식 모드에 대한 기본 지식 점검		
참고문헌	ITPE 기술사회 서브노트		
해설자	서경석 기술사(제119회 정보관리기술사 / akslemf@naver.com)		

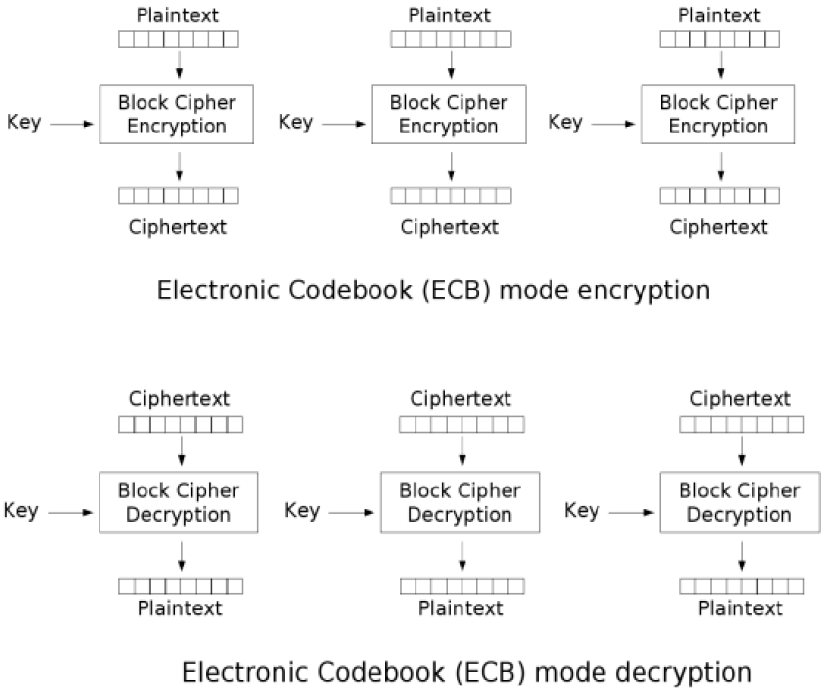
I. 고정 크기의 블록단위 암호화, 블록 암호화의 개념



개념	평문을 고정 길이의 블록단위로 나누어 각 블록마다 암호화를 수행하여 고정된 크기의 블록 단위 암호문을 생성하는 암호화 기술	
특징	- 고정길이	- N-bit 평문 블록을 N-bit 암호화 블록으로 변환하는 기법
	- 암호화구조	- SPN, Feistel 구조 등 S-Box, P-Box, XOR, 시프트를 활용해 암호화
	- 운용모드	- 초기 벡터, 패딩, 시프트, 순환 기능을 선택적으로 이용하는 운영 방식

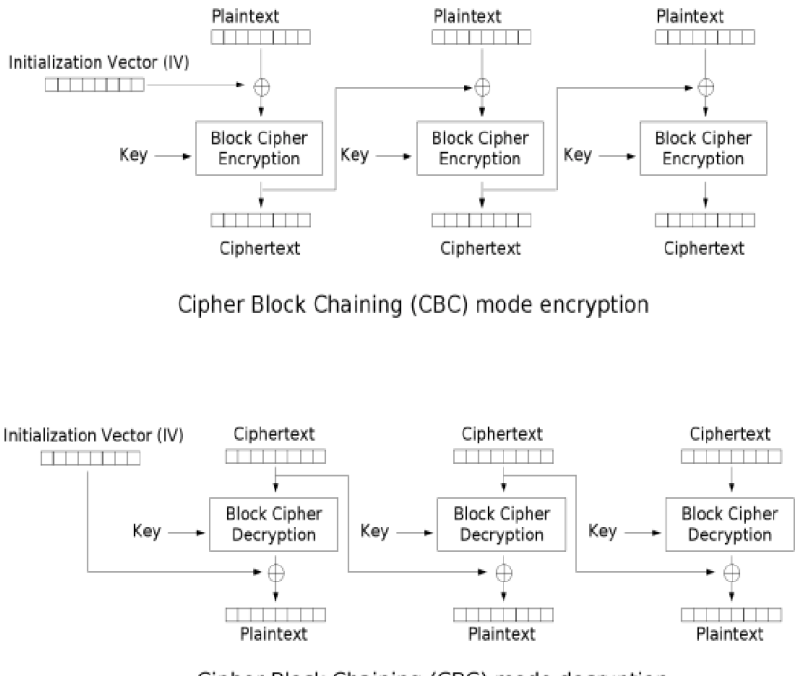
II. 블록암호화만 사용하는 운영 모드

가. ECB(Electronic Code Book) 운영 모드

운영모드	구조	설명
ECB (Electronic Code Book)		- 평문/암호문 블록 1:1 관계 가진 기본적인 블록암호화 모드 - 가장 간단한 처리, 고속/병렬처리 가능, 기밀성 다른 운영모드에 비해 가장 낮음

- 암복호화의 병렬 처리가 가능하며 가장 단순한 운영 모드

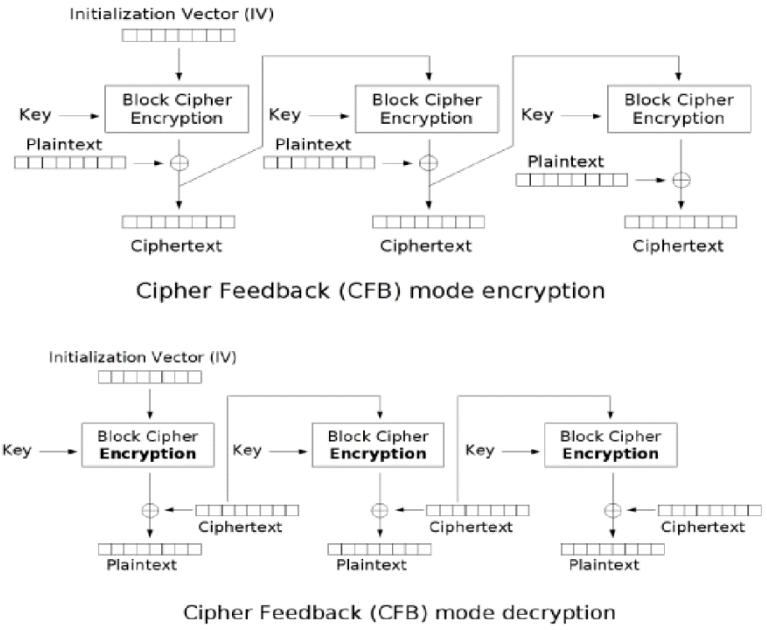
나. CBC(Cipher Block Chaining) 운영 모드

운영모드	구조	설명
CBC (Cipher Block Chaining)		- 맨 첫 블록은 Initialization Vector 를 통해 XOR 처리하여 암호화, 두 번째블록 은 이전 암호화 결과를 XOR 처리 암호화

- 복호화만 병렬 처리가 가능하며 Brute force attack 공격에 대응을 위해 개선된 운영 모드

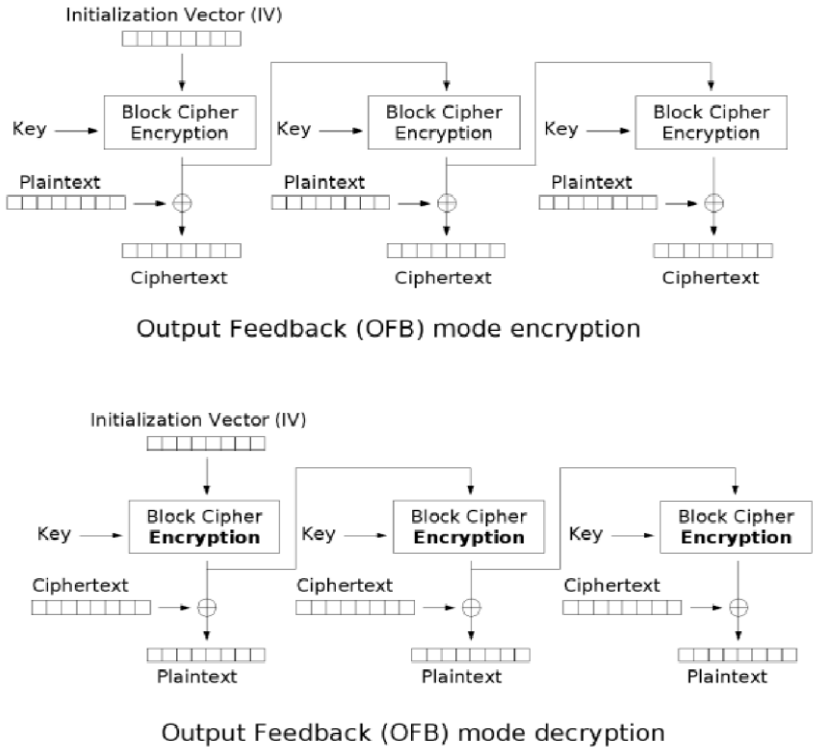
III. 자기 동기 스트림(self-synchronizing Stream) 암호화와 결합한 운영모드

가. CFB(Cipher FeedBack) 운영 모드

운영모드	구조	설명
CFB (Cipher Feedback)		- 데이터를 암호화하는 것이 아니라 IV를 암호화로, 블록 암호를 자기 동기 스트림 암호로 변환하는 방식 - 암호화에서 병렬 처리 불가능

- 복호화에 대한 병렬 처리만 가능하며 Initialization Vector를 활용하여 암호화 진행

나. OFB(Output FeedBack) 운영 모드

운영모드	구조	설명
OFB (Output Feedback)		- IV를 암호화하여 그 Key Stream을 생성해 두어 XOR 처리만 나중에 수행하여 성능을 향상시키는 암호화 운영모드 - 암/복호화가 같은 구조

- 병렬 처리가 불가능하며 복잡도가 높아졌으나 일부 성능이 향상된 운영 모드

IV. 블록 암호화 운영방식별 특징 비교

운영방식	암·복호화 처리	병렬처리	시간성능	복잡도	특징
ECB	암호화 복호화	가능 (암·복호화)	상	하	- 기본 방식 제공
CBC	암호화 복호화	가능 (복호화만)	하	중	- 패턴분석 회피 - Brute Force Attack 개선
PCBC	암호화 복호화	불가능	하	상	- CBC의 Brute Force Attack 추가개선
CFB	암호화 암호화	가능 (복호화만)	하	중	- CBC에서 IV 암호화 - 성능 소폭 개선
OFB	암호화 암호화	불가능	중	상	- CFB에서 IV 암호화 - 성능 소폭 개선
CTR	암호화 암호화	가능 (암·복호화)	중	상	- 병렬처리 개선 - IV 복잡도 증가

"끝"

ITPE 기술사회
제127회 정보관리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2022년 04월 16일
집 필 강정배PE, 안응원PE, 서경석PE, 이상헌PE
출 판 **ITPE(Information Technology Professional Engineer)**
주 소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층
ITPE 선릉점 서울시 강남구 선릉로 86길 15 3층 IT교육센터 아이티피이
ITPE 강남점 서울시 강남구 테헤란로 52길 21 파라다이스벤처타워 3층 303호
ITPE 영등포점 서울시 영등포구 당산동2가 하나비즈타워 7층 ITPE
연락처 070-4077-1267 / itpe@itpe.co.kr