신 입 직 원 (종합기획직원 G5) 채 용 고 시 (2018. 10. 20. (토) 시행)

학 술 (컴퓨터공학)

< 유의사항 >

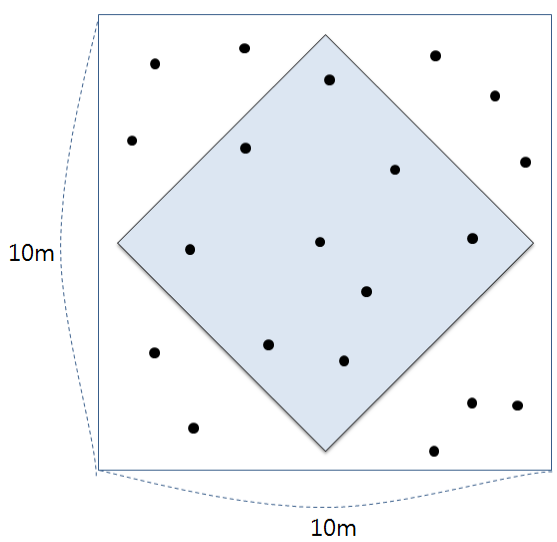
1. 수험번호 및 성명은 **매 페이지마다 기재**하시기 바랍니다.
2. 문제지(또는 답안지)를 낱장으로 뜯어서 사용하는 경우에도 최종 제출시 **페이지 번호 순으로 정렬**되었는지 확인하시기 바랍니다.
3. 필요시 답안을 영어로 작성할 수 있습니다.

Ⅰ. 다음 물음에 답하시오.

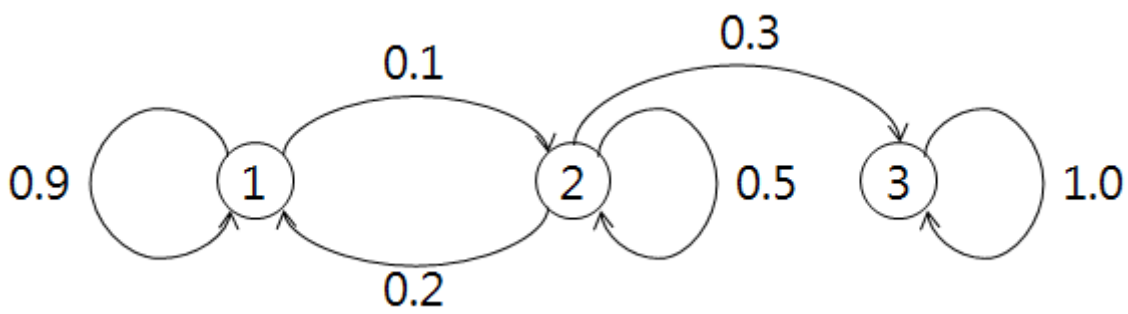
□ 머신러닝(machine learning)과 관련하여 다음 물음에 답하시오.

가. 지도 학습(supervised learning)과 비지도 학습(unsupervised learning)을 간략히 설명하시오.

나. 몬테카를로 시뮬레이션(Monte-Carlo simulation)은 불확실한 상황 하에서 의사결정을 위해 확률적 시스템을 이용한 모의실험을 말한다. 다음 시뮬레이션 결과를 바탕으로 마름모의 넓이를 구하시오.



다. 아래의 마르코프 체인(Markov chain) 전이 다이어그램(transition diagram)을 참고하여 다음 물음에 답하시오.

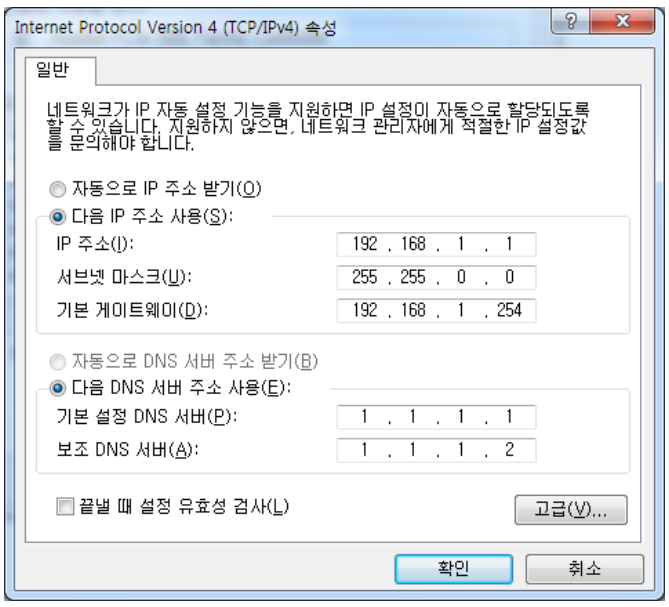


① 문제에서 제시한 전이 다이어그램에 대한 전이 행렬(transition matrix) P를 구하시오.

② 현재 상태가 '2'일 때 두 번 전이한 상태가 '1'일 확률을 문제 '①'에서 구한 전이 행렬을 이용하여 구하시오.

□ 컴퓨터 네트워크와 관련하여 다음 물음에 답하시오.

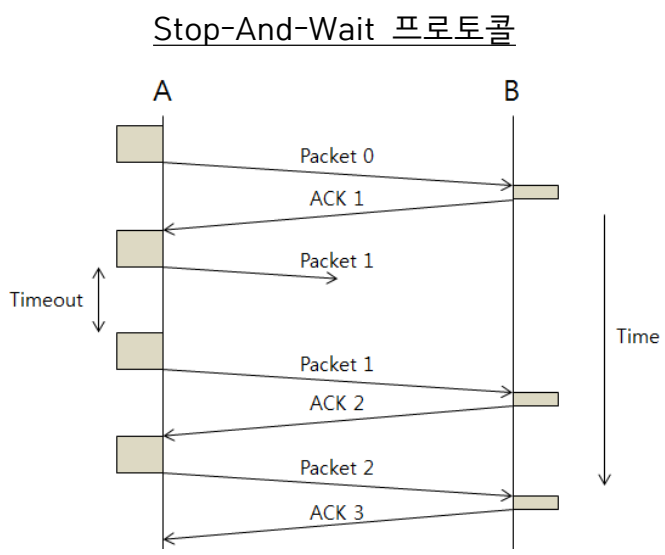
가. 다음 그림은 A과장의 네트워크 설정이다. 각 설정이 의미하는 바를 간략히 서술하시오.



- IP 주소 :
- 서브넷 마스크 :
- 기본 게이트웨이 :
- 기본 설정 DNS 서버 :
- 보조 DNS 서버 :

나. DNS의 기능을 2가지 이상 서술하시오.

다. 전송계층(transport layer)에서 데이터 전송 보장(reliable data transfer)을 위해 다양한 방식의 프로토콜을 사용하고 있다. 그 중 Stop-And-Wait 프로토콜이 가지고 있는 주요 문제점을 간략히 서술하고, 이를 보완한 Go-Back-N(GBN) 프로토콜, Selective Repeat(SR) 프로토콜을 설명하시오.



라. 라우팅 프로토콜(routing protocol) 중 Link-State(LS) 알고리즘과 Distance-Vector(DV) 알고리즘을 간략히 설명하시오.

Ⅱ. 다음 물음에 답하시오.

□ 데이터베이스와 관련하여 다음의 물음에 답하시오.

가. 이벤트참여 관계(relation)와 함수 종속성이 다음과 같이 제시되어 있고 현재 제 1 정규화까지 수행된 상태이다. 이와 관련하여 다음 물음에 답하시오.

회원아이디	회원이름	이벤트번호	당첨여부	회원등급	포인트적립률
101	Smith	A100	Y	VIP	7%
101	Smith	A200	N	VIP	7%
102	John	B100	Y	GOLD	3%
103	Emily	C100	Y	VVIP	10%
103	Emily	C200	N	VVIP	10%

함수 종속성(functional dependency)

- {회원아이디, 이벤트번호} → 당첨여부
- 회원아이디 → 회원이름
- 회원아이디 → 회원등급
- 회원등급 → 포인트적립률

① 제 1 정규화의 특징을 서술하시오.

② 이벤트참여 관계의 주키(primary key)를 기술하시오.

③ 이벤트참여 관계의 함수 종속도(functional dependency diagram)를 그리시오.

④ 이벤트참여 관계에서 부분함수 종속성을 제거하는 제 2 정규화를 수행하시오.

⑤ 문제'④'의 결과에서 이행함수 종속성을 제거하는 제 3 정규화를 수행하시오.

⑥ 일부 개발프로젝트에서는 데이터베이스 정규화가 가지고 있는 단점으로 인하여 정규화를 하지 않는 경우도 있다. 정규화의 단점을 설명하시오.

나. 아래의 트랜잭션 표기 형식을 참고하여 데이터베이스 트랜잭션(transaction)의 동시성(concurrency)에 대한 다음 물음에 답하시오.

트랜잭션 표기 형식

T_A	T_B

read_item(X);
X := X-N;
 	
(중략)
write_item(X);
commit;
	
	read_item(X);
	
	X := X+M
	write_item(X);
	(중략)
	rollback;

① 갱신손실 문제(lost update problem)에 대해 예시를 들어 설명하시오.

T1	T2

② 임시갱신 문제(temporary update problem 또는 dirty read problem)에 대해 예시를 들어 설명하시오.

T1	T2

□ 프로그래밍 언어와 관련하여 다음 물음에 답하시오.

가. 객체지향언어가 지니는 장점에 대해 간략히 설명하시오.

나. 객체지향언어 중 JAVA는 다중 상속이 불가하고 C++는 다중 상속이 가능하다. 상속(inheritance)에 있어서 단일 상속(single inheritance)과 다중 상속(multiple inheritance)의 차이를 설명하고 다중 상속이 가지는 문제점을 서술하시오.

다. 객체지향언어의 특성인 오버로딩(overloading)과 오버라이딩(overriding)에 대해 간략히 설명하시오.

라. 다음 물음에 답하시오.

① 다음 JAVA 코드의 실행 결과를 작성하시오.

```
class Parent{
        Parent( ){
                System.out.println("Parent 1");
        }
        Parent(String str){
                System.out.println("Parent 2");
        }
}

class Child extends Parent{
        Child( ){
                System.out.println("Child 1");
        }
        Child(String str){
                System.out.println("Child 2");
        }
}

class FamilyTest{
        public static void main(String args[]){
                Child c1 = new Child( );
                Child c2 = new Child("a");
        }
}
```

< 실행결과 >

② 다음 JAVA 코드에서 문제가 있는 부분 두 곳을 지적하고 그 이유를 설명하시오.

```
class Parent{
        Parent( ){ }
}

class Child extends Parent{
        Child( ){ }
        public void init( ){ }
}

class FamilyTest{
        public static void main(String args[]){
                Parent p = null;
                Child c1 = new Child( );
                Child c2 = null;

                p = c1;
                p.init( );
                c2 = p;
        }
}
```

< 문제점 >

③ 재귀호출(recursive call) 방식을 이용하여 x^n을 구하는 함수를 JAVA 코드로 작성하시오.

```
static long power(int x, int n){

}
```

□ 정보보호와 관련하여 다음 물음에 답하시오.

가. 비대칭키 알고리즘의 동작 원리에 대해 간략히 서술하시오.

나. 다음은 RSA 공개키(public key) 알고리즘이다.

1. 2개의 소수 p, q를 선택
2. n, $\phi\{n\}$ 계산. 이때 $n=pq$, $\phi\{n\}=(p-1)\times(q-1)$
3. $\phi\{n\}$과 서로소인 정수 e 선택 (e와 $\phi\{n\}$의 최대공약수는 1)
4. $e\times d$의 값을 $\phi\{n\}$으로 나누었을 때 나머지를 1로 갖는 정수 d값 선택
   $\Rightarrow$ **공개키(public key) [n, e], 개인키(private key) d**
5. 암호화 : $C=M^e \bmod n,\ \text{for } 0<M<n$
6. 복호화 : $M=C^d \bmod n$

위에 나타난 동작 알고리즘과 아래의 조건을 참고하여 다음의 물음에 답하시오.

조건 : $p=3,\ q=5,\ M=2$

① 공개키([n, e])와 개인키(d)를 구하시오. (단, 여러 개의 조합 중 한 가지만 기술)

② 메시지 M을 암호화하여 암호문 C를 구하시오.

③ 문제 '②'에서 도출한 암호문 C를 복호화하는 과정을 보이시오.

다. 무선 통신에 유선 통신 수준의 기밀성을 제공하고자 1997년도에 공개된 WEP(wired equivalent privacy)는 2001년 초부터 그 취약점이 발견되기 시작하였다. 이에 IEEE는 무선 통신에 대한 새로운 인증 및 암호화 방식으로 2003년에 WPA(wired protected access)란 이름의 새로운 무선 통신 프로토콜을 공개하였고 이후 WPA가 확장된 형태인 WPA2까지 공개하였다. 이런 배경을 참고하여 보안에 있어서 WEP가 취약한 이유를 서술하시오. (WPA, WPA2와 비교 서술하여도 무방)

라. 네트워크 암호화 방식 중 IPSec방식과 SSL(secure socket layer)/TLS(transport layer security) 방식에 대해 간략하게 비교 서술하시오.

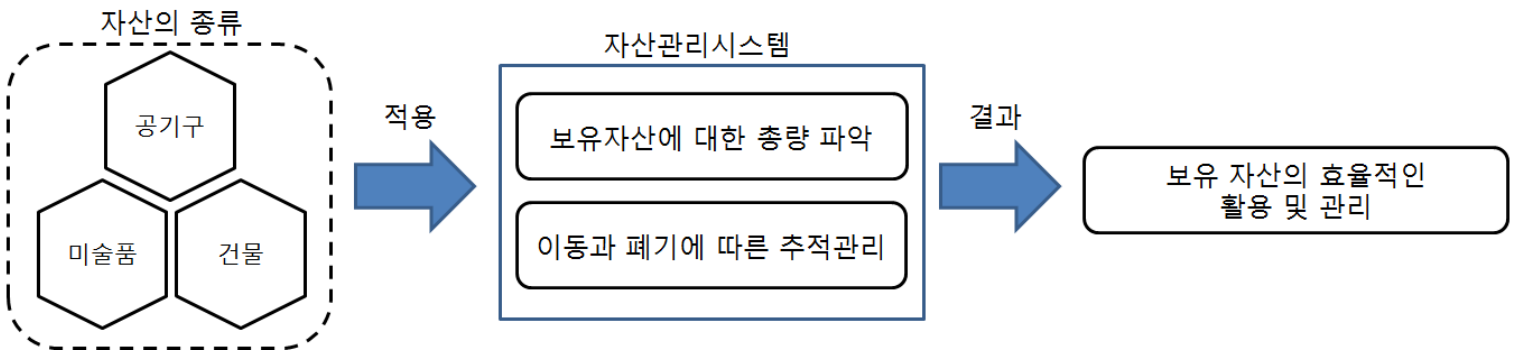
Ⅲ. 다음에 대하여 논술하시오.

< 유의사항 >

1. 답안은 한 페이지 이내로 작성하시기 바랍니다.
2. 내용상 옳은 서술이라 하더라도 문제에서 요구하는 주제와 거리가 먼 경우에는 점수를 얻을 수 없습니다.
3. 필요시 답안을 영어로 작성할 수 있습니다.

가상화폐인 비트코인의 핵심 기술인 블록체인은 전 세계적으로 금융을 포함한 공공, 의료 등 여러 분야에서 활용되고 있다. 이러한 흐름에 따라 A국 중앙은행에서도 블록체인 기술을 이용하여 자산관리시스템을 개발하는 프로젝트를 검토하고 있다. 이 블록체인 기반의 자산관리시스템이 완성되면 A국 중앙은행이 보유한 미술품, 차량, 건물 등과 같은 자산의 정보가 블록체인에 기록되어 지금과는 다른 데이터 관리 형태를 보일 것이라 예측된다. 블록체인이 가지고 있는 장점으로 인하여 시스템의 데이터 변조가 어렵고 탈중앙화가 가능할 것이라는 찬성측 의견과 기존 방식의 데이터베이스 이용이 블록체인 도입보다 더 나을 것이라는 반대측 의견도 있다. 관련 부서에서는 블록체인 기술의 장단점에 대하여 면밀히 검토한 다음 자산관리시스템에 블록체인의 적용여부를 결정하기로 하였다.

<그림> 자산관리시스템 개요



A국 중앙은행 자산관리시스템을 **블록체인 기반으로 개발하는 방안**과 **기존 데이터베이스를 이용하여 개발하는 방안**의 장단점을 분석하고 최적의 시스템 개발방안이 무엇인지 논하시오.

<답안>