2014-계리직-컴퓨터일반-A형-해설-곽후근

1. 〈보기〉는 네트워크 토폴로지(topology)에 대한 설명이다. ㉠~㉢에 들어갈 내용을 옳게 나열한 것은?

〈보기〉
- FDDI는 광케이블로 구성되며 (㉠) 토폴로지를 사용한다.
- 허브 장비가 필요한 (㉡) 토폴로지는 네트워크 관리가 용이하다.
- 터미네이터가 필요한 (㉢) 토폴로지는 전송회선이 단절되면 전체 네트워크가 중단된다.

	㉠	㉡	㉢
①	링형	버스형	트리형
②	링형	트리형	버스형
③	버스형	링형	트리형
④	버스형	트리형	링형

정답 체크 :

(2)

(ㄱ) 링형

FDDI는 전송매체가 광케이블이고, 전송속도가 100Mbps이다.

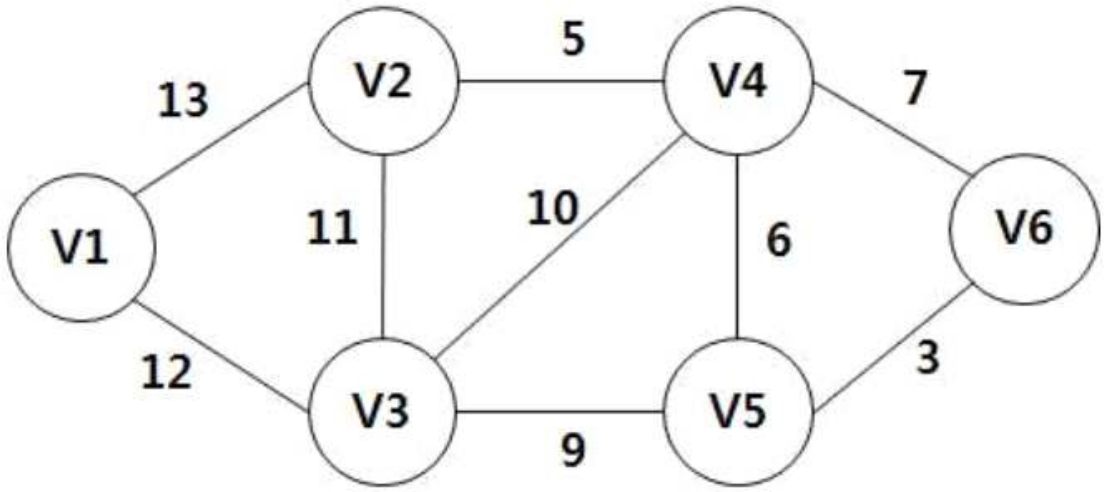
(ㄴ) 트리형

트리형은 허브(Hub)가 필요하다. 트리형의 장점은 장점으로는 제어가 간단하여, 관리 및 확장이 용이(설치와 재구성)하다. 단점으로는 중앙 허브에 병목 현상이 발생하고 중앙 허브의 고장은 네트워크 전체가 마비된다.

(ㄷ) 버스형

버스형은 터미네이터가 필요하다. 버스형의 장점은 설치가 쉽고, 그물형, 성형, 트리형 접속형태보다 적은 양의 케이블 사용한다. 단점은 재구성과 결함 분리가 어렵고 버스 케이블 결함이나 파손은 모든 전송을 중단하게 한다. 그리고 네트워크의 트래픽이 많을 경우 네트워크의 효율성이 떨어진다.

2. 다음 그래프를 대상으로 Kruskal 알고리즘을 이용한 최소 비용 신장 트리 구성을 한다고 할 때, 이 트리에 포함된 간선 중에서 다섯 번째로 선택된 간선의 비용으로 옳은 것은?



① 9
② 10
③ 11
④ 12
정답 체크 :
(4)
Kruskal은 그래프의 간선들을 가중치의 오름차순으로 정렬하고, 정렬된 간선 중에서 사이클을 형성하지 않는 간선을 현재의 간선 집합에 추가 하는 것이다. 만약 사이클을 형성하면 그 간선은 제외한다.
가중치가 가장 작은 3을 선택한다. (첫 번째 간선)
그 다음으로 가중치가 작은 5를 선택한다. (두 번째 간선)
그 다음으로 가중치가 작은 6을 선택한다. (세 번째 간선)
그 다음으로 가중치가 작은 7을 선택한다. 그러나 사이클이 형성되므로 해당 간선은 제외한다.
그 다음으로 가중치가 작은 9를 선택한다. (네 번째 간선)
그 다음으로 가중치가 작은 10을 선택한다. 그러나 사이클이 형성되므로 해당 간선은 제외한다.
그 다음으로 가중치가 작은 11을 선택한다. 그러나 사이클이 형성되므로 해당 간선은 제외한다.
그 다음으로 가중치가 작은 12를 선택한다. (다섯 번째 간선)

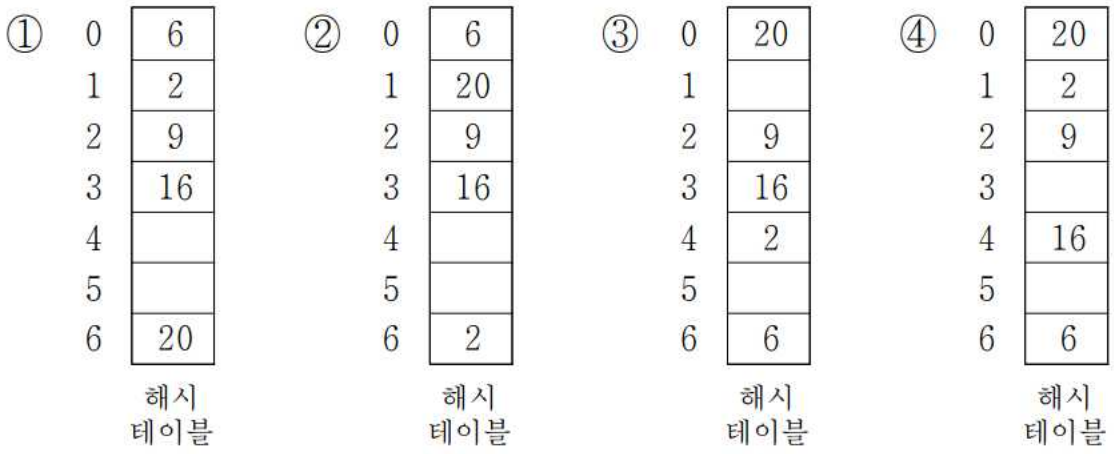
3. 다음 저장장치 중 접근속도가 빠른 것부터 순서대로 나열한 것은?

ㄱ. 레지스터 ㄴ. 주기억장치 ㄷ. 캐시메모리 ㄹ. 하드디스크

① ㄱ, ㄷ, ㄴ, ㄹ
② ㄱ, ㄷ, ㄹ, ㄴ
③ ㄷ, ㄱ, ㄴ, ㄹ
④ ㄷ, ㄱ, ㄹ, ㄴ
정답 체크 :
(1)
저장장치 중 접근속도가 빠른 것부터 순서대로 나열하면 다음과 같다.
레지스터 〉 캐시메모리 〉 주기억장치 〉 하드디스크
ㄱ. 레지스터 : 플립플롭으로 구성되며, CPU 내에 포함되어 있어 접근속도가 가장 빠르다.
ㄷ. 캐시메모리 : SRAM으로 구성되며, CPU 내에 포함(on-chip cache, L1 cache)되거나 CPU 밖(off-chip cache, L2 cache)에 존재한다. CPU와 주기억장치의 속도차를 개선하는 것이 목적이다.
ㄴ. 주기억장치 : DRAM으로 구성되며, CPU와 보조기억장치(하드디스크)의 속도차를 개선하는 것이 목적이다.
ㄹ. 하드디스크 : 보조기억장치로, 기계식인 HDD와 전자식인 SSD가 존재한다.

4. 다음 〈조건〉에 따라 입력 키 값을 해시(hash) 테이블에 저장 하였을 때 해시 테이블의 내용으로 옳은 것은?

〈조건〉
ㅇ 해시 테이블의 크기는 7이다.
ㅇ 해시 함수는 h(k) = k mod 7이다.(단, k는 입력 키 값이고, mod는 나머지를 구하는 연산자이다)
ㅇ 충돌은 이차 조사법(quadratic probing)으로 처리한다.
ㅇ 키 값의 입력 순서: 9, 16, 2, 6, 20



정답 체크 :
(2)
해시 함수 : h(k) = k mod 7, 해시 테이블에서 키 값(k)을 7로 나눈 나머지 주소에 키 값(k)를 저장한다.
이차 조사법 : 충돌이 발생하면 (h(k)+inc*inc) mod 7로 키 값(k)이 들어갈 위치를 조사한다. inc는 0, 1, 2, 3...으로 증가하므로 조사되는 위치는 h(k), h(k)+1, h(k)+4, h(k)+9, ...이 된다.
9 mod 7 = 2 // 2의 위치에 키 값(9)를 저장한다.
16 mod 7 = 2(충돌 발생), 2 + 1 mod 7 = 3 // 3의 위치에 키 값(16)을 저장한다.
2 mod 7 = 2(충돌 발생), 2 + 1 mod 7 = 3(충돌 발생), 2 + 4 mod 7 = 6 // 6의 위치에 키 값(2)를 저장한다.
6 mod 7 = 6(충돌 발생), 6 + 1 mod 7 = 0 // 0의 위치에 키 값(6)을 저장한다.
20 mod 7 = 6(충돌 발생), 6 + 1 mod 7 = 0(충돌 발생), 6 + 4 mod 7 = 3(충돌 발생), 6 + 9 mod 7 = 1 // 1의 위치에 키 값(20)을 저장한다.

5. 다음 〈조건〉에 따라 페이지 기반 메모리 관리시스템에서 LRU(Least Recently Used) 페이지 교체 알고리즘을 구현하였다. 주어진 참조열의 모든 참조가 끝났을 경우 최종 스택(stack)의 내용으로 옳은 것은?

〈조건〉
ㅇ LRU 구현 시 스택 사용한다.
ㅇ 프로세스에 할당된 페이지 프레임은 4개이다.
ㅇ 메모리 참조열: 1 2 3 4 5 3 4 2 5 4 6 7 2 4

①

스택 top	7
	6
	4
스택 bottom	5

②

스택 top	2
	7
	6
스택 bottom	4

③

스택 top	5
	4
	6
스택 bottom	2

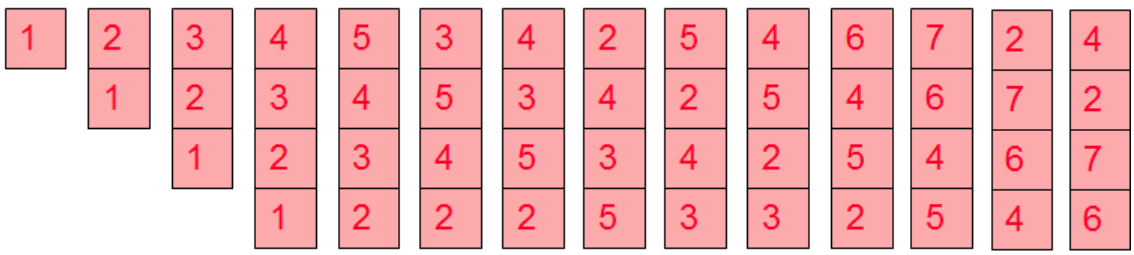
④

스택 top	4
	2
	7
스택 bottom	6

정답 체크 :

(4)

LRU는 프로세스가 가장 최근의 페이지에 액세스했다는 것은 멀지 않아 다시 액세스할 가능성이 있다는 의미이다. 과거 오랫동안 사용하지 않은 페이지로 대치하는 효과로 생각할 수 있다. 페이지를 대치할 때 오랫동안 사용하지 않은 페이지를 선택하므로 시간적으로 거꾸로 찾는 최적 페이지 대치 알고리즘이라고 할 수 있다. 주어진 조건으로 LRU를 적용하면 다음과 같다. 2번째에 2가 들어오면 2가 스택의 최상위로 오고, 기존에 있던 1은 2의 아래에 위치하게 된다. 5번째에 5가 들어왔을 때 페이지 프레임 내에 5가 없기 때문에 교체를 해야 한다. 이때, 스택을 이용하므로 4가 가장 최근에 사용되었고 1이 가장 오랫동안 사용되지 않았다. 그러므로 1이 교체되면서 5가 스택의 최상위에 오게 되고 나머지는 5의 아래에 위치하게 된다. 나머지도 이와 마찬가지 방식으로 동작하고 최종 스택의 내용은 다음 그림과 같이 나타나게 된다.



문 6. 서비스 거부 공격에 해당하는 것을 〈보기〉에서 고른 것은?

〈보기〉

ㄱ. Ping of Death 공격

ㄴ. SYN Flooding 공격

ㄷ. Session Hijacking 공격

ㄹ. ARP Redirect 공격

① ㄱ, ㄴ

② ㄴ, ㄷ

③ ㄷ, ㄹ
④ ㄱ, ㄹ
정답 체크 :
(1)
ㄱ. Ping of Death : 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).
ㄴ. SYN Flooding : 서버에 syn 패킷을 보내고, 서버의 syn+ack에 대한 응답이 ack 패킷을 보내지 않아 서버가 메모리(백로그큐)를 할당한 상태에서 계속 기다린다. 연결이 위한 메모리를 더 이상 사용할 수 없어 서버가 서비스 거부(DoS) 상태가 된다(자원고갈형 DoS 공격).
오답 체크 :
(2), (3), (4)
ㄷ. Session Hijacking : TCP는 클라이언트와 서버간 통신을 할 때 패킷의 연속성을 보장하기 위해 클라이언트와 서버는 각각 시퀀스 넘버를 사용한다. 이 시퀀스 넘버가 잘못되면 이를 바로 잡기 위한 작업을 하는데, 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식이다. DoS(서비스 거부) 공격이 아닌 MITM 공격(중간자 공격)이다.
ㄹ. ARP Redirect : 라우터의 MAC 주소를 알아내어, 공격 대상에게 자신의 MAC 주소가 라우터인 것처럼 속인 후, 브로드캐스트를 주기적으로 하여 패킷을 스니핑하는 공격 방법이다. 2계층 스위칭 환경에서 실시되며, 브로드캐스트를 이용하기 때문에 모든 호스트를 대상으로 한다. DoS(서비스 거부) 공격이 아닌 스니핑 공격이다. 이와 비슷한 ICMP Redirect는 3계층에서 실시된다.

7. 데이지-체인(daisy-chain) 우선순위 인터럽트 방식에 대한 설명으로 옳은 것은?
① 인터럽트를 발생시키는 장치들이 병렬로 연결된다.
② 두 개 이상의 장치에서 동시에 인터럽트가 발생되면 중앙처리장치(CPU)는 이들 인터럽트를 모두 무시한다.
③ 인터럽트를 발생시킨 장치가 인터럽트 인식(acknowledge) 신호를 받으면 자신의 장치번호를 중앙처리장치로 보낸다.
④ 중앙처리장치에서 전송되는 인터럽트 인식 신호는 우선순위가 낮은 장치부터 높은 장치로 순차적으로 전달된다.
정답 체크 :
(3) 인터럽트를 발생시킨 장치가 인터럽트 인식 신호를 받으면 자신의 장치번호와 인터럽트 벡터(인터럽트 서비스 루틴 분기 번지)를 데이터 버스를 통해 CPU에게 보낸다.
오답 체크 :
(1) 다중 인터럽트 선(multiple interrupt lines)에 대한 설명이다.
(2) 우선순위에 의해 인터럽트를 처리하지 않으려면 지문에서 주어진 것처럼 발생된 인터럽트를 무시하는 방법도 존재한다.
(4) 소프트웨어 폴(software poll) 방식에 대한 설명이다. 소프트웨어 폴 방식에서는 TEST I/O 선을 통해 검사하는 순서를 조정할 수 있다.

8. TCP/IP 프로토콜 중 전송계층인 TCP에 대한 설명으로 옳은 것을 〈보기〉에서 고른 것은?

〈보기〉 ㄱ. 비연결형 서비스를 지원한다. ㄴ. UDP보다 데이터 전송 신뢰도가 낮다. ㄷ. 송신할 데이터를 패킷 단위로 전송한다. ㄹ. 수신측에서 잘못 전송된 패킷에 대해 재전송을 요구한다.

① ㄱ, ㄴ
② ㄴ, ㄷ
③ ㄷ, ㄹ
④ ㄱ, ㄹ

정답 체크 :
(3)
ㄷ. 송신할 데이터를 1500바이트 패킷 단위로 쪼개서 보낸다.
ㄹ. 수신측에서 잘못 전송된 패킷에 대해 재전송을 요구한다. 예를 들어, 순서 번호가 맞지 않으면 재전송을 요구한다.
오답 체크 :
(1), (2), (4)
ㄱ. TCP는 연결형(connection-oriented) 서비스를 지원하고(연결을 맺고 패킷을 전송), UDP는 비연결형(connectionless) 서비스를 지원한다(연결을 맺지 않고 패킷을 전송).
ㄴ. TCP가 UDP보다 데이터 전송 신뢰도가 높다. 즉, TCP는 보낸 패킷에 대한 응답 패킷을 받지만, UDP는 보낸 패킷에 대한 응답 패킷을 받지 않는다.

9. 다음 C 프로그램의 실행 결과로 옳은 것은?

```
#include 〈stdio.h〉
int sub(int n)
{
  if(n==0) return 0;
  if(n==1) return 1;
  return (sub(n-1) + sub(n-2));
}
void main() {
  int a=0;
  a=sub(4);
  printf("%d", a);
}
```

① 0
② 1
③ 2
④ 3

정답 체크 :
(4)

sub(4) = sub(3) + sub(2) = 3 // sub(4)는 sub(3)과 sub(2)를 순환 호출한다. sub(4)는 3을 반환한다.
sub(3) = sub(2) + sub(1) = 2 // sub(3)은 sub(2)와 sub(1)을 순환 호출한다. sub(3)은 2를 반환한다.
sub(2) = sub(1) + sub(0) = 1 // sub(2)는 sub(1)과 sub(0)을 순환 호출한다. sub(2)는 1을 반환한다.
sub(1) // 종료 조건에 의해 1을 반환한다.
sub(0) // 종료 조건에 의해 0을 반환한다.

10. 프로세스 동기화 문제를 해결하기 위한 방법인 세마포어(Semaphore) 알고리즘에 대한 설명으로 옳지 않은 것은?
① 세마포어 알고리즘은 상호배제 문제를 해결할 수 없다.
② 세마포어 변수는 일반적으로 실수형 변수를 사용하지 않는다.
③ 세마포어 알고리즘은 P 연산(wait 연산)과 V 연산(signal 연산)을 사용한다.
④ P 연산과 V 연산의 구현 방법에 따라 바쁜 대기(busy waiting)를 해결할 수 있다.
정답 체크 :
(1) 다익스트라가 테스 명령어의 문제 해결(공유 변수 수정하는 동안 인터럽트 발생 억제, 프로세스가 2개 이상일 때 적용하기 어려움)을 위해 제안하였다. 상호배제 및 다양한 연산의 순서도 제공한다.
오답 체크 :
(2) 세마포어 값은 true나 false로, P와 V연산과 관련된다. 네덜란드어로 P는 검사(Proberen), V 증가(Verhogen) 의미한다. 음이 아닌 정수 플래그 변수이다.
(3) 세마포어를 의미하는 S는 표준 단위 연산 P(프로세스 대기하게 하는 wait 동작, 임계 영역에 진입하는 연산)와 V(대기 중인 프로세스 깨우려고 신호 보내는 signal 동작, 임계 영역에서 나오는 연산)로만 접근하는 정수 변수이다.
(4) 바쁜 대기(busy waiting)란 아무것도 하지 않는 빈 반복문을 계속 돌다가 임계 구역에 진입할 수 있을 때 진입하는 방식으로, 빈 반복문을 반복하기 때문에 계속적으로 컨텍스트 교환(context switching)이 발생하며 이로 인하여 처리 효율이 떨어지는 단점이 있다. 또한, 어떠한 프로세스가 먼저 임계 구역에 진입을 할 수 있을지에 대한 처리를 할 수 없다는 단점 또한 존재한다. 바쁜 대기는 세마포어에서 최초에 제시된 방법이고, 이의 단점을 해결하기 위해 준비 큐를 활용하여 프로세스를 일시 정지하는 방식이 제안되었다.

11. 시스템의 보안 취약점을 활용한 공격방법에 대한 설명으로 옳지 않은 것은?
① Sniffing 공격은 네트워크 상에서 자신이 아닌 다른 상대방의 패킷을 엿보는 공격이다.
② Exploit 공격은 공격자가 패킷을 전송할 때 출발지와 목적지의 IP 주소를 같게 하여 공격대상 시스템에 전송하는 공격이다.
③ SQL Injection 공격은 웹 서비스가 예외적인 문자열을 적절히 필터링하지 못하도록 SQL문을 변경하거나 조작하는 공격이다.
④ XSS(Cross Site Scripting) 공격은 공격자에 의해 작성된 악의적인 스크립트가 게시물을 열람하는 다른 사용자에게 전달되어 실행 되는 취약점을 이용한 공격이다.
정답 체크 :

(2) Exploit : 해당 설명은 Land 공격이고, Exploit 공격은 컴퓨터 소프트웨어나 하드웨어의 버그나 취약점 등을 이용하여 공격자가 원하는 악의적 동작을 하도록 하는 공격 방법이다.

오답 체크 :

(1) Sniffing : 패킷을 태핑(Tapping)이나 미러링(Mirroring)을 통해 도청하는 것을 의미한다. 도청만 수행하므로 소극적 공격에 해당한다.

(3) SQL Injection : 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.

(4) XSS : 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

12. 소프트웨어 오류를 찾는 블랙박스 시험의 종류로 옳지 않은 것은?

① 비교 시험(comparison testing)

② 기초 경로 시험(basic path testing)

③ 동치 분할 시험(equivalence partitioning testing)

④ 원인-효과 그래프 시험(cause-effect graph testing)

정답 체크 :

(2) 기초 경로 시험 : 원시 코드의 독립적인 경로가 최소한 한 번은 실행되는 테스트 케이스를 찾아 테스트이다. (대표적인 화이트박스 테스트이다.)

오답 체크 :

(1) 비교 시험 : 완성된 제품의 장점과 단점을 비교하여 결과를 도출하는 테스트이다.

(3) 동치 분할 시험 : 각 영역에 해당하는 입력 값을 넣고 예상되는 출력 값이 나오는지 실제 값과 비교한다.

(4) 원인-효과 그래프 시험 : 동등 분할 기법의 단점(입력 환경의 복합성을 완전하게 고려하지 못함)을 극복하기 위해 나왔다. 프로그램의 명세를 분석하여 원인에 해당하는 입력 조건과 그 원인으로 발생되는 출력 결과를 논리적으로 연결하여 표현한 그래프 테스트 기법이다.

Tip! : 블랙박스 시험(입력 값에 대한 예상 출력 값을 정해놓고 그대로 결과가 나오는지를 체크)과 화이트박스 시험(프로그램 코드의 내부 구조를 테스트 설계의 기반으로 사용)을 테이블로 정리하면 다음과 같다.

블랙박스	동적 테스트 : 테스트 데이터를 이용해 실제 프로그램을 실행함으로써 오류를 찾는다.
	신택스 기법 : 문법을 정해놓고 적합/부적합 입력 값에 따른 예상 결과가 제대로 나오는지 테스트한다.
	동등(동치) 분할 기법 : 각 영역에 해당하는 입력 값을 넣고 예상되는 출력 값이 나오는지 실제 값과 비교한다.

	경계 값 기법 분석 : 경계에 있는 값을 테스트 데이터로 생성하여 테스트하는 방법이다.
	원인-효과 그래프 기법 : 프로그램의 명세를 분석하여 원인에 해당하는 입력 조건과 그 원인으로 발생되는 출력 결과를 논리적으로 연결하여 표현한 그래프 테스트 기법이다.
	그 외(비교 시험) : 완성된 제품의 장점과 단점을 비교하여 결과를 도출하는 테스트이다. (내부 구조를 고려하지 않는 대부분의 테스트가 블랙박스 시험이라고 할 수 있다.)
화이트박스	문장 검증 기준 : 프로그램 내의 모든 문장이 최소한 한 번은 실행될 수 있는 테스트 데이터를 갖는 테스트 케이스(입력값에 대한 출력값을 미리 만들어 놓고 테스트)를 선정한다.
	분기 검증 기준 : 조건문에 대해 T(ture), F(false)가 최소한 한 번은 실행되는 입력 데이터를 테스트 케이스로 사용한다. 분기 시점 또는 합류 위치에서 조건과 관련된 오류를 발견할 가능성이 높다.
	조건 검증 기준 : 두 개의 개별 조건식이 존재할 때 개별 조건식의 T와 F를 최소한 한 번은 테스트할 수 있도록 테스트 케이스 선정한다. 분기 검증 기준에서 발견하지 못한 오류(개별 조건식에 존재하는 오류)를 발견할 수 있는 더 강력한 테스트이다.
	분기/조건 검증 기준 : 개별 조건식을 모두 만족하면서 전체 조건식도 만족하는 테스트 케이스를 선정한다.
	다중 조건 검증 기준 : 마스크 문제까지 해결한 테스트 케이스에 해당하는 테스트 데이터를 생성하는 기준이다. 마스크 문제란 and의 경우 두 식 중 하나가 F인 경우 나머지 식이 F이든 T이든 상관없이 결과가 F인 것이고, or인 경우 두 식 중 하나가 T인 경우 나머지 식은 F이든 T이든 상관없이 결과가 T라는 것이다.
	기본(기초) 경로 테스트 : 원시 코드의 독립적인 경로가 최소한 한 번은 실행되는 테스트 케이스를 찾아 테스트이다.

13. 어떤 릴레이션 R(A, B, C, D)이 복합 애트리뷰트 (A, B)를 기본키로 가지고, 함수 종속이 다음과 같을 때 이 릴레이션 R은 어떤 정규형에 속하는가?

{A, B} → C, D B → C C → D

① 제1정규형
② 제2정규형
③ 제3정규형
④ 보이스-코드 정규형(BCNF)

정답 체크 :

(1) 무조건 제1정규형(릴레이션의 모든 속성이 더는 분해되지 않는 원자 값만 가진다)은 만족한다(만족하지 않으면 답이 없다). 제2정규형이 만족하는지 확인하면 된다.

오답 체크 :

(2) 제2정규형은 기본키가 아닌 모든 속성이 기본키에 완전 함수 종속되어야 하는데 해당 정규형을 만족하지 못한다. 왜냐하면 기본키가 (A, B)인데, 이에 대한 부분 함수 종속인 B → C가 존재하기

때문이다.
(3), (4) 제2정규형이 만족하지 않으므로 나머지도 만족하지 않는다.

14. 〈보기〉는 소프트웨어 개발방법론에 사용되는 분석, 설계 도구에 대한 설명이다. ㉠~㉢에 들어갈 내용을 옳게 나열한 것은?

〈보기〉
ㅇ 시스템 분석을 위하여 구조적 방법론에서는 (㉠) 다이어그램(diagram)이, 객체지향 방법론에서는 (㉡) 다이어그램이 널리 사용된다.
ㅇ 시스템 설계를 위하여 구조적 방법론에서는 구조도(structured chart), 객체지향 방법론에서는 (㉢) 다이어그램 등이 널리 사용된다.

	㉠	㉡	㉢
①	시퀀스(sequence)	데이터흐름(data flow)	유스케이스(use case)
②	시퀀스	유스케이스	데이터흐름
③	데이터흐름	시퀀스	유스케이스
④	데이터흐름	유스케이스	시퀀스

정답 체크 :
(4)
ㄱ. 데이터흐름 : DFD(Data Flow Diagram)은 처리 순서를 구조화하는 방법이다.
ㄴ. 유스케이스 : 시스템에서 제공해야하는 기능이나 서비스를 나타내고 사용자와 시스템 사이의 상호작용을 보여준다. 시스템의 기능을 나타내기 위하여 사용자의 요구를 추출하고 분석하는데 사용한다.
ㄷ. 시퀀스 : Instance(클래스에 메모리를 할당하여 구체화된 객체) 들이 어떻게 상호작용을 하는지를 묘사하는 다이어그램이다.

15. IPv4에서 서브넷 마스크가 255.255.255.0인 경우 하나의 네트워크에 최대 254대의 호스트를 연결할 수 있는 클래스로 옳은 것은?
① A 클래스
② B 클래스
③ C 클래스
④ D 클래스
정답 체크 :
(3) 최대 2^8-2개의 호스트(최대 호스트 254개, 0은 네트워크 ID로 제외, 255는 브로드캐스팅 IP로 제외)를 연결할 수 있다. (아래 그림 참고)
오답 체크 :
(1) 최대 2^{24}-2개의 호스트를 연결할 수 있다. (아래 그림 참고)
(2) 최대 2^{16}-2개의 호스트를 연결할 수 있다. (아래 그림 참고)
(4) 멀티캐스트 그룹용 IP로 사용된다.

16. 사원(사번, 이름) 테이블에서 사번이 100인 투플을 삭제하는 SQL문으로 옳은 것은? (단, 사번의 자료형은 INT이고, 이름의 자료형은 CHAR(20)으로 가정한다)
① DELETE FROM 사원 WHERE 사번=100;

② DELETE IN 사원 WHERE 사번=100;
③ DROP TABLE 사원 WHERE 사번=100;
④ DROP 사원 COLUMN WHERE 사번=100;
정답 체크 :
(1) DELETE FROM 테이블_이름 [WHERE 조건];의 형태로 사용한다.
오답 체크 :
(2) DELETE에 IN을 사용하지 않는다. FROM을 사용한다.
(3) DROP TABLE은 테이블을 삭제한다. (문제의 의도와 맞지 않다.)
(4) DROP COLUMN은 컬럼을 삭제한다. (문제의 의도와 맞지 않다.)

17. 다음과 같은 데이터가 입력되어 있는 엑셀시트에서 수식 =HLOOKUP(INDEX(A2:C5,2,2),B7:E9,2)를 계산한 결과는?

	A	B	C	D	E
1	학번	과목번호	성적		
2	100	C413	D		
3	200	C123	F		
4	300	C324	C		
5	400	C312	C		
6					
7	과목번호	C123	C312	C324	C413
8	과목이름	알고리즘	자료구조	운영체제	반도체
9	수강인원	90명	80명	75명	70명
10					

① 80명
② 75명
③ 반도체
④ 알고리즘
정답 체크 :
(4)
HLOOKUP(lookup_value, table_array, row_index_num, [range_lookup])의 사용법을 설명하면 다음과 같다.
lookup_value : 둘째 인수인 표의 1행에서 찾을 값이므로 C123이 된다. INDEX(A2:C5,2,2)는 A2:C5의 범위에서 2행 2열이므로 C123이 된다.
table_array : 찾는 값과 함수 결과값이 모두 있는 참조표의 범위이므로 B7:E9이다.
row_index_num : 찾는 값을 표의 첫 행에서 찾았을 때 실제 함수의 결과값이 있는 행의 번호이므로 2행이 된다. (알고리즘)
range_lookup : 범위를 이용한 검색을 수행하기 위해 생략되었다(정확히 일치하는 값을 찾고 없으면 범위를 이용한 검색을 수행한다). (TRUE는 생략 가능하다)

18. 공개키 기반 구조(Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?
① 인증기관은 공개키 인증서의 발급을 담당한다.
② 공개키 기반 구조는 부인방지 서비스 제공이 가능하다.
③ 공개키로 암호화 한 데이터는 암호화에 사용된 공개키로 해독한다.
④ 공개키 기반 구조는 공개키 알고리즘을 통한 암호화와 전자서명을 제공하는 복합적인 보안 시스템 환경이다.
정답 체크 :
(3) 공개키로 암호화 한 데이터는 암호화에 사용된 공개키와 수학적으로 연관된 개인키로 해독한다.
오답 체크 :
(1) 인증기관은 인증서의 관리를 행하는 국방부 직할부대 및 기관으로 키 쌍을 작성하고, 공개키 등록 때 본인을 인증한다. 그리고 인증서를 작성해서 발행하고 인증서를 폐지한다.
(2) 공개키 기반 구조(PKI)에서는 공개키에 인증 기관이 디지털 서명을 수행하므로 부인방지, 인증, 무결성 서비스 제공이 가능하다.
(4) 공개키 기반 구조(PKI)에서 공개키를 CA의 전자서명을 이용하여 배포하고, 이용자는 해당 공개키로 암호화를 수행한다.

19. 다음 관계 대수 연산의 수행 결과로 옳은 것은? (단, Π는 프로젝트, σ는 실렉트, $\bowtie_N$은 자연 조인을 나타내는 연산자이다)

관계 대수: $\Pi_{\text{고객번호, 상품코드}}(\sigma_{\text{가격<=40}}(\text{구매} \bowtie_N \text{상품}))$

구매

고객번호	상품코드
100	P1
200	P2
100	P3
100	P2
200	P1
300	P2

상품

상품코드	비용	가격
P1	20	35
P2	50	65
P3	10	27
P4	20	45
P5	30	50
P6	40	55

①

고객번호	상품코드
100	P1
100	P3

②

고객번호	상품코드
100	P1
200	P1

③

고객번호	상품코드
100	P1
100	P3
200	P1

④

고객번호	상품코드
200	P2
100	P2
300	P2

정답 체크 :
(3)
Π는 프로젝트 : 릴레이션에서 선택한 속성의 값으로 결과 릴레이션을 구성한다. P1, P3에서 고객번호와 상품코드의 속성만 선택한다.
σ는 실렉트 : 릴레이션에서 조건을 만족하는 투플만 선택하여 결과 릴레이션을 구성한다. 조건을 만족(가격이 40보다 작거나 같아야 한다)하는 P1, P3만 남는다.
$\bowtie_N$은 자연 조인 : 조인 속성(두 릴레이션이 공통으로 가지고 있는 속성)의 값이 같은 투플만 연결하여 생성된 추플을 결과 릴레이션에 포함한다. (P1, P2, P3가 자연 조인된다.)

20. 소프트웨어 생명주기 모형 중 프로토타입(prototype) 모형에 대한 설명으로 옳은 것을 〈보기〉에서 고른 것은?

〈보기〉
ㄱ. 프로토타입 모형의 마지막 단계는 설계이다.
ㄴ. 발주자가 목표 시스템의 모습을 미리 볼 수 있다.
ㄷ. 폭포수 모형보다 발주자의 요구사항을 반영하기가 용이하다.
ㄹ. 프로토타입별로 구현시스템에 대하여 베타테스트를 실시한다.

① ㄱ, ㄴ
② ㄴ, ㄷ
③ ㄷ, ㄹ
④ ㄱ, ㄹ
정답 체크 :
(2)
ㄴ. 프로토타입을 통해 발주자가 목표 시스템의 모습을 미리 볼 수 있고 수정을 요청할 수 있다.
ㄷ. 폭포수 모형은 프로토타입을 만들지 않기 때문에 발주자의 요구사항을 반영하기가 어렵다. (반대로 프로토타입은 이러한 것이 가능하다)
오답 체크 :
(1), (3), (4)
ㄱ. 프로토타입 모형의 마지막 단계는 인수/설치이다. (아래 그림 참고)
ㄹ. 프로토타입은 말 그대로 사용자의 의견을 반영하기 위한 중간 단계의 원형을 의미한다. 이러한 프로토타입에 최종 테스트 단계에서 수행하는 베타테스트를 실시하지는 않는다.