◆ 28 수능(예시) 14~17번

[14~17] 다음 글을 읽고 물음에 답하시오.

정보 시스템에 대한 '접근'이란 시스템 자원을 사용하기 위해 시스템과 상호 작용하는 작업을 의미한다. 이때 정보의 '객체'는 접근의 대상이 되는 시스템 또는 시스템 자원을, 정보의 '주체'는 접근을 통해 특정 목적을 달성하고자 하는 사람 또는 프로그램 등을 의미한다. '접근제어'는 적절한 권한을 가진 정보 주체만이 정보 객체에 접근할 수 있도록 통제하는 기술이다.

접근제어에서는 보안등급에 따라 접근 권한이 관리되는데, 이때 '보안등급'은 정보 주체와 객체에 부여된 중요도 또는 신뢰도를 나타낸다. 인터넷 카페에서 등급에 따라 읽기 또는 쓰기 권한을 주는 것은 이러한 예에 해당한다. 접근제어에서 관리하는 권한은 접근제어행렬, 접근제어목록 등으로 표현될 수 있다. '접근제어행렬'은 정보 주체를 행으로, 정보 객체를 열로 구성한 테이블로서, 객체에 대한 주체의 접근 권한은 해당 주체의 행과 해당 객체의 열이 만나는 셀에 기록된다. '접근제어목록'은 특정 객체에 대한 접근 권한을 갖는 주체가 나열된 목록이다.

접근제어에는 임의적 접근제어, 강제적 접근제어 등이 있다. ㉠ '임의적 접근제어'에서는 정보 객체의 소유자가 해당 객체에 대한 보안등급을 부여한다. 또한 객체에 대한 주체의 접근 권한 역시 해당 정보 객체의 소유자가 결정한다. 따라서 임의적 접근제어에서 접근 권한을 표현할 때는 접근제어목록이 주로 사용된다. 임의적 접근제어는 구현이 쉽고 권한 관리가 유연한 방식이지만, 정보 객체의 소유자가 접근 권한을 임의로 변경할 수 있어서 접근 권한의 일률적 통제가 어렵다는 문제가 있다. ㉡ '강제적 접근제어'에서는 보안등급 부여와 접근 권한의 관리가 중앙화된 방식으로 수행된다. 따라서 접근 권한을 일률적으로 통제할 수 있다는 장점이 있다. 강제적 접근제어에는 벨라파둘라 모델과 비바 모델 등이 있는데, ㉮ 벨라파둘라 모델은 기밀 정보의 유출 방지에 적합하고, 비바 모델은 정보의 신뢰도 유지에 적합하다.

정보 객체가 문서이고 정보 주체가 객체에 대한 읽기와 쓰기 권한을 갖는다고 가정했을 때, 벨라파둘라 모델에서 정보 주체는 자신보다 높은 등급의 문서를 읽는 것이 금지되지만, 등급이 같거나 낮은 문서에 대해서는 읽는 것이 가능하다. 또한 정보 주체는 자신보다 낮은 등급의 문서에 쓰는 것은 금지되지만, 등급이 같거나 높은 문서에 쓰는 것은 허용된다. 비바 모델에서 정보 주체는 자신보다 높은 등급의 문서에 대해서는 쓰기 권한이 없지만, 등급이 같거나 낮은 문서에 대해서는 쓰기가 가능하다. 또한 정보 주체는 자신보다 낮은 등급의 문서에 대해서는 읽기 권한이 없지만, 등급이 같거나 높은 문서를 읽는 것이 허용된다. 정보 주체는 자신보다 낮은 등급의 문서에 포함된 신뢰도가 낮은 정보를 참조함으로써 자신이 보유한 정보의 신뢰도를 떨어뜨릴 수 있는데, 비바 모델에서는 이를 방지할 수 있다.

14. 윗글의 내용과 일치하지 않는 것은?

① 접근제어행렬은 접근 권한을 나타내는 테이블이다.
② 임의적 접근제어의 접근 권한 표현에는 접근제어목록이 주로 사용된다.
③ 접근은 시스템과의 상호 작용을 통해 시스템 자원을 사용하는 것을 목적으로 한다.
④ 접근제어에서는 정보 주체와 정보 객체에 부여된 중요도나 신뢰도에 따라 접근 권한이 관리된다.
⑤ 접근제어목록은 특정 정보 주체가 접근할 수 있는 정보 객체를 목록화하여 관리하기 위해 사용된다.

15. ㉠과 ㉡에 대한 이해로 적절하지 <u>않은</u> 것은?

① ㉠과 달리 ㉡은 중앙화된 방식으로 접근 권한을 통제하기 때문에 일률적인 권한 관리가 가능하다는 특징이 있다.
② ㉠과 달리 ㉡은 정보 객체의 소유자 외의 정보 주체가 해당 객체를 변경하는 것을 방지하기 위해 사용되는 방식이다.
③ ㉡과 달리 ㉠은 정보 객체의 소유자가 접근 권한을 관리하기 때문에 권한 관리가 유연한 방식이다.
④ ㉠과 ㉡은 모두 권한을 부여하고 관리하기 위해 사용된다.
⑤ ㉠과 ㉡은 모두 접근제어행렬을 이용한 접근 권한 표현이 가능한 방식이다.

16. ㉮의 이유로 가장 적절한 것은?

① 정보 객체의 정보가, 같은 등급의 정보 주체로 전달되지 않기 때문이다.
② 정보 주체와 정보 객체의 보안등급이 중앙화된 방식으로 관리되기 때문이다.
③ 정보 주체가 자신보다 낮은 등급의 정보 객체에 쓰는 것이 금지되기 때문이다.
④ 정보 주체가 자신보다 높은 등급의 정보 객체에 쓰는 것이 가능하기 때문이다.
⑤ 정보 주체와 정보 객체를 중요도에 따라 분류하고 이를 테이블을 이용해서 관리하기 때문이다.

17. 윗글을 바탕으로 〈보기〉를 이해한 내용으로 적절하지 <u>않은</u> 것은? [3점]

〈보 기〉

다음은 비바 모델 접근제어를 사용하는 ○○ 회사의 접근제어행렬이다. 이 회사에는 갑, 을, 병이라는 정보 주체와 A, B, C라는 정보 객체가 있다. 이 회사는 모든 정보 주체 및 객체를 1등급, 2등급, 3등급의 보안등급으로 분류하고 있다. 테이블에서 r은 읽기 권한을, w는 쓰기 권한을 의미한다.

객체 / 주체	A	B	C
갑	[ ]	rw	r
을	rw	w	r
병	w	w	rw

① 모든 주체가 B에 대한 쓰기 권한을, C에 대한 읽기 권한을 가지고 있음을 고려할 때, 갑은 A에 대한 읽기 권한을 가지고 있겠군.
② 을은 병에 비해 읽기 권한이 많다는 점을 고려할 때, 보안등급은 을이 병보다 높겠군.
③ 을은 A에 대한 읽기 권한과 쓰기 권한을 모두 가지고 있음을 고려할 때, 을과 A의 보안등급은 같겠군.
④ 을은 C에 대한 읽기 권한이 있으므로 C보다 보안등급이 낮은 을에게 C의 중요 정보가 유출될 수 있겠군.
⑤ 병이 A와 B에 대한 읽기 권한이 없는 것은 병이 보유한 정보의 신뢰도 하락을 막기 위한 것이겠군.

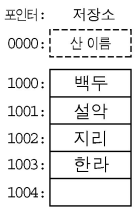
- 정답: 14.⑤ 15.② 16.③ 17.②

◆ 11 수능 25~26번

[25~26] 다음 글을 읽고 물음에 답하시오.

소프트웨어 개발에서 자료 관리를 위한 구조로는 '배열'과 '연결 리스트'가 흔히 사용된다. 이 구조를 가진 저장소가 실제 컴퓨터 메모리에 구현된 위치를 '포인터'라고 한다.

㉠ 배열은 물리적으로 연속된 저장소들을 사용한다. 배열에서는 흔히 <그림 1>과 같이 자료의 논리적 순서와 실제 저장 순서가 일치하도록 자료가 저장된다. 이때 원하는 자료의 논리적인 순서만 알면 해당 포인터 값을 계산할 수 있으므로, 바로 접근하여 읽기와 쓰기를 할 수 있다. 그런데 <그림 1>에서 자료 '지리'를 삭제하려면 '한라'를 한 칸 당겨야 하고, 가나다순에 따라 '소백'을 삽입하려면 '지리'부터 한 칸씩 밀어야 한다. 따라서 삽입하거나 삭제하는 자료의 순번이 빠를수록 나머지 자료의 재정렬 시간이 늘어난다.



<그림 1> 배열

<그림 2> 연결 리스트

㉡ 연결 리스트는 저장될 자료와 다음에 올 자료의 포인터인 '다음 포인터'를 한 저장소에 함께 저장한다. 이 구조에서는 <그림 2>와 같이 '다음 포인터'의 정보를 담을 공간이 더 필요하지만, 이 정보에 의해 물리적 저장 위치에 상관없이 자료의 논리적 순서를 유지할 수 있다. 또한 자료의 삽입과 삭제는 '다음 포인터'의 내용 변경으로 가능하므로 상대적으로 간단하다. 예를 들어 <그림 2>에서 '소백'을 삽입하려면 빈 저장소의 ⓐ에 '소백'을 쓰고 ⓑ와 ⓒ에 논리적 순서에 따라 다음에 올 포인터 값인 '1004'와 '1002'를 각각 써 주면 된다. 하지만 특정 자료를 읽으려면 접근을 시작하는 포인터부터 그 자료까지 저장소들을 차례로 읽어야 하므로 자료의 논리적 순서에 따라 접근 시간에 차이가 있다.

한편 '다음 포인터'뿐만 아니라 논리순으로 앞에 연결된 저장소의 포인터를 하나 더 저장하는 ㉢ '이중 연결 리스트'도 있다. 이 구조에서는 현재 포인터에서부터 앞뒤 어느 방향으로도 연결된 자료에 접근할 수 있어 연결 리스트보다 자료 접근이 용이하다.

25. 위 글을 통해 알 수 있는 사실로 옳지 않은 것은?

① 저장된 자료에 접근할 때는 포인터를 이용한다.
② 자료 접근 과정은 사용하는 자료 관리 구조에 따라 달라진다.
③ '배열'에서는 자료의 논리적 순서에 따라 자료 접근 시간이 달라진다.
④ '연결 리스트'는 저장되는 전체 자료의 개수가 자주 변할 때 편리하다.
⑤ '이중 연결 리스트'의 한 저장소에는 세 가지 다른 정보가 저장된다.

26. ㉠~㉢에 대해 <보기>의 실험을 한 후 얻은 결과로 옳은 것은? [3점]

<보 기>

동일 수의 자료를 논리순이 유지되도록 메모리에 저장한 다음 읽기, 삽입, 삭제를 동일 횟수만큼 차례로 실행하였다.

* 단, 충분히 많은 양의 자료로 충분한 횟수만큼 실험을 하되, 자료를 무작위로 선택하고 자료의 논리순이 유지되도록 함.

① ㉠은 ㉡에 비해 삭제 실험에 걸리는 총시간이 길었다.
② ㉠은 ㉢에 비해 저장 실험의 메모리 사용량이 많았다.
③ ㉡은 ㉠에 비해 삽입 실험에 걸리는 총시간이 길었다.
④ ㉡은 ㉢에 비해 저장 실험의 메모리 사용량이 많았다.
⑤ ㉢은 ㉡에 비해 읽기 실험에 걸리는 총시간이 길었다.

- 정답: 25.③ 26.①

◆ 13년 10월 고3 A형 28~30번

[28 ~ 30] 다음 글을 읽고 물음에 답하시오.

빅 데이터(Big Data)란 기존의 일반적인 기술로는 관리하기 곤란한 대량의 데이터를 가리키는 것으로, 그 특성은 데이터의 방대한 양과 다양성 및 데이터 발생의 높은 빈도로 요약된다. 이전과 달리 특수 학문 분야가 아닌 일상생활과 밀접한 환경에서도 엄청난 분량의 데이터가 만들어지게 되었고, 소프트웨어 기술의 발달로 이전보다 적은 시간과 비용으로 대량의 데이터 분석이 가능해졌다. 또한 이를 분석하여 유용한 규칙이나 패턴을 발견하고 다양한 예측에 활용하는 사례가 늘어나면서 빅 데이터 처리 기술의 중요성이 부각되고 있다.

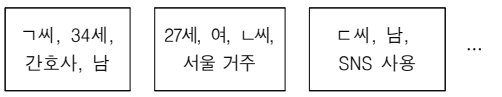
이러한 빅 데이터의 처리 및 분류와 관계된 기술에는 NoSQL 데이터베이스 시스템에 의한 데이터 처리 기술이 있다. 이를 이해하기 위해서는 기존의 관계형 데이터베이스 관리 시스템(RDBMS)에 대한 이해가 필요하다. RDBMS에서는 특정 기준이 제시된 데이터 테이블을 구성하고 이 기준을 속성으로 갖는 정형적 데이터를 다룬다. 고정성이 중요한 시스템이므로 상호 합의된 데이터 테이블의 기준을 자의적으로 추가, 삭제하거나 변용하는 것이 쉽지 않다. 또한 데이터 간의 일관성과 정합성*이 유지될 것을 요구하므로 데이터의 변동 사항은 즉각적으로 반영되어야 한다. <그림 1>은 RDBMS를 기반으로 은행들 간의 상호 연동되는 데이터를 정리하기 위해 사용하는 데이터 테이블의 가상 사례이다.

한예금 씨의 A 은행 거래내역

	거래일자	입금액	출금액	잔액	거래내용	기록사항	거래점
㉠ ……							
㉡ ……	2013.10.08.	30,000		61,217	이체	나저축	B 은행
㉢ ……	2013.10.09.		55,000	6,217	자동납부	전화료	A 은행
㉣ ……							

<그림 1> RDBMS에 의해 구성된 데이터 테이블의 예

NoSQL 데이터베이스 시스템은 특정 기준을 적용하기 어려운 비정형적 데이터를 효율적으로 처리할 수 있도록 설계되었다. 이 시스템에서는 선형으로 데이터의 특성을 나열하여 정리하는 방식을 통해 데이터의 속성을 모두 반영하여 처리한다. <그림 2>는 NoSQL 데이터베이스 시스템으로 자료를 다루는 방식을 나타낸 것이다.



[A]

행 = 1, 이름 = ㄱ씨, 나이 = 34세, 직업 = 간호사, 성별 = 남
행 = 2, 나이 = 27세, 성별 = 여, 이름 = ㄴ씨, 거주지 = 서울
행 = 3, 이름 = ㄷ씨, 성별 = 남, SNS = 사용

<그림 2> NoSQL 데이터베이스 시스템에 의한 데이터 처리의 예

<그림 2>에서는 '이름=', '나이=', '직업='과 같이 데이터의 속성을 표시하는 기준을 같은 행 안에 포함시킴으로써 데이터의 다양한 속성을 빠짐없이 기록하고, 처리된 데이터를 쉽게 활용할 수 있도록 하고 있다. 또한 이 시스템은 데이터와 관련된 정보의 변용이 상대적으로 자유로우며, 이러한 변화가 즉각적으로 반영되지 않는다는 특성을 지닌다.

* 정합성 : 논리적 모순이 없는 성질이나 상태.

28. 윗글의 설명 방식으로 가장 적절한 것은?

① 시간의 흐름에 따른 빅 데이터 개념의 변화를 설명하고 있다.
② 빅 데이터를 다루는 기술을 기존 기술과 비교하여 설명하고 있다.
③ 빅 데이터가 활용되는 유형을 기준에 따라 구분하여 제시하고 있다.
④ 다양한 사례를 들어 빅 데이터의 특성을 구체적으로 설명하고 있다.
⑤ 빅 데이터의 중요성을 개인적 차원과 사회적 차원으로 나누어 설명하고 있다.

29. ㉠ ~ ㉣에 대한 설명으로 적절하지 <u>않은</u> 것은? [3점]

① ㉠행에 제시된 것은 은행 거래 데이터를 처리하기 위한 기준이다.
② ㉠행의 각 항목은 'A 은행'의 개별 지점에서 임의로 변경하기 어렵다.
③ ㉡행의 거래로 인해 발생한 데이터는 '나저축'의 'B 은행 데이터베이스'에도 즉시 반영된다.
④ ㉡행과 ㉢행의 데이터는 특정 기준을 속성으로 갖는 정형적 데이터이다.
⑤ ㉣행에 기준과 다른 항목을 지닌 데이터가 올 경우 ㉠행의 기준을 즉시 변경하여 데이터를 처리한다.

30. [A]에 'ㄱ씨의 취미는 독서이다.'라는 정보를 추가하고자 한다. 윗글에 비추어 그 방법에 대한 설명으로 가장 적절한 것은?

① 1행의 '성별 = 남' 다음에 '취미 = 독서'를 기록한다.
② 1행과 2행 사이에 행을 삽입하여 '취미 = 독서'를 기록한다.
③ 3행 다음에 행을 추가하여 '행 = 4, 이름 = ㄱ씨, 취미 = 독서'를 기록한다.
④ 기준에 맞는 데이터 테이블을 구성하여 해당란에 '독서'를 기록한다.
⑤ 1행에 '독서'라는 속성을 반영할 수 있는 기준이 없으므로 기록 자체가 불가능하다.

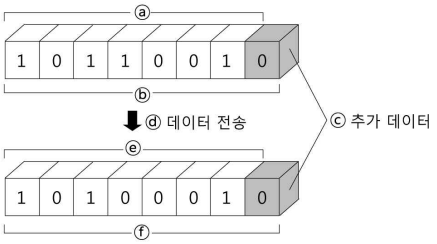
- 출전 : 시로타 마코토 저. 《빅 데이터의 충격》(한빛미디어, 2013)
- 정답: 28.② 29.⑤ 30.①

◆ 14년 7월 고3 A형 28~30번

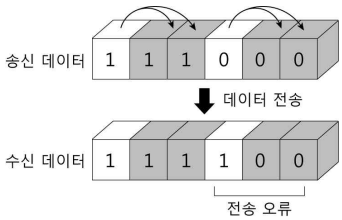
[28~30] 다음 글을 읽고 물음에 답하시오.

무선 통신 시스템에서 전파로 전송되는 신호는 때에 따라 왜곡될 수도 있고, 안테나나 통신 장비에서 발생하는 다양한 열잡음*으로 원하지 않는 신호가 더해질 수도 있다. 이처럼 데이터 전송 과정에서 오류가 생기면 수신기는 잘못된 신호를 받아 정확한 정보 전달이 어려워진다. 이런 경우에 추가 데이터를 함께 보내서 오류가 발생한 데이터를 검출하거나 복구하는 방식을 사용하는데, 이는 크게 자동 재전송 요구 방식과 순방향 오류 정정 방식으로 나눌 수 있다.

먼저 자동 재전송 요구 방식은 송신기에서 데이터를 전송할 때 데이터 중 1의 개수가 홀수이면 1을, 짝수이면 0의 추가 데이터를 송신 정보 데이터와 함께 보낸다. 수신기에서 받은 수신 정보 데이터의 1의 개수와 추가 데이터의 값을 비교하여 두 값이 다르면 수신기는 전송된 데이터 속에 오류가 있음을 알게 된다.



예를 들어 위의 그림과 같이 7개의 데이터를 전송할 때 네 번째 데이터 비트가 1이 아닌 0으로 수신될 수 있다. 이때 수신 정보 데이터의 1의 개수가 홀수인데 추가 데이터가 0이므로 오류가 발생했다는 것을 알게 된다. 그러나 수신기는 오류가 발생한 데이터의 위치를 알 수 없고, 오류를 정정할 능력 또한 없다. 이 경우 수신기는 자동 재전송 요구를 통해 송신기에 데이터 재전송을 요청한 후 오류를 복구하게 된다.



다음으로 순방향 오류 정정 방식은 송신기에서 전송할 데이터를 위의 그림처럼 각각 두 번씩 복사한 추가 데이터를 송신 정보 데이터와 함께 전송하는 방식이다. 데이터 전송에 오류가 발생한 경우, 수신기는 수신 데이터에서 복사된 데이터들과 비교하여 다른 값으로 전송됐는지를 확인해 오류가 발생한 위치를 알 수 있다. 만약 수신 데이터가 1인데 복사된 데이터들의 값이 모두 0이라면 실제 전송된 데이터는 1이 아닌 0으로, 오류를 고칠 수 있다. 이처럼 순방향 오류 정정 방식은 복사된 추가 데이터를 이용해 수신기가 단독으로 오류를 정정할 수 있다.

* 열잡음 : 수신기나 전송 선로 또는 전파 매체에서 전자 운동이 열에너지에 의해 동요하여 발생하는 잡음.

28. 윗글에 대한 설명으로 가장 적절한 것은?

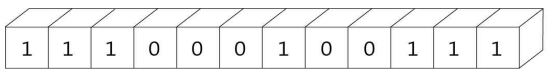
① 다른 대상과의 비교를 통해 가설을 입증하고 있다.
② 설명 대상을 구분하여 각각의 원리를 서술하고 있다.
③ 기술의 변화 양상을 시대별로 나누어 서술하고 있다.
④ 기술의 문제점을 분석하여 향후 개선 방향을 제시하고 있다.
⑤ 전문가의 견해를 인용하여 원리를 체계적으로 설명하고 있다.

29. ⓐ~ⓕ에 대한 설명으로 적절하지 <u>않은</u> 것은?

① ⓐ는 송신 정보 데이터이다.
② ⓑ는 전송 오류를 알기 위해 ⓐ에 ⓒ를 더한 데이터이다.
③ ⓒ는 ⓑ의 데이터 비트 전체의 개수에 따라 값이 결정된다.
④ ⓓ에서 열잡음으로 인해 전송 오류가 발생할 수 있다.
⑤ ⓕ에서 ⓒ의 값과 ⓔ의 분석 결과를 비교해 전송 오류를 확인할 수 있다.

30. <보기>는 '순방향 오류 정정 방식'을 통해 전송된 수신 데이터이다. 윗글을 바탕으로 <보기>에 대해 이해한 내용으로 적절한 것을 있는 대로 고른 것은?

<보 기>



ㄱ. 복사된 추가 데이터의 개수는 모두 8개이다.
ㄴ. 추가 데이터로 확인하면 송신 정보 데이터는 '1011'이다.
ㄷ. 오류가 발생한 위치는 송신 정보 데이터의 세 번째 데이터 비트이다.
ㄹ. 송신기에 추가 데이터 전송을 요청한 후 수신 데이터와 비교해 오류를 정정한다.

① ㄱ, ㄴ ② ㄱ, ㄷ ③ ㄷ, ㄹ
④ ㄱ, ㄴ, ㄷ ⑤ ㄴ, ㄷ, ㄹ

- 출전: ETRI(한국전자통신연구원) 전파기술연구부 저. 《훤히 보이는 전파기술》. (전자신문사, 2009)
- 정답: 28.② 29.③ 30.②

◆ 11년 4월 고3 48~50번

[48 ~ 50] 다음 글을 읽고 물음에 답하시오.

프로토콜이란 통신 상황에서 송신자의 정보를 정확하고 안정적으로 수신자에게 전송하기 위해 국제적으로 표준화한 약속을 의미한다. 이러한 프로토콜이 실제 통신 상황에서 적용되기 위해서는 표준화된 논리적 구조가 필요한데, 그 중 가장 대표적인 것이 통신 기능을 일곱 단계로 분할한 OSI 7계층 모델이다. 이때 송신자가 보내고자 하는 정보는 송신의 7단계부터 1단계까지의 과정을 거치며 발송되고 수신의 1단계부터 7단계까지의 과정을 통해 수신자에게 전달된다.

이 모델의 7단계에서 5단계까지는 정보가 소프트웨어적인 측면에서 다루어지고 있다는 공통점이 있는데, 이를 상위 계층이라고 한다. 최상위 단계인 7단계를 응용 계층이라고 하는데, 송신자나 소프트웨어가 네트워크에 접근하는 단계이다. 예를 들면 송신자가 사이트에 접속하여 로그-인하는 것 등이 이 단계에 해당된다. 6단계인 표현 계층은 보내고자 하는 정보를 다른 컴퓨터와의 호환이 가능하도록 문자열, 숫자 등의 컴퓨터 표준 형식으로 변환하는 단계이다. 또한 송신 과정에서 정보를 압축하고 수신 과정에서 압축을 푸는 단계이기도 한다. 5단계인 세션 계층은 보내려는 정보에 검사점을 추가하여 오류 발생 시 재전송하기 위한 일종의 기준점을 제시하는 단계이다.

이와는 달리 4단계에서 1단계까지를 하위 계층이라고 하는데, 정보가 전달될 수 있도록 물리적인 측면에서 기능한다는 공통점이 있다. 이 중 4단계인 전송 계층은 정보를 '프레임(frame)'이라는 단위로 분할한 후 각 프레임에 수신자의 인터넷 주소를 입력하여 정보가 정확하게 전달되도록 하는 기능을 한다. 또한 3단계인 네트워크 링크 계층에서는 보내고자 하는 정보를 수신자에게 가장 빠르고 안전하게 전송하기 위한 최적의 경로를 설정해주는 기능을 한다. 경로가 설정되면 2단계인 데이터 링크 계층에서는 프레임 단위로 변환된 정보를 물리적으로 전송이 가능한 2진수 0과 1로 표시되는 비트(bit)로 변환하여 이를 물리 계층으로 보낸다. 마지막으로 물리 계층은 정보를 보내기 위한 케이블의 종류나 전기 신호 등의 기계적 조건을 점검하여 이상이 없으면 케이블을 통해 정보를 발송한다.

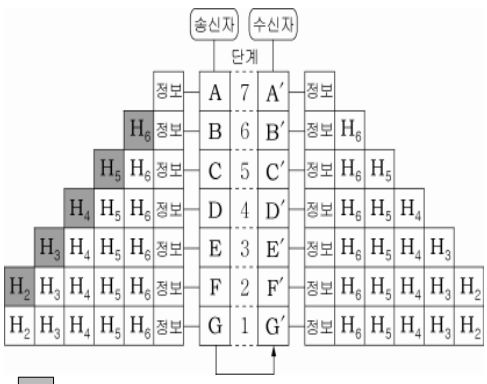
이러한 정보의 송·수신 과정에서 케이블로 연결되어 있는 물리계층을 제외하면 송신의 n계층과 수신의 n계층이 직접 연결되어 있지 않다. 하지만 정보를 정확히 전달하기 위해 송신과 수신의 n계층끼리는 해당 계층의 프로토콜을 중심으로 기능상 상호 작용해야 하므로 송신의 n계층마다 해당 계층의 프로토콜을 정보에 덧붙여 보내야 한다. 이처럼 각 계층에서 추가된 프로토콜들은 수신자의 해당 계층에서 해석된 후, 즉시 삭제되고 수신자의 7단계에서는 받고자 하는 정보만이 남게 된다.

48. 위 글의 표제와 부제로 적절한 것은? [1점]

① OSI 7계층 모델의 필요성
— 정보의 압축 과정을 중심으로
② OSI 7계층 모델의 장점과 단점
— 프로토콜의 변화 양상을 중심으로
③ 프로토콜을 이용한 정보 전달
— OSI 7계층 모델의 단계를 중심으로
④ 프레임의 분할과 결합 과정
— OSI 7계층 모델의 발전 과정을 중심으로
⑤ 통신의 과정에서 프로토콜의 전달 방식
— 전송 과정상 오류의 해결방법을 중심으로

※ <보기>는 OSI 7계층 모델을 간략히 도식화한 것이다. 위 글과 <보기>를 바탕으로 49번과 50번의 두 물음에 답하시오.

〈 보 기 〉



* H_n 부분은 n 단계에서 새롭게 추가된 프로토콜을 의미함.
(단, 7단계 및 1단계에서는 프로토콜을 추가하지 않음.)

49. <보기>의 단계에서 이루어지는 작업으로 적절하지 <u>않은</u> 것은?

① B : 정보를 호환 가능한 형식으로 변환한다.
② D : 정보를 프레임 단위로 분할한다.
③ E : 정보를 전송하기 위한 최적의 경로를 설정한다.
④ F : 보내고자 하는 정보를 비트 단위로 변환한다.
⑤ G : 정보에 검사점을 추가하여 오류에 대비한다.

50. 위 글을 읽고 난 후 <보기>에 대해 보일 반응으로 적절하지 <u>않은</u> 것은?

① B에서 정보를 압축했다면 B′에서는 압축이 풀리겠군.
② C의 정보 속에는 수신자의 인터넷 주소가 포함되어 있겠군.
③ D에서 추가된 H_4는 D′에서 해석된 후 삭제되겠군.
④ E와 E′는 동일한 프로토콜로 연계되어 상호 작용하겠군.
⑤ D′~G′까지는 물리적 측면에서 기능하는 단계로군.

- 출전: 베루즈 A. 포루잔 저. 《TCP/IP 프로토콜》. (한국맥그로힐, 2007)
- 정답: 48.③ 49.⑤ 50.②

[30~34] 다음 글을 읽고 물음에 답하시오.

DNS(도메인 네임 시스템) 스푸핑은 인터넷 사용자가 어떤 사이트에 접속하려 할 때 사용자를 위조 사이트로 접속시키는 행위를 말한다. 이는 도메인 네임을 IP 주소로 변환해 주는 과정에서 이루어진다.

인터넷에 연결된 컴퓨터들이 서로를 식별하고 통신하기 위해서 각 컴퓨터들은 IP(인터넷 프로토콜)에 따라 ㉠ 만들어지는 고유 IP 주소를 가져야 한다. 프로토콜은 컴퓨터들이 연결되어 서로 데이터를 주고받기 위해 사용하는 통신 규약으로 소프트웨어나 하드웨어로 구현된다. 현재 주로 사용하는 IP 주소는 '***.126.63.1'처럼 점으로 구분된 4개의 필드에 숫자를 사용하여 ㉡ 나타낸다. 이 주소를 중복 지정하거나 임의로 지정해서는 안 되고 공인 IP 주소를 부여받아야 한다.

공인 IP 주소에는 동일한 번호를 지속적으로 사용하는 고정 IP 주소와 번호가 변경되기도 하는 유동 IP 주소가 있다. 유동 IP 주소는 DHCP라는 프로토콜에 의해 부여된다. DHCP는 IP 주소가 필요한 컴퓨터의 요청을 받아 주소를 할당해 주고, 컴퓨터가 IP 주소를 사용하지 않으면 주소를 반환받아 다른 컴퓨터가 그 주소를 사용할 수 있도록 해 준다. 한편, 인터넷에 직접 접속은 안 되고 내부 네트워크에서만 서로를 식별할 수 있는 사설 IP 주소도 있다.

인터넷은 공인 IP 주소를 기반으로 동작하지만 우리가 인터넷을 사용할 때는 IP 주소 대신 사용하기 쉽게 'www.***.***' 등과 같이 문자로 ㉢ 이루어진 도메인 네임을 이용한다. 따라서 도메인 네임을 IP 주소로 변환해 주는 DNS가 필요하며 DNS를 운영하는 장치를 네임서버라고 한다. 컴퓨터에는 네임서버의 IP 주소가 기록되어 있어야 하는데, 유동 IP 주소를 할당받는 컴퓨터에는 IP 주소를 받을 때 네임서버의 IP 주소가 자동으로 기록되지만, 고정 IP 주소를 사용하는 컴퓨터에는 사용자가 네임서버의 IP 주소를 직접 기록해 놓아야 한다. 인터넷 통신사는 가입자들이 공동으로 사용할 수 있는 네임서버를 운영하고 있다.

㉮ 사용자가 어떤 사이트에 정상적으로 접속하는 과정을 살펴보자. 웹 사이트에 접속하려고 하는 컴퓨터를 클라이언트라 한다. 사용자가 방문하고자 하는 사이트의 도메인 네임을 주소창에 직접 입력하거나 포털 사이트에서 그 사이트를 검색해 클릭하면 클라이언트는 기록되어 있는 네임서버에 도메인 네임에 해당하는 IP 주소를 물어보는 질의 패킷을 보낸다. 네임서버는 해당 IP 주소가 자신의 목록에 있으면 클라이언트에 이 IP 주소를 알려 주는 응답 패킷을 보낸다. 응답 패킷에는 어느 질의 패킷에 대한 응답인지가 적혀 있다. 만일 해당 IP 주소가 목록에 없으면 네임서버는 다른 네임서버의 IP 주소를 알려 주는 응답 패킷을 보내고, 클라이언트는 다시 그 네임서버에 질의 패킷을 보내는 단계로 돌아가 같은 과정을 반복한다. 클라이언트는 이렇게 ㉣ 알아낸 IP 주소로 사이트를 찾아간다. 네임서버와 클라이언트는 UDP라는 프로토콜에 ㉤ 맞추어 패킷을 주고받는다. UDP는 패킷의 빠른 전송 속도를 확보하기 위해 상대에게 패킷을 보내기만 할 뿐 도착 여부는 확인하지 않으며, 특정 질의 패킷에 대해 처음 도착한 응답 패킷을 신뢰하고 다음에 도착한 패킷은 확인하지 않고 버린다. DNS 스푸핑은 UDP의 이런 허점들을 이용한다.

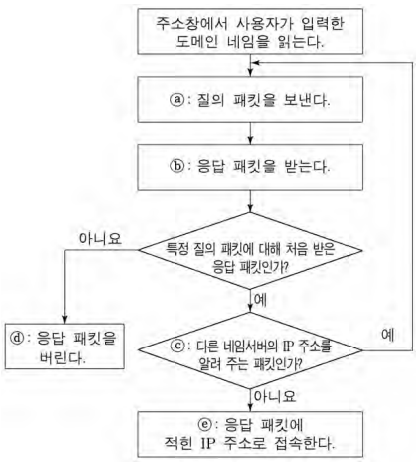
㉯ DNS 스푸핑이 이루어지는 과정을 알아보자. 악성 코드에 감염되어 DNS 스푸핑을 행하는 컴퓨터를 공격자라 한다. 클라이언트가 네임서버에 특정 IP 주소를 묻는 질의 패킷을 보낼 때, 공격자에도 패킷이 전달되고 공격자는 위조 사이트의 IP 주소가 적힌 응답 패킷을 클라이언트에 보낸다. 공격자가 보낸 응답 패킷이 네임서버가 보낸 응답 패킷보다 클라이언트에 먼저 도착하고 클라이언트는 공격자가 보낸 응답 패킷을 옳은 패킷으로 인식하여 위조 사이트로 연결된다.

30. 윗글의 '프로토콜'에 대한 설명으로 적절하지 않은 것은?

① 컴퓨터 사이의 통신을 위한 규약으로서 저마다 정해진 기능이 있다.
② IP에 따르면 현재 주로 사용하는 IP 주소는 4개의 필드에 적힌 숫자로 구성된다.
③ DHCP를 이용하는 컴퓨터는 IP 주소를 요청해야 IP 주소를 부여받을 수 있다.
④ DHCP를 이용하는 컴퓨터에는 네임서버의 IP 주소를 사용자가 기록해야 한다.
⑤ UDP는 패킷 전송 속도를 높이기 위해 패킷이 목적지에 제대로 도착했는지 확인하지 않는다.

31. <보기>는 ㉮ 또는 ㉯에서 이루어지는 클라이언트의 동작을 나타낸 것이다. 이에 대한 이해로 적절한 것은? [3점]

<보 기>



① ㉮: ⓐ가 두 번 동작했다면, 두 질의 내용이 동일하고 패킷을 받는 수신 측도 동일하다.
② ㉮: ⓑ가 두 번 동작했다면, 두 응답 내용이 서로 다르고 패킷을 보낸 송신 측은 동일하다.
③ ㉮: ⓒ는 ⓐ에서 질의한 도메인 네임에 해당하는 IP 주소를 네임서버가 찾았는지 여부를 확인하는 절차이다.
④ ㉯: ⓓ의 응답 패킷에는 공격자가 보내 온 IP 주소가 포함되어 있다.
⑤ ㉯: ⓔ의 IP 주소는 ⓐ에서 질의한 도메인 네임에 해당하는 IP 주소이다.

32. 윗글을 바탕으로 알 수 있는 것은?

① DNS는 도메인 네임을 사설 IP 주소로 변환한다.
② 동일한 내부 네트워크에 연결된 컴퓨터들의 사설 IP 주소는 서로 달라야 한다.
③ 유동 IP 주소 방식의 컴퓨터들에는 동시에 동일한 공인 IP 주소를 할당할 수 있다.
④ 고정 IP 주소 방식의 컴퓨터들에는 동시에 동일한 공인 IP 주소를 부여할 수 있다.
⑤ IP 주소가 서로 다른 컴퓨터들은 각각에 기록되어 있는 네임서버의 IP 주소도 서로 달라야 한다.

33. 윗글과 <보기>를 참고할 때, DNS 스푸핑을 피하기 위한 방법으로 적절한 것은?

<보 기>

DNS가 고안되기 전에는 특정 컴퓨터의 사용자가 'hosts'라는 파일에 모든 도메인 네임과 그에 해당하는 IP 주소를 적어 놓았고, 클라이언트들은 이 파일을 복사하여 사용하였다. 네임서버를 사용하는 현재에도 여전히 클라이언트는 질의 패킷을 보내기 전에 hosts 파일의 내용을 확인한다. 클라이언트가 이 파일에서 원하는 도메인 네임의 IP 주소를 찾으면 그 주소로 바로 접속하고, IP 주소를 찾지 못했을 때 클라이언트는 네임서버에 질의 패킷을 보낸다.

① 클라이언트에서 사용자가 hosts 파일을 찾아 삭제하면 되겠군.
② 클라이언트의 IP 주소를 사용자가 클라이언트의 hosts 파일에 적어 놓으면 되겠군.
③ 클라이언트에 hosts 파일이 없더라도 사용자가 주소창에 도메인 네임만 입력하면 되겠군.
④ 네임서버의 도메인 네임과 IP 주소를 사용자가 클라이언트의 hosts 파일에 적어 놓으면 되겠군.
⑤ 접속하려는 사이트의 도메인 네임과 IP 주소를 사용자가 클라이언트의 hosts 파일에 적어 놓으면 되겠군.

34. 문맥상 ㉠~㉤과 바꿔 쓰기에 가장 적절한 것은?

① ㉠: 제조(製造)되는
② ㉡: 표시(標示)한다
③ ㉢: 발생(發生)된
④ ㉣: 인정(認定)한
⑤ ㉤: 비교(比較)해

- 정답: 30.④ 31.③ 32.② 33.⑤ 34.②

◆ 18 수능 38~42번

[38~42] 다음 글을 읽고 물음에 답하시오.

디지털 통신 시스템은 송신기, 채널, 수신기로 구성되며, ⓐ전송할 데이터를 빠르고 정확하게 전달하기 위해 부호화 과정을 거쳐 전송한다. 영상, 문자 등인 데이터는 ⓑ기호 집합에 있는 기호들의 조합이다. 예를 들어 기호 집합 {a, b, c, d, e, f}에서 기호들을 조합한 add, cab, beef 등이 데이터이다. 정보량은 어떤 기호가 발생했다는 것을 알았을 때 얻는 정보의 크기이다. 어떤 기호 집합에서 특정 기호의 발생 확률이 높으면 그 기호의 정보량은 적고, 발생 확률이 낮으면 그 기호의 정보량은 많다. 기호 집합의 평균 정보량*을 기호 집합의 엔트로피라고 하는데 모든 기호들이 동일한 발생 확률을 가질 때 그 기호 집합의 엔트로피는 최댓값을 갖는다.

송신기에서는 소스 부호화, 채널 부호화, 선 부호화를 거쳐 기호를 ⓒ부호로 변환한다. 소스 부호화는 데이터를 압축하기 위해 기호를 0과 1로 이루어진 부호로 변환하는 과정이다. 어떤 기호가 110과 같은 부호로 변환되었을 때 0 또는 1을 비트라고 하며 이 부호의 비트 수는 3이다. 이때 기호 집합의 엔트로피는 기호 집합에 있는 기호를 부호로 표현하는 데 필요한 평균 비트 수의 최솟값이다. 전송된 부호를 수신기에서 원래의 기호로 ⓓ복원하려면 부호들의 평균 비트 수가 기호 집합의 엔트로피보다 크거나 같아야 한다. 기호 집합을 엔트로피에 최대한 가까운 평균 비트 수를 갖는 부호들로 변환하는 것을 엔트로피 부호화라 한다. 그중 하나인 '허프만 부호화'에서는 발생 확률이 높은 기호에는 비트 수가 적은 부호를, 발생 확률이 낮은 기호에는 비트 수가 많은 부호를 할당한다.

채널 부호화는 오류를 검출하고 정정하기 위하여 부호에 잉여 정보를 추가하는 과정이다. 송신기에서 부호를 전송하면 채널의 잡음으로 인해 오류가 발생하는데 이 문제를 해결하기 위해 잉여 정보를 덧붙여 전송한다. 채널 부호화 중 하나인 '삼중 반복 부호화'는 0과 1을 각각 000과 111로 부호화한다. 이때 수신기에서는 수신한 부호에 0이 과반수인 경우에는 0으로 판단하고, 1이 과반수인 경우에는 1로 판단한다. 즉 수신기에서 수신된 부호가 000, 001, 010, 100 중 하나라면 0으로 판단하고, 그 이외에는 1로 판단한다. 이렇게 하면 000을 전송했을 때 하나의 비트에서 오류가 생겨 001을 수신해도 0으로 판단하므로 오류는 정정된다. 채널 부호화를 하기 전 부호의 비트 수를, 채널 부호화를 한 후 부호의 비트 수로 나눈 것을 부호율이라 한다. 삼중 반복 부호화의 부호율은 약 0.33이다.

채널 부호화를 거친 부호들을 채널을 통해 전송하려면 부호들을 전기 신호로 변환해야 한다. 0 또는 1에 해당하는 전기 신호의 전압을 결정하는 과정이 선 부호화이다. 전압의 ⓔ결정 방법은 선 부호화 방식에 따라 다르다. 선 부호화 중 하나인 '차동 부호화'는 부호의 비트가 0이면 전압을 유지하고 1이면 전압을 변화시킨다. 차동 부호화를 시작할 때는 기준 신호가 필요하다. 예를 들어 차동 부호화 직전의 기준 신호가 양(+)의 전압이라면 부호 0110은 '양, 음, 양, 양'의 전압을 갖는 전기 신호로 변환된다. 수신기에서는 송신기와 동일한 기준 신호를 사용하여, 전압의 변화가 있으면 1로 판단하고 변화가 없으면 0으로 판단한다.

* 평균 정보량 : 각 기호의 발생 확률과 정보량을 서로 곱하여 모두 더한 것.

38. 윗글에서 알 수 있는 내용으로 적절한 것은?

① 영상 데이터는 채널 부호화 과정에서 압축된다.
② 수신기에는 부호를 기호로 복원하는 기능이 있다.
③ 잉여 정보는 데이터를 압축하기 위해 추가한 정보이다.
④ 영상을 전송할 때는 잡음으로 인한 오류가 발생하지 않는다.
⑤ 소스 부호화는 전송할 기호에 정보를 추가하여 오류에 대비하는 과정이다.

39. 윗글을 바탕으로, 2가지 기호로 이루어진 기호 집합에 대해 이해한 내용으로 적절하지 않은 것은?

① 기호들의 발생 확률이 모두 1/2인 경우, 각 기호의 정보량은 동일하다.
② 기호들의 발생 확률이 각각 1/4, 3/4인 경우의 평균 정보량이 최댓값이다.
③ 기호들의 발생 확률이 각각 1/4, 3/4인 경우, 기호의 정보량이 더 많은 것은 발생 확률이 1/4인 기호이다.
④ 기호들의 발생 확률이 모두 1/2인 경우, 기호를 부호화하는 데 필요한 평균 비트 수의 최솟값이 최대가 된다.
⑤ 기호들의 발생 확률이 각각 1/4, 3/4인 기호 집합의 엔트로피는 발생 확률이 각각 3/4, 1/4인 기호 집합의 엔트로피와 같다.

40. 윗글의 '부호화'에 대한 내용으로 적절한 것은?

① 선 부호화에서는 수신기에서 부호를 전기 신호로 변환한다.
② 허프만 부호화에서는 정보량이 많은 기호에 상대적으로 비트 수가 적은 부호를 할당한다.
③ 채널 부호화를 거친 부호들은 채널로 전송하기 전에 잉여 정보를 제거한 후 선 부호화한다.
④ 채널 부호화 과정에서 부호에 일정 수준 이상의 잉여 정보를 추가하면 부호율은 1보다 커진다.
⑤ 삼중 반복 부호화를 이용하여 0을 부호화한 경우, 수신된 부호에서 두 개의 비트에 오류가 있으면 오류는 정정되지 않는다.

41. 윗글을 바탕으로 <보기>를 이해한 내용으로 적절한 것은? [3점]

<보 기>

날씨 데이터를 전송하려고 한다. 날씨는 '맑음', '흐림', '비', '눈'으로만 분류하며, 각 날씨의 발생 확률은 모두 같다. 엔트로피 부호화를 통해 '맑음', '흐림', '비', '눈'을 각각 00, 01, 10, 11의 부호로 바꾼다.

① 기호 집합 {맑음, 흐림, 비, 눈}의 엔트로피는 2보다 크겠군.
② 엔트로피 부호화를 통해 4일 동안의 날씨 데이터 '흐림비맑음흐림'은 '01001001'로 바뀌겠군.
③ 삼중 반복 부호화를 이용하여 전송한 특정 날씨의 부호를 '110001'과 '101100'으로 각각 수신하였다면 서로 다른 날씨로 판단하겠군.
④ 날씨 '비'를 삼중 반복 부호화와 차동 부호화를 이용하여 부호화하는 경우, 기준 신호가 양(+)의 전압이면 '음, 양, 음, 음, 음, 음'의 전압을 갖는 전기 신호로 변환되겠군.
⑤ 삼중 반복 부호화와 차동 부호화를 이용하여 특정 날씨의 부호를 전송할 경우, 수신기에서 '음, 음, 음, 양, 양, 양'을 수신했다면 기준 신호가 양(+)의 전압일 때 '흐림'으로 판단하겠군.

42. 문맥을 고려할 때, 밑줄 친 말이 ⓐ~ⓒ의 동음이의어가 아닌 것은?

① ⓐ: 공항에서 해외로 떠나는 친구를 전송(餞送)할 계획이다.
② ⓑ: 대중의 기호(嗜好)에 맞추어 상품을 개발한다.
③ ⓒ: 나는 가난하지만 귀족이나 부호(富豪)가 부럽지 않다.
④ ⓓ: 한번 금이 간 인간관계를 복원(復原)하기는 어렵다.
⑤ ⓔ: 이 작품은 그 화가의 오랜 노력의 결정(結晶)이다.

- 정답: 38.② 39.② 40.⑤ 41.④ 42.④

◆ 22년 10월 고3 14~17번

[14 ~ 17] 다음 글을 읽고 물음에 답하시오.

일반적으로 거리는 두 개의 지점이 공간적으로 ⓐ 떨어진 정도를 나타내는 물리적 개념이다. 2차원 평면에 두 지점이 (0, 0)과 (1, 1)에 있다면 두 지점 사이의 최단 거리는 두 점을 잇는 직선의 길이 $\sqrt{2}$가 된다. 한편 거리는 추상적인 성질이나 가치에 대한 차이를 나타내는 척도로도 사용될 수 있다. 이럴 경우 떨어진 정도를 나타내는 기능은 유지되지만, 기준이나 관점에 따라 거리를 계산하는 방법이 달라진다.

거리의 개념은 디지털 데이터에도 적용될 수 있다. 데이터 간의 거리는 추상적 거리의 개념으로, 데이터가 표현하려는 정보에 따라 측정 방법이 다르다. 00, 11과 같은 2비트의 데이터가 2진수로 표현된 수치를 가리킨다면 00과 11의 거리는 두 수치의 차인 $|(0\times2^1+0\times2^0)-(1\times2^1+1\times2^0)|=3$이 된다.

그런데 2비트의 데이터 00이나 11이 어떤 상태를 나타내는 부호라면 거리는 두 부호가 구별되는 정도라 할 수 있다. 해밍 거리는 부호의 관점에서 부호들 간의 거리를 표현하는 방법 중 하나이다. 해밍 거리는 길이가 같은 두 부호를 비교하였을 때 두 부호의 같은 자리에 있는 서로 다른 문자의 개수로 나타낸다. 예를 들어 세 개의 부호 00, 01, 11이 있다면 00과 01의 해밍 거리는 1이고, 00과 11의 해밍 거리는 2이다. 이때 부호들 간의 최소 해밍 거리는 1이고, 최대 해밍 거리는 2이다.

부호들 간의 최소 해밍 거리를 충분히 멀게 한다면 통신이나 저장 과정에서 발생하는 오류를 검출하여 수정할 수 있다. 예를 들어 전송하려는 1비트의 원시 부호 0과 1이 있고 부호 단위로 송수신한다고 가정해 보자. 송신자가 1을 보낸다면 수신자는 0이나 1 중 하나를 받게 될 것이고, 송신자가 어떤 데이터를 보냈는지 알 수 없기 때문에 오류가 발생하더라도 오류가 있는지 알 수 없다. 이 경우 부호들 간의 최소 해밍 거리는 1이다. 0이나 1을 송수신하는 대신 원시 부호(x) 뒤에 확인 부호(p)를 덧붙여 x p에 해당하는 2비트 단위의 전송 부호를 만들어 보자. ㉠전송 부호는 고정된 원시 부호에 확인 부호를 덧붙이고, 확인 부호는 원시 부호에 대한 1의 개수가 짝수가 되도록 만든다는 규칙을 정한다면 전송 부호는 0 0과 1 1이 된다. 만일 수신자가 0 1이나 1 0 중 하나를 받은 경우 전송 부호에 오류가 있음을 알 수 있다. 하지만 어느 자리에서 오류가 났는지 알 수 없기 때문에 오류를 수정할 수는 없다.

[A] 0 0이나 1 1을 송수신하는 대신 p와 동일한 규칙의 확인 부호(q)를 한 번 더 덧붙여 x p q에 해당하는 3비트 단위의 전송 부호 0 0 0과 1 1 1 중 하나를 송수신한다고 가정해 보자. 한 자리의 오류만 있다고 가정하면 수신자가 0 0 1, 0 1 0, 1 0 0, 0 1 1, 1 0 1, 1 1 0 중 하나를 받은 경우 오류 발생 자리를 검출하여 수정할 수 있다. 예를 들어 1 1 0의 경우 x인 1에 대해 p와 q는 각각 1이 되어야 1의 개수가 짝수가 되지만 q가 0이므로 1의 개수가 홀수이다. 따라서 오류 발생 자리를 검출하여 1 1 0을 1 1 1로 수정할 수 있다. 이 경우 전송 부호 간의 최소 해밍 거리가 3이어서 한 자리의 오류를 검출하여 수정할 수 있는 것이다.

원시 부호에 확인 부호를 충분히 덧붙이면 전송 부호의 길이는 길어지지만 전송 부호들 간의 최소 해밍 거리도 함께 멀어져 오류가 많이 발생하더라도 오류를 검출하여 수정하는 것이 가능하다. 하지만 동일한 정보를 보낼 때 덧붙이는 확인 부호의 개수가 늘어나면 보내야 하는 데이터의 양이 늘어나 전송 효율이 낮아진다.

14. 윗글을 통해 알 수 있는 내용으로 적절하지 않은 것은?

① 2진수로 표현된 수치를 가리키는 데이터들 간의 거리는 수치 간의 차로 표현될 수 있다.
② 추상적인 성질이나 가치의 차이를 나타내는 척도로 거리의 개념이 사용될 수 있다.
③ 물리적 개념에서의 거리는 두 지점이 공간적으로 떨어져 있는 정도를 나타낸다.
④ 00과 11의 2진수 수치의 차이와 해밍 거리는 같은 값으로 측정된다.
⑤ 데이터가 표현하려는 정보에 따라 거리를 측정하는 방법이 다르다.

15. [A]와 <보기>를 이해한 내용으로 적절하지 않은 것은? [3점]

< 보 기 >

확인 부호가 오류 발생 자리에 대한 정보가 되도록 규칙을 정하면 전송 부호에서 한 자리 오류가 발생했을 때 수정이 가능하다. 확인 부호를 검사하여 p에 오류가 있으면 **p 자리**를 1로, 오류가 없으면 0으로 표현한다. 같은 방식으로 q에 오류가 있으면 **q 자리**를 1로, 오류가 없으면 0으로 표현한다. 0과 1로 표현된 **p 자리** **q 자리**를 계산하면 한 자리의 오류가 발생했을 때 그 자리를 알아낼 수 있다.

송신	수신	규칙			오류 발생 자리
		오류		계산	
		p 자리	q 자리		
000	000	0	0	$0\times2^1+0\times2^0$	□□□
	010		0	$1\times2^1+0\times2^0$	□☑□
	110	0	1	$0\times2^1+1\times2^0$	
	011	1	1	$1\times2^1+1\times2^0$	
⋮	⋮	⋮	⋮	⋮	⋮

① 송신자는 전송 부호 간의 해밍 거리가 3이 될 수 있도록 0은 000으로, 1은 111로 보내는 것이겠군.
② 수신자가 010을 받았다면 **p 자리**의 오류를 1로 표현하여 000으로 판단하겠군.
③ 수신자가 110이나 101을 받았다면 수신한 부호에 있는 0을 1로 수정하여 모두 111로 판단하겠군.
④ 수신자가 011을 받았다면 **p 자리**와 **q 자리** 모두에 오류가 있는 경우이므로 두 자리의 오류를 수정하겠군.
⑤ 수신자가 111을 받았다면 **p 자리**와 **q 자리**의 오류를 모두 0으로 표현하여 오류가 없는 것으로 판단하겠군.

16. ㉠에 대한 이해로 가장 적절한 것은?

① 전송 부호들 간의 최소 해밍 거리를 멀게 하면 전송하는 데이터의 양은 늘어난다.
② 전송 부호들 간의 최소 해밍 거리가 1이면 전송 과정에서의 오류 검출이 가능하다.
③ 두 전송 부호의 같은 자리에 같은 문자의 개수가 많을수록 해밍 거리는 멀어진다.
④ 덧붙이는 확인 부호가 많아지면 전송 부호들 간의 최대 해밍 거리는 가까워진다.
⑤ 전송 부호들 간의 최소 해밍 거리가 가까워질수록 전송 효율은 낮아진다.

17. ⓐ의 문맥적 의미와 가장 유사한 것은?

① 식당은 본관과 조금 떨어져 있는 별관이다.
② 해가 떨어지자 새는 보금자리로 돌아갔다.
③ 그들의 실력은 평균보다 떨어지는 편이다.
④ 상처가 나서 생긴 딱지가 아물어 떨어졌다.
⑤ 물건을 팔면 본전을 빼고 만 원이 떨어진다.

- 정답: 14.④ 15.④ 16.① 17.①

◆ 22년 3월 고1 26~30번

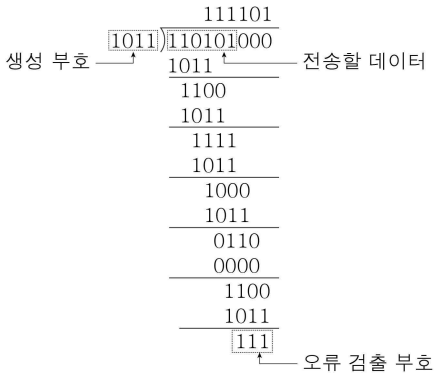
[26 ~ 30] 다음 글을 읽고 물음에 답하시오.

컴퓨터 네트워크에서 데이터가 전송될 때 수신된 데이터에 오류가 있는 경우가 있다. 오류를 검출하기 위해 송신기는 오류 검출 부호를 포함한 데이터를 전송하고 수신기는 수신한 데이터를 검사하여 오류가 있으면 재전송을 요청한다.

수신한 데이터에 오류가 있는지 검출하는 가장 간단한 방식은 ㉠ 패리티 검사이다. 이 방식은 전송할 데이터에 패리티 비트라는 오류 검출 부호를 추가하는 방법으로, 패리티 비트를 추가하여 데이터의 1의 개수를 짝수나 홀수로 만든다. 1의 개수를 짝수로 만드는 방식을 짝수 패리티, 홀수로 만드는 방식을 홀수 패리티라고 하고 송·수신기는 모두 같은 방식을 사용해야 한다. 예를 들어 짝수 패리티를 사용한다면 송신기는 항상 데이터의 1의 개수를 짝수로 만들어서 전송하지만 만일 수신한 데이터의 1의 개수가 홀수가 되면 수신기는 오류가 발생했다고 판단하는 것이다. 하지만 패리티 검사는 ㉮ 수신한 데이터에서 짝수 개의 비트에 오류가 동시에 있으면 이를 검출하기 어렵다. 또한 오류의 발생 여부를 검출할 수 있을 뿐 데이터 내 오류의 위치는 알아낼 수 없다.

전송할 데이터를 2차원 배열로 구성해서 패리티 비트를 생성하면 오류의 발생 여부뿐만 아니라 오류의 위치도 알아낼 수 있다. 예를 들어 송신기가 1100011 1111111을 전송한다고 하자. 송신기는 이를 $\begin{matrix}1100011\\1111111\end{matrix}$과 같이 2차원 배열로 구성하고 가로 방향인 모든 행과 세로 방향인 모든 열에 패리티 비트를 생성한 후 이를 포함한 데이터를 전송한다. 수신기는 수신한 데이터의 각각의 행과 열의 1의 개수를 세어 오류를 검사한다. 만약 어떤 비트에 오류가 발생하면 그 비트가 포함된 행과 열에서 모두 오류가 검출된다. 따라서 오류가 발생한 위치를 알 수 있다. 다만 동일한 행 또는 열에서 짝수 개의 오류가 발생하면 오류가 발생한 정확한 위치를 알 수 없다.

㉡ CRC 방식은 미리 선택된 생성 부호를 사용해서 오류 검출 부호를 생성하는 방식이다. 전송할 데이터를 생성 부호로 나누어서 오류 검출 부호를 생성하는 데 모듈로-2 연산을 활용한다. 모듈로-2 연산은 자릿수가 제한된 상태에서 나머지를 구하는 연산으로 해당 자릿수의 비트 값이 같으면 0, 다르면 1이 된다.



<그림>

<그림>과 같이 생성 부호가 1011이고 전송할 데이터가 110101인 경우를 보자. 전송할 데이터는 오류 검출 부호를 추가해야 하기 때문에 그만큼의 비트가 더 필요하다. 송신기는 전송할 데이터의 오른쪽 끝에 생성 부호의 비트 수보다 하나 작은 비트 수만큼 0을 추가한 후 이를 생성 부호로 나누고 그 나머지가 오류 검출 부호가 된다. 송신기는 오류 검출 부호를 포함한 데이터 ㉢ 110101111만을 전송하고 수신기는 수신한 데이터를 송신기와 동일한 생성 부호로 나눈다. 수신한 데이터는 전송할 데이터에 나머지를 추가했으므로 오류가 없다면 생성 부호로 나누었을 때 나머지가 0이 된다. 이때 나머지가 0이 아니면 수신한 데이터에 오류가 있다고 판단한다. CRC 방식은 복잡하지만 여러 개의 오류가 동시에 생겨도 이를 검출할 수 있어서 오류 검출 확률이 높다.

26. 윗글에서 알 수 있는 내용으로 적절하지 않은 것은?

① CRC 방식은 모듈로-2 연산을 사용해서 생성 부호를 만들어 낸다.
② 패리티 검사에서 송신기와 수신기는 동일한 패리티 방식을 사용해야 한다.
③ CRC 방식에서 생성 부호의 비트 수는 오류 검출 부호의 비트 수보다 하나가 더 많다.
④ 짝수 패리티는 패리티 비트를 포함한 데이터의 1의 개수가 짝수인지 여부를 검사한다.
⑤ CRC 방식은 여러 개의 오류가 동시에 생겨도 검출할 수 있어서 오류 검출 확률이 높다.

27. ㉠과 ㉡에 대해 이해한 내용으로 적절하지 않은 것은?

① ㉠은 ㉡과 달리 데이터에 포함된 1의 개수가 짝수나 홀수가 되도록 오류 검출 부호를 생성한다.
② ㉡은 ㉠과 달리 데이터의 오류를 검출하기 위해 송신기와 수신기 모두에서 오류 검사를 해야 한다.
③ ㉠과 ㉡은 모두, 수신한 데이터의 오류 발생 여부를 수신기가 판단한다.
④ ㉠과 ㉡은 모두, 데이터를 전송하기 전에 오류 검출 부호를 생성해야 한다.
⑤ ㉠과 ㉡은 모두, 전송할 데이터가 같더라도 오류 검출 부호는 다를 수 있다.

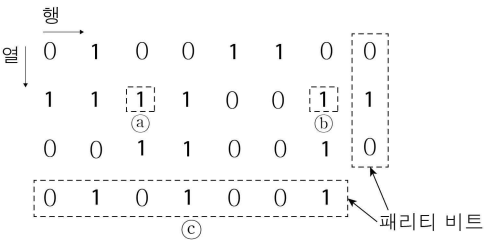
28. ㉮의 이유로 가장 적절한 것은?

① 송신기가 패리티 비트를 생성하는 것이 불가능하기 때문에
② 전송되는 데이터에 포함된 1의 개수가 항상 홀수로 나타나기 때문에
③ 전송되는 데이터에 포함된 1의 개수가 항상 짝수로 나타나기 때문에
④ 오류가 발생했을 때 전송되는 패리티 비트의 크기가 늘어나기 때문에
⑤ 수신한 데이터가 정상일 때와 수신한 데이터에 오류가 있을 때의 패리티 비트가 동일하기 때문에

29. 윗글을 바탕으로 <보기>를 설명한 내용으로 적절하지 <u>않은</u> 것은? [3점]

< 보 기 >

송신기는 오류 검출 방식으로 홀수 패리티를 활용하기로 하였다. 수신기는 수신한 데이터에 오류가 있다고 다음과 같이 판단하였다.



(단, 패리티 비트의 오류는 없다고 가정한다.)

① 첫 번째 행은 패리티 비트를 포함한 데이터의 1의 개수가 홀수이므로 오류가 없다고 판단했을 것이다.
② 여섯 번째 열은 패리티 비트를 포함한 데이터의 1의 개수가 홀수이므로 오류가 없다고 판단했을 것이다.
③ ⓐ가 포함된 행과 열의 패리티 비트를 포함한 데이터의 1의 개수가 각각 짝수이므로 수신기는 ⓐ를 오류라고 판단했을 것이다.
④ 수신한 데이터에서 ⓑ도 0으로 바뀌어서 수신되었다면 데이터의 오류 발생 여부를 검출할 수 없었을 것이다.
⑤ 짝수 패리티를 활용했다면 송신기는 ⓒ를 1010110으로 생성했을 것이다.

30. <보기>는 수신기가 ⓒ의 오류를 검사한 연산이다. 윗글을 바탕으로 <보기>를 이해한 내용으로 적절하지 <u>않은</u> 것은?

< 보 기 >

```
          111101
1011)110101111
     1011
      1100
      1011
       1111
       1011
        1001
        1011
         0101
         0000
          1011
          1011
             0
```

① 수신기는 송신기와 동일한 생성 부호인 '1011'을 사용하여 모듈로-2 연산을 하였군.
② 수신기가 수신한 데이터의 오른쪽 끝에 있는 '111'은 송신기에서 생성한 오류 검출 부호이군.
③ 수신기가 모듈로-2 연산을 할 때는 수신한 데이터에 생성 부호보다 하나 작은 비트 수만큼의 0을 추가하지 않았군.
④ 수신기가 연산한 몫인 '111101'이 송신기가 전송한 데이터와 동일하기 때문에 수신기는 오류가 없다고 판단했겠군.
⑤ 수신기가 연산한 결과의 나머지가 0이 아니었다면 수신기는 송신기에 재전송을 요청했겠군.

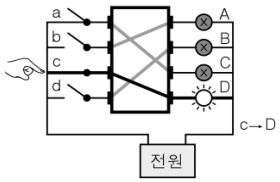
- 정답: 26.① 27.② 28.⑤ 29.④ 30.④

◆ 12년 3월 고3 19~21번

[19~21] 다음 글을 읽고 물음에 답하시오.

암호를 만드는 방식에는 크게 전치(轉置) 방식과 환자(換字) 방식이 있다. 전치 방식은 전하고자 하는 메시지인 평문의 철자 위치를 바꾸어 암호문을 만드는 방식이고, 환자 방식은 평문 철자를 일정한 규칙에 따라 다른 문자로 바꾸어 암호문을 만드는 방식이다. 더 복잡하게 하고자 할 때는 전치 방식과 환자 방식을 함께 적용한 혼합 방식을 사용할 수도 있다. 이렇게 평문을 암호문으로 만드는 암호화의 규칙을 '알고리즘(algorism)'이라 하고 역으로 암호문을 평문으로 푸는 해독의 규칙을 '키(key)'라 한다.

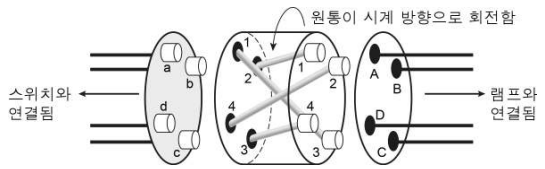
암호의 원리는 현대 문명의 발달과 함께 다양한 암호 장치들로 구현되었다. 특히 전신(電信)에 의한 송·수신이 가능하게 되면서 전기 암호 장치가 개발되었다.



[그림 1] 전기 암호 장치의 구조

[그림 1]에서 스위치 a, b, c, d와 연결된 램프 A, B, C, D로 구성된 이 장치는, 스위치 역할을 하는 키보드에서 평문 철자를 입력했을 때 불이 켜지는 램프가 암호 철자를 나타낸다. [그림 1]에서처럼 송신자가 평문 철자 c를 입력했을 때 c에 연결된 램프 D가 켜지고 이 암호 철자 D를 전신으로 받은 수신자는 암호 철자인 D를 눌러 D에 연결된 원래의 평문 철자 c를 얻게 되는 방식이다.

그러나 전기 암호 장치는 회로 구조가 파악되면 쉽게 암호가 노출될 수 있고, 그런 경우 다시 회로 구조를 바꿔야 하는 불편함이 있었기 때문에 전시(戰時)와 같이 분초를 다투는 위급한 상황에는 적합하지 않았다. 이런 문제를 극복하기 위해 회전하는 원통 속에 전기 회로를 넣은 '에니그마'가 개발되었다.



[그림 2] 에니그마의 구조

에니그마는 원통이 회전함에 따라 스위치와 램프의 연결 상태가 계속 바뀌기 때문에 회로 구조를 조작하지 않고도 평문 철자와 암호 철자의 대응 규칙을 쉽게 바꿀 수 있다. 예를 들어 원통이 회전하지 않는 경우에는 평문 'b'를 입력하면 [그림 2]의 회로 구조를 거쳐 암호문 'A'로 나타나지만(b-2-1-A), 원통이 시계 방향으로 1/4바퀴 돌아간 경우에는 같은 'b'를 입력하더라도 원통 속의 회로가 다른 단자와 연결되면서 암호문 'C'로 나타나게 된다(b-3-4-C). 따라서 암호를 파악하기 위해서는 원통 바퀴 내부의 회로 구조뿐만 아니라 한 글자를 입력할 때마다 원통이 언제, 얼마나 회전하는지 등 원통의 회전 규칙도 함께 알아야 한다.

19. '전기 암호 장치'와 '에니그마'에 대한 설명으로 적절하지 <u>않은</u> 것은?

① 전기 암호 장치의 한계를 극복하기 위해 에니그마를 개발했다.
② 전기 암호 장치와 에니그마는 전기 회로를 통해 환자 방식을 구현했다.
③ 전기 암호 장치와 에니그마의 스위치는 평문 철자, 램프는 암호 철자를 나타낸다.
④ 에니그마는 전기 암호 장치와 같이 회로 구조만 알아도 암호를 해독할 수 있다.
⑤ 전기 암호 장치는 에니그마와 달리 대응 규칙을 쉽게 바꾸기 어렵다는 문제점이 있다.

20. 위 글을 통해 <보기>를 이해한 것으로 적절하지 <u>않은</u> 것은?

<보 기>

영희가 철수에게 보낸 문자　　철수가 영희에게 보낸 문자

① '널 사랑해'는 영희가 전하고 싶은 평문이군.
② '널 사랑해'를 '해랑사널'로 바꾼 것은 전치 방식이군.
③ '해랑사널'을 'gofkdtksjf'로 바꾼 것은 환자 방식이군.
④ '한글 입력 모드에서 이 영문을 입력하고, 그걸 거꾸로 읽어'는 알고리즘에 해당하는군.
⑤ 철수가 보낸 '해랑사도나'는 전치 방식으로 보낸 것이군.

21. 위 글의 내용을 바탕으로 할 때, <보기>의 괄호 안에 들어갈 '암호 철자'는?

<보 기>

[그림 2]의 에니그마로 암호를 보내고자 한다. 에니그마에 첫 번째 평문 철자를 입력할 때는 원통이 고정되어 있고, 그 이후에는 평문 철자를 입력할 때마다 원통이 반시계 방향으로 1/4만큼 회전하도록 설계되었다고 하자. 평문 철자 'bc'를 입력했을 때 나올 암호 철자는 (　　)이다.

① AB　② AC　③ BC　④ DA　⑤ DB

- 출전 : 루돌프 키펜한 저, 김시형 역. 《암호의 세계》. (이지북, 2001)
- 정답: 19.④ 20.④ 21.①

◆ 07 경찰대 1차 47~50번

[47-50] 다음 글을 읽고 물음에 답하시오.

1941년 6월 22일 독일은 소련을 침공했다. 소련은 독일뿐 아니라 일본까지도 동시에 막아야 할 위기에 처했다. 그 때 동경으로부터 날아온 비밀 정보는 전쟁의 흐름을 바꾸어 놓았다. "일본은 소련을 공격할 계획이 없음." 마샬 추코프 사령관은 이 보고에 따라 시베리아 주둔 몇 개 사단과 탱크, 비행기를 모스크바 전선으로 이동시켜 독일군을 저지했다.

소련은 어떤 방법으로 일본에게 들키지 않고 비밀 정보를 송신할 수 있었을까? 스파이 클라우젠이 사용한 방법은 다음과 같다. 먼저 오른쪽의 암호 표에서처럼 맨 위에 **subway**를 쓴 다음, 그 밑에 나머지 알파벳을 순서대로 적고, 마지막에는 마침표와 빗금을 첨가했다. 그리고 빈도가 높은 8개 철자 'a, s, i, n, t, o, e, r'에는 0부터 7까지 숫자를 매기는데, 왼쪽 칸의 's'에서부터 아래로 내려가면서 숫자를 적었다. 나머지 철자들도 같은 방법으로 해서 80에서 99까지의 수를 기입했다. 이것으로 정보 문서는 숫자로 변환되었다. 가령, 클라우젠이 '**no attack**(공격 없음)'이라는 정보를 암호화 한다고 가정해 보자. 그러면 위의 방법에 따라 '**no attack**'은 **729456658088**로 바뀐다.

s	u	b	w	a	y
c	d	e	f	g	h
i	j	k	l	m	n
o	p	q	r	t	v
x	z	.	/		

s	u	b	w	a	y
0				5	
c	d	e	f	g	h
		3			
i	j	k	l	m	n
1					7
o	p	q	r	t	v
2			4	6	
x	z	.	/		

s	u	b	w	a	y
0	82	87	91	5	97
c	d	e	f	g	h
80	83	3	92	95	98
i	j	k	l	m	n
1	84	88	93	96	7
o	p	q	r	t	v
2	85	89	4	6	99
x	z	.	/		
81	86	90	94		

그런데 ㉠이런 방법으로만 암호화를 하면 일본 정보부가 쉽게 알아챌 것이다. 그래서 그는 모스크바와 미리 약속한 방식대로 이 숫자들에다 <독일 제국 연감>(1935년)에서 선택한 다른 숫자들을 결합하였다. 가령, 연감의 34째 면, 23째 줄, 6째 단에서 '4230, 5166, 7821, 9421'을 선택한 다음, 이것을 세 번째 숫자부터 사용했다. 이렇게 만들어진 수 '**305166782194……**'가 해독의 열쇠이다. 그는 이것을 앞에서 만든 암호문 **729456658088** 아래에 배열했다.

729456658088
305166782194

그 다음에는 두 줄의 수를 위아래로 더하되, 9를 넘더라도 10을 윗자리로 넘기지 않는 방법을 사용했다. 즉, '7+3'은 10이 아니라 0이다. 이렇게 해서 나온 결과가 '중간 암호문'이다. ㉡여기에 다시 연감의 해당 위치를 나타낸 수 **34236**을 덧붙여야만 했다. 이것은 34면 23째줄 6째 단을 뜻한다. 덧붙이는 방법은, 먼저 이 수를 중간 암호문의 앞자리 5개와 더한 다음에(이때에도 10을 윗자리로 넘기지 않고 더했음), 그 결과를 중간 암호문의 앞에 배열하는 것이다. 이리하여 완성된 암호문을 다섯 자리씩 간격을 두어 나열하면, '**no attack**'은 다음과 같은 암호로 바뀐다. (㉢) **02451 23301 72.**

일본 정보부에서는 클라우젠이 만든 암호문들을 전쟁이 끝나도록 풀지 못했다. 사용된 암호화 과정이 워낙 정교한데다 평범한 책을 활용했기 때문이다. 클라우젠의 가택 수색에서도 별다른 주위를 끌지 못했던 연감이 실마리였다는 사실을 일본은 눈치 채지 못했다.

47. 다음 중 모스크바와 클라우젠 사이에 암호 해독을 위하여 사전에 약속된 것으로 보기 어려운 것은?

① 연감에서 선택한 숫자의 위치
② 1935년 <독일 제국 연감>을 활용
③ 빈도가 높은 알파벳으로 선택된 것들
④ 암호문과 해독의 열쇠를 더하는 방법
⑤ 빈도가 높지 않은 알파벳에 숫자를 매기는 순서

48. 다음 중 ㉠과 가장 유사한 암호 작성 방법은?

① 토마스 제퍼슨은 '제퍼슨 바퀴'라는 암호 제조기를 발명하였는데, 이것은 기존의 철자를 다른 철자로 바꾸는 방법을 이용하였다. a, b, c가 F, X, Y로 바뀔 수도 있다.
② 교황의 대사들은 나름대로의 암호를 고안해 냈다. 헤이그의 대사는 MUSEUM을 '바티칸' 대신에 사용했고 비엔나의 대사는 숫자를 이용했다. **7690**은 '나폴레옹'을 가리켰다.
③ 셰익스피어의 작품들은 프란시스 베이컨이 썼을 것이라는 의혹이 제기된 적이 있다. 그렇다면 작품 어디엔가는 'Bacon'이라는 글자가 존재할 것이다. 파비언은 <사랑의 헛소동> 4막 3장에서, 각 줄의 첫 한두 글자를 따보면, 'B CO AN'이 나온다고 주장하였다.
④ 1943년, 일본의 전쟁 포로 수용소에서 한 사무실로 편지가 왔다. 일본의 검열에도 걸리지 않았지만 FBI에서는 이 편지에 특별한 사연이 있을 것으로 짐작했다. 편지의 각 줄마다 맨 앞에 있는 두 단어만 뽑았더니 다음과 같은 문장이 되었다. "After Surrender fifty percent Americans lost in Philippines in Nippon 30%."

⑤ ISBN 코드는 네 부분이다. '89-89422-42-6'에서 89는 대한민국을 의미하고 89422는 출판사의 고유번호이며 42는 출판사에서 붙인 책의 고유번호이다. 네 번째는 0부터 9까지이며, 10을 쓸 때에는 로마숫자 X를 사용한다. 이 번호는 검사를 위한 수이다. 원래 번호를 쓰고 그 아래에 1부터 10까지를 거꾸로 쓴 다음, 위아래 숫자를 곱해서 이것들을 모두 더하면 11로 나누어지는 숫자가 되어야 한다.

49. 다음 중 ㉡의 이유로 적절한 것은?

① 연감의 통계 수치를 정확하게 보고하기 위하여
② 제3자의 암호 해독 과정을 혼란스럽게 하기 위하여
③ 송신자의 암호문 전문을 다른 코드로 전환하기 위하여
④ 송신자가 정보를 보낼 때 전달 내용의 혼동을 피하기 위하여
⑤ 수신자가 같은 책에서 정확한 열쇠를 뽑아낼 수 있도록 하기 위하여

50. 다음 중 ㉢에 들어갈 숫자에 해당하는 것은?

① 02451 ② 30516 ③ 34236 ④ 36687 ⑤ 72945

- 정답: 47.① 48.① 49.⑤ 50.④

◆ 05-6평 57~60번

[57 ~60] 다음 글을 읽고 물음에 답하시오.

(가) 인터넷 쇼핑몰에서 물건을 살 때, 다른 사람이 내 컴퓨터와 인터넷 쇼핑몰의 컴퓨터 사이에 오고가는 정보를 읽어서 내가 입력한 신용 카드 정보를 ㉠ 빼내면 어쩌나 하고 걱정하는 사람이 많다. 그러나 공개키 암호화 방식을 이용하면 정보를 주고받는 당사자 이외에는 그 정보를 볼 수 없도록 할 수 있다.

(나) 공개키 암호화 방식에서는 각각의 컴퓨터가 다른 컴퓨터와 절대로 겹치는 법이 없는 한 쌍의 키를 준비한다. 내 컴퓨터가 준비한 키 쌍을 각각 공개키 A와 비밀키 a라고 하자. 공개키 A는 다른 컴퓨터에 알려주는 데에 사용하고 비밀키 a는 내 컴퓨터에만 보관한다. 공개키 A로 암호화된 정보는 오직 비밀키 a가 있어야만 해독되어 원래의 정보로 만들 수 있으며, 공개키 A를 가지고도 해독될 수 없다. 따라서 비밀키 a만 내 컴퓨터 밖으로 빠져나가지 않게 하면 공개키 A는 다른 컴퓨터에 알려 주어도 무방하다.

(다) 이제 인터넷 서점 '책마을'에 접속하여 책을 구매하는 경우를 생각해 보자. 책마을 컴퓨터가 공개키 B와 비밀키 b를 가지고 있다고 하면, 내 컴퓨터가 책마을 컴퓨터에 접속하자마자 두 컴퓨터는 자동적으로 자신들의 공개키를 교환한다. 즉 내 컴퓨터는 B를, 책마을 컴퓨터는 A를 알게 되는 것이다. 이제 내가 책을 주문하기 위해서 신용 카드 정보를 내 컴퓨터에 입력하면 내 컴퓨터는 이것을 책마을 컴퓨터의 공개키 B로 암호화하여 전송한다. 책마을 컴퓨터는 암호화된 정보를 자신의 비밀키 b로 해독하여 원래의 신용 카드 정보를 얻는다. 공개키 B로 암호화하여 보내진 정보는 비밀키 b를 갖고 있는 책마을 컴퓨터만 해독할 수 있으므로 다른 사람이 내 신용 카드 정보를 해독하기는 불가능하다.

(라) 내 컴퓨터의 공개키 A는 다른 컴퓨터에서도 알 수 있으므로 다른 사람이 나인 척하고 자기 컴퓨터에서 공개키 A를 알려주고 책을 주문한다면 곤란한 문제가 발생할 수 있다. 이러한 문제를 방지하기 위해서는 책마을 컴퓨터가 받고 있는 정보의 송신자가 내 컴퓨터라는 것을 확인해야 한다. 이를 위해서 책마을 컴퓨터는 내 컴퓨터에 '책마을만세'와 같은 임의의 단어를 보내면서 이 단어를 내 컴퓨터의 비밀키 a로 암호화한 후, 원래 단어와 암호화된 단어를 함께 보내달라고 요구한다. 공개키 암호화 방식에서는 비밀키 a로 암호화된 정보가 공개키 A로만 해독이 가능하다. 따라서 ㉡ 내 컴퓨터는 원래의 단어와 암호화된 단어를 함께 전송하고, 이 두 정보를 전송 받은 책마을 컴퓨터는 암호화된 단어를 공개키 A로 해독한 후에 전송 받은 원래 단어와 일치하는지 확인한다. 만약 이들이 일치한다면 공개키 A를 가진 컴퓨터(내 컴퓨터)가 보낸 정보임에 틀림없다는 것을 알 수 있다.

(마) 어떤 사람은 자기 컴퓨터가 가르쳐 준 공개키 A에서 비밀키 a를 알아내면 어쩌나 하고 걱정할지 모른다. 그러나 이러한 일은 기술적으로만 본다면 거의 불가능하다. 비밀키 a에서는 간단한 계산만으로 공개키 A를 얻을 수 있다. 그러나 공개키 A에서 비밀키 a를 구하기 위해서는 현재 가장 속도가 빠른 슈퍼컴퓨터를 동원하더라도 수십 년 동안 계산해야 할 정도로 엄청난 시간을 필요로 한다. 따라서 공개키 암호화 방식은 일반적으로 사람들이 안심하고 사용해도 좋다고 할 수 있다.

57. 각 단락의 중심 화제로 적절하지 않은 것은? [1점]

① (가): 공개키 암호화 방식의 효용성
② (나): 공개키와 비밀키를 생성하는 방법
③ (다): 공개키 암호화 방식의 동작 원리
④ (라): 송신자 컴퓨터를 확인하는 원리
⑤ (마): 공개키 암호화 방식의 안전성

58. 위 글에 나타난 '공개키 암호화 방식'에 대한 설명으로 가장 적절한 것은?

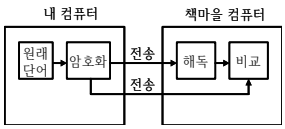
① 정보를 주고받는 컴퓨터끼리는 공통의 비밀키를 사용한다.
② 공개키로 암호화하여 보내는 정보는 비밀키로 해독될 수 없다.
③ 컴퓨터의 속도가 빨라지면 공개키 암호화의 안전성은 높아진다.
④ 정보를 주고받는 컴퓨터끼리는 상대방 컴퓨터의 비밀키를 모르고 있다.
⑤ 공개키로 암호화된 정보는 암호화에 사용된 공개키를 알면 해독될 수 있다.

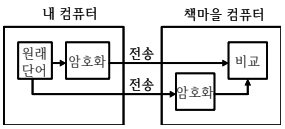
59. 국어 사전에서 ㉠의 의미를 바르게 찾은 것은? [1점]

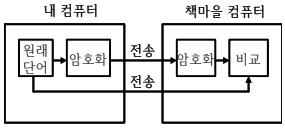
> **빼-내다**[빼:--] 〔-내어(-내), -내니〕동 (…에서 …을) (1) 박혀 있거나 끼워져 있는 것을 뽑다. (2) 여럿 가운데에서 필요한 것 혹은 불필요한 것만을 골라내다. (3) 남의 물건 따위를 돌려내다. (4) 남을 꾀어서 나오게 하다. (5) 얽매인 사람을 자유롭게 해 주다.

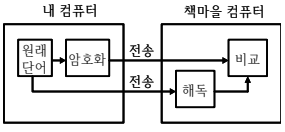
① (1) ② (2) ③ (3) ④ (4) ⑤ (5)

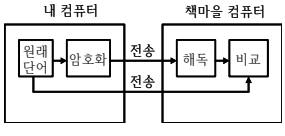
60. ㉡의 내용을 그림으로 올바르게 표현한 것은? [3점]

①


②


③


④


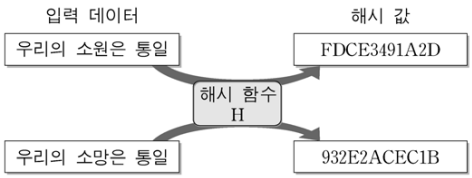
⑤


- 정답: 57.② 58.④ 59.③ 60.⑤

◆ 16-6평 16~18번

[16~18] 다음 글을 읽고 물음에 답하시오.

온라인을 통한 통신, 금융, 상거래 등은 우리에게 편리함을 주지만 보안상의 문제도 안고 있는데, 이런 문제를 해결하기 위하여 암호 기술이 동원된다. 예를 들어 전자 화폐의 일종인 비트코인은 해시 함수를 이용하여 화폐 거래의 안전성을 유지한다. 해시 함수란 입력 데이터 x에 대응하는 하나의 결과 값을 일정한 길이의 문자열로 표시하는 수학적 함수이다. 그리고 입력 데이터 x에 대하여 해시 함수 H를 적용한 수식을 H(x)=k라 할 때, k를 해시 값이라 한다. 이때 해시 값은 입력 데이터의 내용에 미세한 변화만 있어도 크게 달라진다. 현재 여러 해시 함수가 이용되고 있는데, 해시 값을 표시하는 문자열의 길이는 각 해시 함수마다 다를 수 있지만 특정 해시 함수에서의 그 길이는 고정되어 있다.



[해시 함수의 입·출력 동작의 예]

이러한 특성을 갖고 있기 때문에 해시 함수는 데이터의 내용이 변경되었는지 여부를 확인하는 데 이용된다. 가령, 상호 간에 동일한 해시 함수를 사용한다고 할 때, 전자 문서와 그 문서의 해시 값을 함께 전송하면 상대방은 수신한 전자 문서에 동일한 해시 함수를 적용하여 결과 값을 얻은 뒤 전송받은 해시 값과 비교함으로써 문서가 변경되었는지 확인할 수 있다.

그런데 해시 함수가 ㉠일방향성과 ㉡충돌회피성을 만족시키면 암호 기술로도 활용된다. 일방향성이란 주어진 해시 값에 대응하는 입력 데이터의 복원이 불가능하다는 것을 말한다. 특정 해시 값 k가 주어졌을 때 H(x)=k를 만족시키는 x를 계산하는 것이 매우 어렵다는 것이다. 그리고 충돌회피성이란 특정 해시 값을 갖는 서로 다른 데이터를 찾아내는 것이 현실적으로 불가능하다는 것을 의미한다. 서로 다른 데이터 x, y에 대해서 H(x)와 H(y)가 각각 도출한 값이 동일하면 이것을 충돌이라 하고, 이때의 x와 y를 충돌쌍이라 한다. 충돌회피성은 이러한 충돌쌍을 찾는 것이 현재 사용할 수 있는 모든 컴퓨터의 계산 능력을 동원하더라도 그것을 완료하기가 사실상 불가능하다는 것이다.

[가] 해시 함수는 온라인 경매에도 이용될 수 있다. 예를 들어 ○○ 온라인 경매 사이트에서 일방향성과 충돌회피성을 만족시키는 해시 함수 G가 모든 경매 참여자와 운영자에게 공개되어 있다고 하자. 이때 각 입찰 참여자는 자신의 입찰가를 감추기 위해 논스*의 해시 값과, 입찰가에 논스를 더한 것의 해시 값을 함께 게시판에 게시한다. 해시 값 게시 기한이 지난 후 각 참여자는 본인의 입찰가와 논스를 운영자에게 전송하고 운영자는 최고 입찰가를 제출한 사람을 낙찰자로 선정한다. 이로써 온라인 경매 진행 시 발생할 수 있는 다양한 보안상의 문제를 해결할 수 있다.

* 논스: 입찰가를 추측할 수 없게 하기 위해 입찰가에 더해지는 임의의 숫자.

16. 윗글의 '해시 함수'에 대한 이해로 적절하지 <u>않은</u> 것은?

① 전자 화폐를 사용한 거래의 안전성을 위해 해시 함수가 이용될 수 있다.
② 특정한 해시 함수는 하나의 입력 데이터로부터 두 개의 서로 다른 해시 값을 도출하지 않는다.
③ 입력 데이터 x를 서로 다른 해시 함수 H와 G에 적용한 H(x)와 G(x)가 도출한 해시 값은 언제나 동일하다.
④ 입력 데이터 x, y에 대해 특정한 해시 함수 H를 적용한 H(x)와 H(y)가 도출한 해시 값의 문자열의 길이는 언제나 동일하다.
⑤ 발신자가 자신과 특정 해시 함수를 공유하는 수신자에게 어떤 전자 문서와 그 문서의 해시 값을 전송하면 수신자는 그 문서의 변경 여부를 확인할 수 있다.

17. 윗글의 ㉠과 ㉡에 대하여 추론한 내용으로 가장 적절한 것은?

① ㉠을 지닌 특정 해시 함수를 전자 문서 x, y에 각각 적용하여 도출한 해시 값으로부터 x, y를 복원할 수 없다.
② 입력 데이터 x, y에 특정 해시 함수를 적용하여 도출한 문자열의 길이가 같은 것은 해시 함수의 ㉠ 때문이다.
③ ㉡을 지닌 특정 해시 함수를 전자 문서 x, y에 각각 적용하여 도출한 해시 값의 문자열의 길이는 서로 다르다.
④ 입력 데이터 x, y에 특정 해시 함수를 적용하여 도출한 해시 값이 같은 것은 해시 함수의 ㉡ 때문이다.
⑤ 입력 데이터 x, y에 대해 ㉠과 ㉡을 지닌 서로 다른 해시 함수를 적용하였을 때 도출한 결과 값이 같으면 이를 충돌이라고 한다.

18. [가]에 따라 <보기>의 사례를 이해한 내용으로 가장 적절한 것은? [3점]

<보 기>

온라인 미술품 경매 사이트에 회화 작품 △△이 출품되어 A와 B만이 경매에 참여하였다. A, B의 입찰가와 해시 값은 다음과 같다. 단, 입찰 참여자는 논스를 임의로 선택한다.

입찰 참여자	입찰가	논스의 해시 값	'입찰가+논스'의 해시 값
A	a	r	m
B	b	s	n

① A는 a, r, m 모두를 게시 기한 내에 운영자에게 전송해야 한다.
② 운영자는 해시 값을 게시하는 기한이 마감되기 전에 최고가 입찰자를 알 수 없다.
③ m과 n이 같으면 r과 s가 다르더라도 A와 B의 입찰가가 같다는 것을 의미한다.
④ A와 B 가운데 누가 높은 가격으로 입찰하였는지는 r과 s를 비교하여 정할 수 있다.
⑤ B가 게시판의 m과 r을 통해 A의 입찰가 a를 알아낼 수도 있으므로 게시판은 비공개로 운영되어야 한다.

- 정답: 16.③ 17.① 18.②

◆ 19년 7월 고3 33~37번

[33~37] 다음 글을 읽고 물음에 답하시오.

온라인 전자 상거래나 공인 인증이 일상화되면서 보안을 위해 메시지를 암호화하여 주고받는 암호통신의 중요성이 강조되고 있다. 암호통신에서 가장 핵심적인 문제 중 하나는 메시지를 암호화하거나 이를 다시 원래의 메시지로 복호화하는 데 필요한 키를 암호통신의 대상자인 송·수신자가 어떻게 안전하게 주고받느냐에 대한 것이다. 이러한 암호통신은 암호화나 복호화에 필요한 키를 관리하는 방식에 따라 크게 ㉠ 대칭키 방식과 ㉡ 공개키 방식으로 구분된다.

대칭키 방식은 메시지를 암호화하거나 복호화할 때 동일한 키를 사용한다. 이러한 이유로 송신자와 수신자만 아는 비밀키를 미리 분배하고 사용하는 과정에서 키 정보가 유출될 가능성이 높아 암호통신을 시도할 때마다 상대에 따라 새로운 비밀키를 사용해야 한다. 이에 반해 공개키 방식은 암호화 키와 복호화 키가 서로 다른 방식이다. 수신자가 미리 생성하여 공개한 공개키(public key)로 송신자가 메시지를 암호화하여 전송하면 수신자는 공개키에 대응하여 생성한, 자신만 알고 있는 비밀키(private key)를 이용하여 복호화한다. 공개키 방식은 별도의 비밀키 분배 과정이 필요 없고 통신 상대에 따라 비밀키를 바꿀 필요도 없어 대칭키 방식에 비해 보안에 유리하다.

대표적인 공개키 방식인 RSA 알고리즘은 큰 소수의 곱과 추가 연산을 통해 만들어진 정수의 소인수 분해가 매우 어렵다는 점에 기반하여 한 쌍의 공개키와 비밀키를 생성한다. 키를 만드는 연산 과정이 복잡하여 대칭키 방식에 비해 암호화나 복호화 속도가 상대적으로 느리지만 암호화된 문서가 유출되어도 현재의 컴퓨터 성능으로는 비밀키를 유추하는 데 비현실적으로 오랜 시간이 걸리기 때문에 비밀키를 바꿀 필요가 없다. 하지만 컴퓨터 연산 속도가 급격하게 발전하게 되면 복잡한 연산 과정을 기반으로 한 공개키 방식의 암호 체계가 위협받을 가능성이 높아질 수 있다.

그래서 최근 수학적 복잡성에 의존하지 않으면서도 도청으로부터 비밀키를 안전하게 나누어 가질 수 있는 ㉢ 양자암호통신 기술이 주목받고 있다. 양자암호통신에서는 매번 새롭게 만들어지는 비밀키를 안전하게 나누어 갖기 위해 양자의 종류 중 하나인 광자의 물리적 특성을 이용한다. 원자나 분자 단위 이하의 미시 세계를 다루는 양자 역학에서 광자는 더 이상 나눌 수 없는 최소 단위이기 때문에 광자 하나하나에 정보를 실어 보내는 양자암호통신에서 단일광자에 실린 정보의 일부만을 가로채는 것은 불가능하다. 또한 도청자가 단일광자 자체를 가로챈다 하더라도 수신자에게 가로챈 광자와 동일한 상태의 광자를 보내야만 도청 사실을 숨길 수 있는데 여러 상태를 동시에 지니는 '중첩'이라는 양자의 특성 때문에 단일광자의 원래 상태를 정확히 측정해 보낼 수 없다. 이러한 이유들로 인해 양자암호통신은 도청으로부터 안전한 신호 전달이 가능하다.

양자암호통신의 대표적인 키 분배 기술로는 단일광자의 편광 상태에 정보를 실을 수 있는 BB84 프로토콜*을 들 수 있다. 자연 상태의 빛은 진행하는 방향과 수직인 모든 방향으로 진동하는 특성이 있는데, 진동 방향에 따라 빛을 선택적으로 통과시킬 수 있는 필터를 이용하면 특정한 방향으로 진동하는 빛을 만들 수 있다. 이러한 빛을 '편광'이라고 하며, 편광을 만들 때 이용하는 필터를 '편광필터'라고 한다. 그런데 편광된 광자 또한 여러 방향으로 진동하는 '중첩' 특성을 지니고 있다. 즉 편

광필터를 통과한 수직(↕)이나 수평(↔) 편광의 경우 대각(⤢)·역대각(⤡) 편광 특성도 지니고 있으며, 마찬가지로 편광필터를 통과한 대각이나 역대각 편광 또한 수직·수평 편광 특성을 동시에 지니고 있다. 따라서 수직이나 수평 편광을 ✚편광필터를 이용하여 측정하면 수직이나 수평 편광으로 100% 측정되지만, 수직이나 수평 편광을 ✖편광필터를 이용하여 측정하면 대각 혹은 역대각 편광으로 잘못 측정된다.

[A] 이러한 편광의 중첩 특성이 BB84 프로토콜에서 어떻게 이용되는지 알아보자.

(a) 송신자의 비트 정보	0	1	1	0	1	0
(b) 송신자의 편광필터	✚	✚	✖	✚	✖	✖
(c) 송신자의 편광 신호	↔	↕	⤡	↔	⤡	⤢
(d) 수신자의 편광필터	✚	✚	✖	✖	✚	✖
(e) 수신자의 측정 신호	↔	×	⤡	⤢	↕	⤢
(f) 비밀키 공유	0		1			0

※'×'는 누락된 광자.

BB84 프로토콜은 먼저 위 <표>의 (a)처럼 송신자가 무작위로 비트 정보를 생성하는 것으로 시작한다. 이때 BB84 프로토콜은 수직 편광과 역대각 편광은 '1'이라는 비트 정보로, 수평 편광과 대각 편광은 '0'이라는 비트 정보로 표시하기로 약속되어 있어 (b)처럼 송신자가 ✚편광필터와 ✖편광필터를 무작위로 선정하면 (c)와 같은 편광 신호들이 생성된다. 수신자는 (c)에서 생성된 편광 신호들이 어떤 편광인지 전혀 모르는 상태에서 (d)처럼 스스로 무작위로 편광필터를 선택하여 (e)와 같이 편광된 광자를 측정한다. 이때 전송 과정에서 잡음 등으로 인해 누락된 광자가 발생할 수 있으며, 누락된 광자는 측정에서 제외된다. 이후 송·수신자는 공개 채널에서 자신들이 어떤 편광필터를 어떤 순서로 사용했는지 서로 공유하면 (f)와 같이 동일한 편광필터를 사용한 '010'이라는 비트 정보만 걸러낼 수 있어 비밀키로 사용하는 측정값을 안전하게 공유할 수 있다.

* 프로토콜 : 통신 규약.

33. 다음은 윗글을 읽은 학생의 독서 기록 중 일부이다. 윗글을 참고할 때, '점검 결과'로 적절하지 <u>않은</u> 것은?

○ 읽기 계획 : 1문단을 훑어보면서 뒷부분을 예측하고 질문 만들기를 한 후 글을 읽고 점검하기

예측 및 질문 내용	점검 결과
○ 암호통신을 이용하여 온라인 전자 상거래가 이루어지는 과정을 보여 줄 것이다.	예측과 다름 ····· ①
○ 암호통신 방식에 따른 장단점을 비교하며 설명할 것이다.	예측과 같음 ····· ②
○ 암호화 키를 만드는 방법은 복호화 키를 만드는 방법과 어떠한 차이가 있을까?	질문의 답이 제시됨 ····· ③
○ 암호통신 방식에 따라 안전성을 확보하기 위한 방법은 어떻게 다를까?	질문의 답이 제시됨 ····· ④
○ 각각의 암호통신 방식이 실생활에 적용된 사례로는 어떤 것이 있을까?	질문의 답이 언급되지 않음 ····· ⑤

34. 윗글에 대한 이해로 적절하지 <u>않은</u> 것은?

① 공개키 방식에서 공개키와 비밀키를 생성하는 주체는 동일하겠군.
② 컴퓨터의 연산 능력이 발전하더라도 양자암호통신은 비밀키를 안전하게 나누어 가질 수 있겠군.
③ 양자암호통신에서는 도청자가 단일광자에 담긴 정보를 도청할 경우 수신자에게 도청 사실을 숨길 수 없겠군.
④ RSA 알고리즘에서 암호화된 문서가 전송 과정 중 유출되어도 수신자는 비밀키를 다시 생성할 필요가 없겠군.
⑤ RSA 알고리즘이 대칭키 방식에 비해 암·복호화 속도가 느린 이유는 서로 다른 암·복호화 키를 주고받기 때문이겠군.

35. ㉠~㉢을 비교한 내용으로 가장 적절한 것은?

① ㉠은 ㉡이나 ㉢에 비해 비밀키가 유출될 가능성이 낮다.
② ㉢은 ㉠이나 ㉡에 비해 수학적 복잡성에 더 많이 의존한다.
③ ㉠과 ㉡은 ㉢과 달리 비밀키를 나누어 갖는 과정이 필요하다.
④ ㉠과 ㉢은 ㉡과 달리 암호화를 위해 송신자가 비밀키를 알아야 한다.
⑤ ㉠, ㉡, ㉢은 모두 암호통신 상대의 수만큼 비밀키가 필요하다.

36. <u>BB84 프로토콜</u>에 대한 이해로 가장 적절한 것은?

① BB84 프로토콜은 안전한 비밀키를 사용하여 암·복호화를 하는 과정에 대한 통신 규약이다.
② BB84 프로토콜에 사용되는 수평 편광을 ✖편광필터로 측정하면 수평 편광으로 측정되지 않는다.
③ BB84 프로토콜 실행 과정에서 편광된 광자가 다시 편광필터를 통과하면 양자의 중첩 특성이 사라진다.
④ 광자는 더 이상 나눌 수 없기 때문에 BB84 프로토콜이 진행되는 동안 단일광자 자체를 가로챌 수 없다.
⑤ BB84 프로토콜에서 수직 편광은 대각 편광의 특성도 동시에 지니고 있어 '0'이라는 비트 정보로 표현한다.

37. BB84 프로토콜을 이용하여 송신자와 수신자가 <보기>와 같이 정보를 주고받았다. [A]를 참고했을 때 <보기>의 과정을 통해 생성되는 비밀키로 적절한 것은? [3점]

<보 기>

○ 송신자의 비트 정보 생성 및 편광된 광자 전송

비트 정보	0	1	0	0	1	1	1	0	1	0
편광필터 정보	0	1	1	0	1	0	1	1	1	0
편광 신호	↔	⤡	⤢	↔	⤡	↕	⤡	⤢	⤡	↔

○ 수신자의 광자 측정

편광필터 정보	1	1	0	1	1	0	0	1	1	1
측정한 신호	⤡	⤡	↕	⤡	×	↕	↔	⤢	⤡	⤢

* ✚편광필터 : 0, ✖편광필터 : 1, 누락된 광자 : ×

① 1011 ② 1100 ③ 1101 ④ 11011 ⑤ 11101

- 정답: 33.③ 34.⑤ 35.④ 36.② 37.③