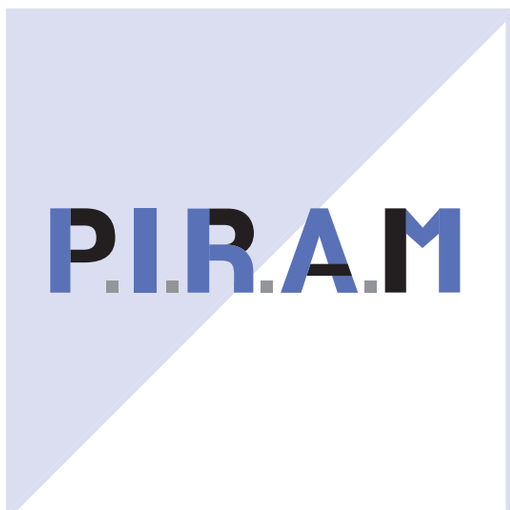

P.I.R.A.M

CONTENTS

'P.I.R.A.M 국어 생각의 전개'의 목차와 똑같이 구성했기 때문에, 2022학년도 수능 예시문항 및 2021학년도 수능 지문으로 이루어져 있던 M step은 제외되어 있습니다. 착오 없으시기 바랍니다!

교재의 사용법 004P

P(reliminar) step

5. 적용연습 008P

I(mprove) step

2. 비교/대조 026P
3. 시간순 서술 046P
4. 문제해결 054P
5. 과정과 비례/증감 관계 060P

R(einforce) step

1. 화제 중심으로 읽기 074P
2. 카테고리 만들며 읽기 090P

A(dvance) step

1. 필연적 문제풀이 104P
2. 제재별 독해 태도 110P

지문 목차 _ 생각 워크북 : 독서편

복습시 이용할 수 있도록 각 지문의 목차를 정리했습니다. 이 교재는 제재 구분 없이, 각 테마에 맞는 지문들이 모여 있습니다. 특정 제재 위주로 공부하거나 복습하시고 싶은 분들을 위해 어떤 제재인지도 적어두었습니다. 다양하게 활용하시기 바랍니다.

P(reliminar) step

5. 적용연습

[인문] 2015.06AB [16~19] '작가주의' 008P
[예술] 2011.11 [21~24] '체계 이론 미학' 010P
[인문] 2011.09 [44~47] '공리주의' 012P
[인문] 2016.09B [17~20] '설명 이론' 014P
[과학] 2014.09A [16~18] '동물의 길찾기' 016P
[기술] 2015.06A [26~27] '원유의 열처리' 018P
[인문] 2012.11 [17~20] '비트겐슈타인' 019P
[과학] 2015.11A [16~19] '단백질 합성&분해' 020P
[기술] 2016.09A [16~18] '해시 함수' 022P

I(mprove) step

2. 비교/대조

[인문] 2011.06 [13~14] '추론' 026P
[인문] 2014.09B [17~20] '주희&정약용' 028P
[예술] 2011.09 [39~43] '고대 그리스 음악' 030P
[인문] 2014.09A [26~27] '반실재론' 032P
[기술] 2011.11 [25~26] '소프트웨어 자료 관리' 033P
[인문] 2013.11 [21~24] '논증' 034P
[인문] 2014.06B [17~20] '본질' 036P
[인문] 2014.11B [19~21] '심신 이원론&일원론' 038P
[인문] 2015.11AB [27~30] '취미 판단 이론' 040P
[인문] 2016.11B [17~20] '도덕적 운' 042P
[인문] 2017.06 [20~24] '유비 논증' 044P

3. 시간순 서술

[인문] 2013.06 [19~22] '역사' 046P
[과학] 2011.09 [19~20] '시간&공간' 048P
[인문] 2015.09A [26~30] '법과 정의의 관계' 050P
[과학] 2014.11A [16~18] '분광 분석법' 052P

4. 문제해결

[사회(정치)] 2013.06 [47~50] '민주주의 대표 체계' 054P
[인문] 2016.11A [22~26] '귀납의 문제' 056P
[사회(경제)] 2012.09 [35~37] '자원 배분의 효율성' 058P

5. 과정과 비례/증감 관계

[기술] 2012.09 [47~50] '디지털 피아노' 060P
[과학] 2015.06B [25~26] '별의 밝기' 062P
[기술] 2015.11A [20~22] '디지털 영상' 064P
[과학] 2014.11B [26~27] '전향력' 066P
[기술] 2014.06A [19~21] '플래시 메모리' 068P
[기술] 2011.06 [36~38] '연비' 070P

R(einforce) step

1. 화제 중심으로 읽기

[인문] 2011.11 [17~20] '자산의 개혁' 074P
[인문] 2016.11B [21~24] '지식 경영' 076P
[인문] 2012.09 [21~23] '데카르트 좌표계' 078P
[예술] 2018.09 [16~19] '하이퍼리얼리즘' 080P
[인문] 2018.11 [16~19] '목적론' 082P
[과학] 2014.06B [28~29] '단안 단서' 084P
[과학] 2016.06A [19~21] '원자의 모형' 085P
[인문+예술] 2020.09 [21~26] '사료&영화' 086P

2. 카테고리 만들며 읽기

[예술] 2014.11A [19~21] '승선교' 090P
[사회] 2016.09A [22~26] '경쟁 정책&소비자 정책' 092P
[인문] 2020.06 [19~22] '에피쿠로스' 094P
[인문+예술] 2019.09 [33~38] '근대 도시의 삶의 양식' 096P
[과학] 2016.09B [25~26] '항암제' 098P
[과학] 2011.06 [15~18] '사막' 100P

A(dvance) step

1. 필연적 문제풀이

[예술+기술] 2017.06 [28~33] '음악적 아름다움' 104P
[과학] 2014.09B [28~29] '각운동량 보존 법칙' 107P
[과학] 2015.11B [25~26] '천체 현상의 원인' 108P

2. 제재별 독해 태도

[기술] 2013.09 [17~19] '포토리소그래피' 110P
[기술] 2013.06 [44~46] '하드 디스크' 112P
[기술] 2011.09 [48~50] '가스 센서' 114P
[사회(경제)] 2012.11 [29~30] '외부성' 116P
[사회(경제)] 2011.09 [28~31] '환율&경상 수지' 118P
[사회(법)] 2014.09AB [22~25] '소송' 120P
[사회(법)] 2014.06A [28~29] '입증 책임' 122P

[20~21] 다음 글을 읽고 물음에 답하시오. 2015.06A [26~27]

(해설 p.021)

우유는 인간에게 양질의 영양소를 공급하는 식품이다. 하지만 아무런 처리를 하지 않은 우유, 즉 원유를 가공하지 않고 그대로 유통하게 되면 부패나 질병을 유발하는 유해 미생물이 빠르게 증식할 위험이 있다. 그렇기 때문에 평소에 우리가 마시는 우유는 원유를 열처리하여 미생물을 제거한 것이다.

원유를 열처리하게 되면 원유에 포함되어 있는 미생물의 개체 수가 줄어드는데, 일반적으로 가열 온도가 높을수록 가열 시간이 길수록 그 수는 더 많이 감소한다. 그런데 미생물의 종류에 따라 미생물을 제거하는 데 필요한 시간과 온도가 다르기 때문에 적절한 열처리 조건을 알아야 한다. 이때 D값과 Z값을 이용한다. D값은 어떤 미생물을 특정 온도에서 열처리할 때 그 개체 수를 1/10로 줄이는 데 걸리는 시간을 말한다. 만약 같은 온도에서 개체 수를 1/100로 줄이고자 한다면 D값의 2배의 시간으로 처리하면 된다. Z값은 특정 D값의 1/10 만의 시간에 개체 수를 1/10로 줄이는 데 추가적으로 높여야 하는 온도를 말한다. 그렇기 때문에 열에 대한 저항성이 큰 미생물일수록 특정 온도에서의 D값과 Z값이 크다. 예를 들어, 어떤 미생물 100개를 63℃에서 열처리한다고 하자. 이때 360초 후에 남아 있는 개체 수가 10개라면 D값은 360초가 된다. 만약 이 D값의 1/10인 36초 만에 미생물의 개체 수를 100개에서 10개로 줄이고자 할 때의 온도가 65℃라면 Z값은 2℃가 된다.

이러한 D값과 Z값의 원리에 기초하여 원유를 열처리하는 여러 가지 방법이 개발되었다. 먼저, 원유를 63℃에서 30분간 열처리하여 그 안에 포함된 미생물을 99.999% 이상 제거하는 '저온살균법'이 있다. 저온살균법은 미생물을 제거하는 데는 효과적이나 시간이 오래 걸린다는 단점이 있다. 이를 보완하기 위해 개발된 방법이 '저온순간살균법'이다. 저온순간살균법은 원유를 75℃에서 15초간 열처리하는 방법이다. 이 방법은 미생물 제거 효과가 저온살균법과 동일하지만 우유의 대량 생산을 위해 열처리 온도를 높여서 열처리 시간을 단축시킨 것이다.

저온살균법이나 저온순간살균법으로 처리한 우유의 유통 기간은 냉장 상태에서 5일 정도이다. 만약 우유의 유통 기간을 늘리려면, 저온살균법이나 저온순간살균법으로 처리해도 죽지 않는 미생물까지도 제거해야 한다. 열에 대한 저항성이 큰 종류의 미생물까지 제거하기 위해서는 134℃에서 2~3초간 열처리하는 '초고온처리법'을 사용한다. 이렇게 처리된 우유를 멸균 포장하면 상온에서 1개월 이상의 장기 유통이 가능하다.

20 윗글을 통해 알 수 있는 내용으로 적절하지 <u>않은</u> 것은?

① 원유는 부패나 질병을 유발하는 유해 미생물이 성장하기에 좋은 조건을 가지고 있다.
② 우유의 유통 기간을 1개월 이상으로 늘리려면 원유를 초고온처리법으로 열처리해야 한다.
③ 열처리 시간이 같다면 원유에서 더 많은 수의 미생물을 제거하기 위해서는 열처리 온도를 높여야 한다.
④ 원유를 저온살균법으로 열처리하면 대부분의 미생물은 제거되지만 열에 대한 저항성이 큰 미생물은 제거되지 않는다.
⑤ 초고온처리법을 사용하면 저온순간살균법을 사용할 때보다 원유를 열처리한 후 제거되지 않고 남는 미생물의 개체 수가 많다.

21 윗글을 고려할 때, 〈보기〉와 같은 조건에서의 열처리에 대한 설명으로 적절한 것은? [3점]

[보기]

같은 양의 원유가 담긴 세 개의 병이 있다. 이 중 한 병에는 미생물 A, 또 다른 병에는 미생물 B, 나머지 한 병에는 미생물 C가 각각 1,000개씩 들어 있다고 가정하자. 각 미생물의 열처리 온도 및 그 온도에서의 D값과 Z값은 다음과 같다.

A : 60℃에서의 D값은 50초이고, Z값은 10℃
B : 60℃에서의 D값은 50초이고, Z값은 5℃
C : 65℃에서의 D값은 50초이고, Z값은 5℃

① A, B가 들어 있는 원유를 60℃에서 100초 동안 열처리하면, A와 B의 남은 개체 수는 각각 10개씩 된다.
② A, B가 들어 있는 원유를 65℃에서 같은 시간 동안 열처리하면, A의 개체 수는 B의 개체 수보다 더 적다.
③ A, B가 들어 있는 원유를 70℃에서 열처리하면, B는 A에 비해 더 오랜 시간 견딜 수 있다.
④ A, C가 들어 있는 원유를 70℃에서 5초 동안 열처리하면, A의 개체 수는 C의 개체 수보다 더 적다.
⑤ B가 들어 있는 원유를 65℃에서 5초 동안, C가 들어 있는 원유를 70℃에서 5초 동안 열처리하면, B와 C의 남은 개체 수는 각각 10개씩 된다.

[22~25] 다음 글을 읽고 물음에 답하시오. 2012.11 [17~20]

(해설 p.023)

비트겐슈타인이 1918년에 쓴 『논리 철학 논고』는 '빈학파'의 논리실증주의를 비롯하여 20세기 현대 철학에 큰 영향을 주었다. 그는 많은 철학적 논란들이 언어를 애매하게 사용하여 발생한다고 보았기 때문에 언어를 분석하고 비판하여 명료화하는 것을 철학의 과제로 삼았다.

그는 이 책에서 언어가 세계에 대한 그림이라는 '그림 이론'을 주장한다. 이 이론을 세우는 데 그에게 영감을 주었던 것은, 교통사고를 다루는 재판에서 장난감 자동차와 인형 등을 이용한 ㉠ 모형을 통해 ㉡ 사건을 설명했다는 기사였다. 그런데 모형을 가지고 사건을 설명할 수 있는 이유는 무엇일까? 그것은 모형이 실제의 자동차와 사람 등에 대응하기 때문이다. 그는 언어도 이와 같다고 보았다. 언어가 의미를 갖는 것은 언어가 세계와 대응하기 때문이다. 다시 말해 언어가 세계에 존재하는 것들을 가리키고 있기 때문이다. 언어는 명제들로 구성되어 있으며, 세계는 사태들로 구성되어 있다. 그리고 명제들과 사태들은 각각 서로 대응하고 있다. 이처럼 언어와 세계의 논리적 구조는 동일하며, 언어는 세계를 그림처럼 기술함으로써 의미를 가진다.

'그림 이론'에서 명제에 대응하는 '사태'는 '사실'이 아니라 사실이 될 수 있는 논리적 가능성을 의미한다. 따라서 언어를 구성하는 명제들은 사실적 그림이 아니라 논리적 그림이다. 사태가 실제로 일어나서 사실이 되면 그것을 기술하는 명제는 참이 되지만, 사태가 실제로 일어나지 않는다면 그 명제는 거짓이 된다. 어떤 명제가 '의미 있는 명제'가 되기 위해서는 그 명제가 실재하는 대상이나 사태에 대해 언급해야 하며, 그것에 대해서는 참, 거짓을 따질 수 있다. 만약 어떤 명제가 실재하지 않는 대상이나 사태가 아닌 것에 대해 언급하면 그것은 '의미 없는 명제'가 되며, 그것에 대해 참, 거짓을 따질 수 없다. 따라서 경험적 세계에 대해 언급하는 명제만이 의미 있는 것이 된다.

이러한 관점에서 비트겐슈타인은 기존의 철학자들이 다루었던 신, 영혼, 형이상학적 주체, 윤리적 가치 등과 관련된 논의가 의미 없는 말들에 불과하다고 보았다. 왜냐하면 그 말들이 가리키는 대상이 세계 속에 존재하지 않는, 즉 경험 가능하지 않은 대상이기 때문이다. 이와 같은 형이상학적 문제와 관련된 명제나 질문들은 의미가 없는 말들이다. 그러한 문제는 우리의 삶을 통해 끊임없이 드러나는 신비한 것들이지만 이에 대해 말로 답변하거나 설명할 수는 없다. 그래서 비트겐슈타인은 "말할 수 없는 것에 대해서는 침묵해야 한다."라고 말했다.

22 비트겐슈타인의 이론에 대한 이해로 적절하지 <u>않은</u> 것은?

① 언어의 문제를 철학의 중요한 과제로 보았다.
② '그림 이론'으로 논리실증주의에 큰 영향을 주었다.
③ '사태'와 '사실'의 개념을 구별하였다.
④ 경험적 대상을 언급하는 명제는 참이라고 보았다.
⑤ 형이상학적 문제를 다룬 기존 철학을 비판하였다.

23 윗글의 '의미 없는 명제'에 해당하는 것은?

① 곰팡이는 생물의 일종이다.
② 물은 1기압에서 90℃에 끓는다.
③ 피카소는 1881년 스페인에서 태어났다.
④ 우리 반 학생의 절반 이상이 헌혈을 했다.
⑤ 선생님은 한평생 바람직한 삶을 살아왔다.

24 ㉠ : ㉡의 관계에 해당하는 것만을 〈보기〉에서 있는 대로 고른 것은?

[보기]

ㄱ. 언어 : 세계
ㄴ. 명제 : 사태
ㄷ. 논리적 그림 : 의미 있는 명제
ㄹ. 형이상학적 주체 : 경험적 세계

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

25 윗글로 미루어 볼 때, 비트겐슈타인이 〈보기〉와 같이 말한 이유로 가장 적절한 것은? [3점]

[보기]

사다리를 딛고 올라간 후에 그 사다리를 던져 버리듯이, 『논리 철학 논고』를 이해한 사람은 거기에 나오는 내용을 버려야 한다. ㉮ <u>이 책의 내용</u>은 의미 있는 언어의 한계를 넘어선 것이기 때문에 엄밀하게 보면 '말할 수 있는 것'의 범주에 속하지 않는다.

① ㉮는 자신이 내세웠던 철학의 과제를 넘어서는 주제들을 다루고 있기 때문이다.
② ㉮는 객관적 세계에 존재하는 대상을 과학적으로 분석하여 서술하고 있기 때문이다.
③ ㉮는 실재하는 대상이 아니라 논리적으로 가능한 사태에 대해 기술하고 있기 때문이다.
④ ㉮는 경험적 세계가 아니라 언어와 세계의 논리적 관계에 대해 언급하고 있기 때문이다.
⑤ ㉮는 기존의 철학자들이 다루었던 형이상학적 물음에 대해 관념적으로 답하고 있기 때문이다.

[26~29] 다음 글을 읽고 물음에 답하시오. 2015.11A [16~19]

(해설 p.027)

우리 몸은 단백질의 합성과 분해를 끊임없이 반복한다. 단백질 합성은 아미노산을 연결하여 긴 사슬을 만드는 과정인데, 20여 가지의 아미노산이 체내 단백질 합성에 이용된다. 단백질 합성에서 아미노산들은 DNA 염기 서열에 담긴 정보에 따라 정해진 순서대로 결합된다. 단백질 분해는 아미노산 간의 결합을 끊어 개별 아미노산으로 분리하는 과정이다. 체내 단백질 분해를 통해 오래되거나 손상된 단백질이 축적되는 것을 막고, 우리 몸에 부족한 에너지 및 포도당을 보충할 수 있다.

단백질 분해 과정의 하나인, 프로테아솜이라는 효소 복합체에 의한 단백질 분해는 세포 내에서 이루어진다. 프로테아솜은 유비퀴틴이라는 물질이 일정량 이상 결합되어 있는 단백질을 아미노산으로 분해한다. 단백질 분해를 통해 생성된 아미노산의 약 75%는 다른 단백질을 합성하는 데 이용되며, 나머지 아미노산은 분해된다. 아미노산이 분해될 때는 아미노기가 아미노산으로부터 분리되어 암모니아로 바뀐 다음, 요소(尿素)로 합성되어 체외로 배출된다. 그리고 아미노기가 떨어지고 남은 부분은 에너지나 포도당이 부족할 때는 이들을 생성하는 데 이용되고, 그렇지 않으면 지방산으로 합성되거나 체외로 배출된다.

단백질이 지속적으로 분해됨에도 불구하고 체내 단백질의 총량이 유지되거나 증가할 수 있는 것은 세포 내에서 단백질 합성이 끊임없이 일어나기 때문이다. 단백질 합성에 필요한 아미노산은 세포 내에서 합성되거나, 음식으로 섭취한 단백질로부터 얻거나, 체내 단백질을 분해하는 과정에서 생성된다. 단백질 합성에 필요한 아미노산 중 체내에서 합성할 수 없어 필요량을 스스로 충족할 수 없는 것을 필수아미노산이라고 한다. 어떤 단백질 합성에 필요한 각 필수아미노산의 비율은 정해져있다. 체내 단백질 분해를 통해 생성되는 필수아미노산도 다시 단백질 합성에 이용되기도 하지만, 부족한 양이 외부로부터 공급되지 않으면 전체의 체내 단백질 합성량이 줄어들게 된다. 그러므로 필수아미노산은 반드시 음식물을 통해 섭취되어야 한다. 다만 성인과 달리 성장기 어린이의 경우, 체내에서 합성할 수는 있으나 그 양이 너무 적어서 음식물로 보충해야하는 아미노산도 필수아미노산에 포함된다.

각 식품마다 포함된 필수아미노산의 양은 다르며, 필수아미노산이 균형을 이룰수록 공급된 필수아미노산의 총량 중 단백질 합성에 이용되는 양의 비율, 즉 필수아미노산의 이용 효율이 ㉠높다. 일반적으로 육류, 계란 등 동물성 단백질은 필수아미노산을 균형 있게 함유하고 있어 필수아미노산의 이용 효율이 높은 반면, 쌀이나 콩류 등에 포함된 식물성 단백질은 제한아미노산을 가지며 필수아미노산의 이용 효율이 상대적으로 낮다.

제한아미노산은 단백질 합성에 필요한 각각의 필수아미노산의 양에 비해 공급된 어떤 식품에 포함된 해당 필수아미노산의 양의 비율이 가장 낮은 필수아미노산을 말한다. 가령, 가상의 P 단백질 1몰*을 합성하기 위해서는 필수아미노산 A와 B가 각각 2몰과 1몰이 필요하다고 하자. P를 2몰 합성하려고 할 때, A와 B가 각각 2몰씩 공급되었다면 A는 필요량에 비해 2몰이 부족하게 되어 P는 결국 1몰만 합성된다. 이때 A가 부족하여 합성할 수 있는 단백질의 양이 제한되기 때문에 A가 제한아미노산이 된다.

* 몰: 물질의 양을 나타내는 단위.

26 윗글의 내용과 일치하지 않는 것은?

① 체내 단백질의 분해를 통해 오래되거나 손상된 단백질의 축적을 막는다.
② 유비퀴틴이 결합된 단백질을 아미노산으로 분해하는 것은 프로테아솜이다.
③ 아미노산에서 분리되어 요소로 합성되는 것은 아미노산에서 아미노기를 제외한 부분이다.
④ 세포 내에서 합성되는 단백질의 아미노산 결합 순서는 DNA 염기 서열에 담긴 정보에 따른다.
⑤ 성장기의 어린이에게 필요한 필수아미노산 중에는 체내에서 합성할 수 있는 것도 포함되어 있다.

27 윗글을 읽고 이해한 내용으로 적절하지 <u>않은</u> 것은?

① 필수아미노산을 제외한 다른 아미노산도 제한아미노산이 될 수 있겠군.
② 체내 단백질을 분해하여 얻어진 필수아미노산의 일부는 단백질 합성에 다시 이용되겠군.
③ 체내 단백질 합성에 필요한 필수아미노산은 음식물의 섭취나 체내 단백질 분해로부터 공급되겠군.
④ 제한아미노산이 없는 식품은 단백질 합성에 필요한 필수아미노산이 균형 있게 골고루 함유되어 있겠군.
⑤ 체내 단백질 합성과 분해의 반복 과정에서, 외부로부터 필수아미노산의 공급이 줄어들면 체내 단백질 총량은 감소하겠군.

28 윗글을 바탕으로 할 때, 〈보기〉의 실험에 대한 이해로 적절하지 않은 것은? [3점]

[보기]

가상의 단백질 Q를 1몰 합성하는 데 필수아미노산 A, B, C가 각각 2몰, 3몰, 1몰이 필요하다고 가정하자. 단백질 Q를 2몰 합성하려고 할 때 (가), (나), (다)에서와 같이 A, B, C의 공급량을 달리하고, 다른 조건은 모두 동일한 상황에서 최대한 단백질을 합성하는 실험을 하였다.

(가) : A 4몰, B 6몰, C 2몰
(나) : A 6몰, B 3몰, C 3몰
(다) : A 4몰, B 3몰, C 3몰

(단, 단백질과 아미노산의 분해는 없다고 가정한다.)

① (가)에서는 단백질 합성을 제한하는 필수아미노산이 없겠군.
② (가)에서는 (다)에 비해 단백질 합성에 이용된 필수아미노산의 총량이 많겠군.
③ (나)에서는 (다)에 비해 합성된 단백질의 양이 많겠군.
④ (나)와 (다) 모두에서는 단백질 합성을 제한하는 필수아미노산이 B가 되겠군.
⑤ (나)에서는 (다)에 비해 단백질 합성에 이용되지 않고 남은 필수아미노산의 총량이 많겠군.

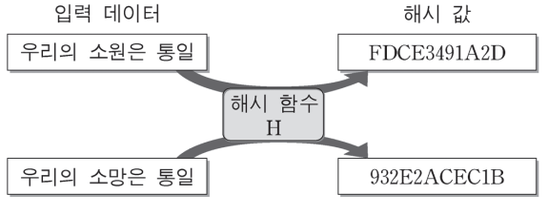
29 ㉠의 문맥적 의미와 가장 가까운 것은?

① 가을이 되면 그 어느 때보다 하늘이 <u>높다</u>.
② 우리나라는 원자재의 수입 의존도가 <u>높다</u>.
③ 이번에 새로 지은 건물은 높이가 매우 <u>높다</u>.
④ 잘못을 시정하라는 주민들의 목소리가 <u>높다</u>.
⑤ 친구는 이 분야의 전문가로서 이름이 <u>높다</u>.

[30~32] 다음 글을 읽고 물음에 답하시오. 2016.09A [16~18]

(해설 p.031)

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 특정해시 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.

30 윗글의 '해시 함수'에 대한 이해로 적절하지 않은 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.

31 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.

32 [가]에 따라 〈보기〉의 사례를 이해한 내용으로 가장 적절한 것은? [3점]

[보기]

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.

는 경우가 많습니다. 이런 선지도 쉽게 풀어낼 수 있어야 해요!

② (가)에서는 Q를 2몰 합성했고, (다)에서는 Q를 1몰만 합성했으니 단백질 합성에 이용된 필수아미노산은 (가)가 2배 많겠죠.

③ (나)와 (다) 둘 다 Q를 1몰만 합성했죠? (나)가 더 많을 리가 없습니다. 마지막 문단의 예시를 잘 이해하고, 〈보기〉 정리만 잘 했으면 아주 쉽게 답을 고를 수 있네요.

④⑤ 역시 미리 정리한 정보들이네요. 〈보기〉 문제 풀이는 〈보기〉 정리에서 시작한다는 것! 잊지 맙시다.

29 ②

선지	①	②	③	④	⑤
선택률	3%	79%	2%	15%	1%

| 핵심 point |

① 화제 check : 독서 독해의 처음이자 끝. 첫 문단에서 잡은 '화제'를 마지막 문단까지 놓지 않아야 합니다.

② 정보의 역할 : 모든 정보는 '화제'를 뒷받침하는 역할을 하고 있습니다. 이 '역할'을 바탕으로, 정보를 특정한 기준으로 카테고리화하며 읽는 것이 중요합니다.

③ 사례–원리 연결 : 모든 사례는 어떠한 원리를 이해시키기 위해 존재합니다. 독해 속도를 늦추면서 확실하게 '이해'하고 넘어갑시다.

④ 〈보기〉 정리 : 〈보기〉 문제를 해결할 때, 선지를 판단하기 전에 반드시 〈보기〉의 내용을 어느 정도 정리하는 것이 중요합니다.

[30~32] 2016.09A [16~18] ☆☆☆

> 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 함수**란 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.

'온라인을 통한 통신, 금융, 상거래' 등이 가지고 있는 '보안상 문제'에 대한 글입니다. '편리함'보다는 '문제'가 훨씬 중요하게 다뤄질 것이라는 느낌은 오시죠? 아무튼 이걸 '해결'하기 위해 '암호 기술'이 동원되는데, '비트코인' 예시를 통해 암호 기술의 일종인 '해시 함수'를 소개하고 있네요. 이제부터 '해시 함수'에 대해 이해할 것인데, 중요한 건 이게 '보안상의 문제'를 해결해주는 '암호 기술'이라는 생각을 갖고 있는 거예요! 그러니까 해시 함수를 이용하면 '화폐 거래의 안전성'을 유지할 수 있겠죠? '암호' 기술이니까요!

'해시 함수'는 어떠한 결과 값을 '일정한' 길이의 문자열로 표시하는 함수라고 하네요. 일단 고정된 값이 나왔으니 확실하게 인식해 주시는 것이 중요하겠죠? 해시 함수의 결과 값은 길이가 '일정'하다는 것이죠. 그리고 이 '결과 값'은 '해시 값'이라고 부른다고 합니다. '결과 값'과 '해시 값'의 정의가 같으니 같은 말이라고 인식할 수 있어야 합니다. 일종의 '재진술'이니까요. 아무튼 입력 데이터의 내용에 미세한 변화만 있어도 크게 달라지는 '해시 값'을 표시하는 '문자열의 길이'는 특정 해시 함수에서는 고정되어 있다고 합니다. 크게 달라지긴 하는데, 길이 자체는 '고정'되어 있네? 이런 생각을 해주는 게 중요해요. 앞에서도 '문자열의 길이'가 고정되어 있다고 했는데, 이 내용을 한 번 더 설명해주고 있네요.

뭔가 내용이 많았습니다. '문제'에 대한 인식, '고정값' 및 '재진술' 생각하기 등 꼭 했어야 할 생각들이 많았네요. 앞으로 정확히 어떤 이야기를 할지는 알 수 없지만, '해시 함수'에 대한 이야기를 할 것은 확실해 보입니다. 계속 읽어봅시다.

| 하이라이트 문장 |

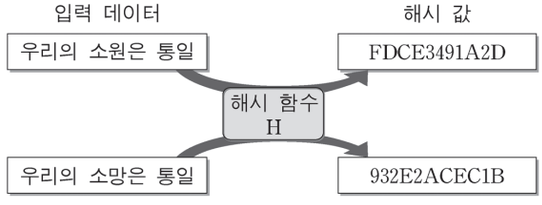
해시 함수란 입력 데이터 x에 대응하는 하나의 결과 값을 일정한 길이의 문자열로 표시하는 수학적 함수이다.

해시 함수의 '정의'인 동시에 '고정값'을 나타내주는 문장입니다. '정의'만 있어도 정말 중요한데, 자주 출제되는 포인트인 '고정값'까지 서술되어 있으니 더 꼼꼼히 읽어줬어야겠죠? 심지어 마지막 문장에서 한 번 더 강조해주니까요.

이러한 특성을 갖고 있기 때문에 **해시 함수**는 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.>

이러한 특성 때문에 '해시 함수'는 '데이터 내용의 변경 여부'를 알 수 있게 해준다고 합니다. '해시 값'은 데이터가 조금만 변해도 크게 달라진다고 했으니, '해시 값'의 변화 여부로 데이터 내용의 변경 여부를 알 수 있는 것이죠! 예시를 이용하면 더 잘 이해할 수 있겠네요.

여기에 첫 문단과 두 번째 문단 사이에 있는 그림을 이해해보고 가도 좋을 것 같습니다. 그림이란 일종의 '예시'에 해당하므로, '해시 함수'라는 원리를 이해하는 데 큰 도움을 줄 테니까요.



[해시 함수의 입·출력 동작의 예]

그림을 보니, 먼저 입력 데이터 중 '소원/소망'이라는 글자만 변했는데도 (입력 데이터의 미세한 변화) '해시 값'은 크게 달라지는 모습입니다. 그 와중에 해시 값을 나타내는 문자열의 길이는 문자 11개로 똑같네요. (고정값) 그림 역시 예시이니까, 최대한 완벽하게 이해할 수 있게 노력하는 게 필요하겠죠?

또한 이렇게 되면 2문단에서 말한 것처럼 '해시 값'의 변화를 통해 '입력 데이터의 변경 여부'도 쉽게 알 수 있겠습니다. 만약 입력 데이터가 변경됐으면, 아주 작은 변화라도 해시 값이 크게 달라지니까 전송된 입력 데이터에 대한 해시 값이랑 크게 다르겠죠? 데이터가 변경되었는지 아닌지 알 수 있는 거죠. 어렵지 않죠?

그런데 해시 함수가 일방향성과 충돌회피성을 만족시키면 암호 기술로도 활용된다. **일방향성**이란 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 **충돌회피성**이란 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.

그런데 이런 '해시 함수'가 '일방향성'과 '충돌회피성'을 만족시키면 '암호 기술'이 되기도 한다고 해요! 그렇죠. 결국 이 지문에서 '해시 함수'는 '암호 기술'의 역할을 하기 위해 나온 것이므로, 이런 내용이 나왔어야 합니다. 반가워하면서 읽어봅시다.

먼저 '일방향성'은 한마디로 '데이터의 복원이 어렵다'는 내용이네요. 입력 데이터를 입력하면 해시 값이 나오지만, 해시 값을 통해서는 입력 데이터를 알 수 없습니다. 즉, '입력 데이터 → 해시 값'은 가능하지만 '해시 값 → 입력 데이터'는 불가능하니, '일/방향성'이라고 할 수 있네요. 한 방향으로밖에 못 움직이니까요.

또한 '충돌회피성'은 '충돌쌍'이라는 것을 찾는 게 거의 불가능하다는 것이구요. 말 그대로 '충돌'을 '회피'하는 성질인 것입니다. 여기서 '충돌'은 '입력 데이터'가 다른데, '해시 값'이 같은 상황이네요. 입력 데이터가 조금이라도 달라지면 해시 값은 크게 달라야 하는데, 같은 상황인 거죠. '문제'라고 할 수 있겠네요. 그리고 이런 '충돌쌍'을 찾는 것이 사실상 불가능하다는 것은 너무나도 당연한 서술입니다. 왜냐하면 위에 설명한 대로 입력 데이터가 아주 조금이라도 달라지면 해시 값이 크게 바뀌니까요. 애초에 해시 함수의 특성상 충돌 상황이 발생할 가능성이 너무 낮아 그러한 '충돌쌍'을 찾기가 어려운 거예요.

그런데 이런 내용 자체를 이해하는 데에서 그치시면 안 됩니다. 이걸 갖추면 '해시 함수'가 '암호 기술'이 된다는 것이 더 중요해요! 지문 길이의 한계 때문인지 왜 암호 기술이 될 수 있는지 자세히 설명되어 있지는 않지만, 대충 이런 성질을 가지면 '암호 기술'

의 역할을 할 수 있겠다는 생각은 할 수 있겠죠?

> 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.> ① 이때 각 입찰 참여자는 자신의 입찰가를 감추기 위해 논스의 해시 값과, 입찰가에 논스를 더한 것의 해시 값을 함께 게시판에 게시한다. ② <해시 값 게시 기한이 지난 후> 각 참여자는 본인의 입찰가와 논스를 운영자에게 전송하고 ③ 운영자는 최고 입찰가를 제출한 사람을 낙찰자로 선정한다. 이로써 온라인 경매 진행 시 발생할 수 있는 다양한 보안상의 문제를 해결할 수 있다.

왜 '해시 함수'가 암호 기술이 될 수 있는지에 대해서는 자세히 설명되어 있지 않지만, 이를 '온라인 경매'라는 예시를 통해 이해시키려는 모습입니다.

물론 정확하게 이해하기는 어렵지만, ①~③의 과정에서 '해시 값'을 이용하며 '보안상의 문제'를 해결하고 있다는 흐름을 잡아주시면 되겠습니다.

| 생각 심화 |

예시를 한번 이해해볼까요? 지금까지 앞 문단들에 등장했던 여러 개념과 정의를 적용하면 충분히 이해할 수 있습니다.

우선 해시 함수 G는 모든 사람에게 공개되어 있습니다. 참가자와 운영자 모두 어떤 데이터가 주어지면 얼마든지 해시 값을 계산할 수 있는 거예요. 나아가 '일방향성'과 '충돌회피성'을 만족시키는 해시 함수를 사용하기 때문에, 해시 값을 역으로 계산하여 원래의 데이터를 알아내거나 같은 해시 값을 가진 다른 데이터를 알아내는 것은 불가능합니다. 이걸 대전제로 삼고 가야겠죠?

먼저 참여자들은 '논스의 해시 값'과 '(입찰가+논스)의 해시 값'을 게시판에 게시합니다. 정확히 봐야 해요. 자신의 '진짜 입찰가'를 바로 쓰는 게 아니라, '논스'라고 하는 것과 '진짜 입찰가'에 '논스'를 더한 데이터의 '해시 값'을 게시하는 거예요. 이를 게시한 사람을 제외하고는, 그 누구도 이 사람이 '논스'와 '진짜 입찰가'를 얼마로 설정했는지 절대 알 수 없을 겁니다. '일방향성'을 만족하니까요! 이렇게 각자의 입찰가를 숨기는 방식으로 경매가 진행됩니다. 만약 누가 얼마를 불렀는지 모두가 알 수 있다면, 그로 인한 여러 부작용이 발생하겠죠? 정시 지원을 할 때 각 학과에 지원한 사람의 점수를 마감 전에 알 수 있다면 여러 문제가 발생하는 것과 비슷한 겁니다. 따라서 각자의 입찰가를 숨기면서 경매를 진행하는 것이죠.

아니 그러면, 누가 얼마를 불렀는지 어떻게 알 수 있을까요? 다 숨겨져 있는데 말이죠. 일단 지문을 읽어보니, 해시 값 게시 기한이 끝난 후에 각 참여자가 운영자에게 본인의 '입찰가'와 '논스'를 운영자에게 전송합니다. 중요한 건, 이때는 '해시 값'이 아닌 원래 데이터를 전송한다는 거예요. 그럼 운영자는 이 데이터로 뭘 할까요? 그렇죠! 바로 해시 함수 G에 넣어서, 그 결과 값이 이 사람이 처음 게시한 '논스의 해시 값' 및 '(입찰가+논스)의 해시 값'과 똑같이 나오는지 확인할 겁니다. 만약 그 두 값이 다르다면, 입력 데이터의 내용에 '미세한 변화'만 있어도 '크게' 달라지는 해시 값의 특성상 참여자가 거짓말을 하고 있음을 쉽게 알아낼 수 있겠네요. 나아가, '충돌회피성' 때문에 혹시나 거짓말을 했는데 해시 값이 같게 나오는 경우도 거의 없을 거예요. 이런 방식으로 정말 그 사람이 처음 게시판에 게시한 입찰가가 얼마인지를 파악하고, 이 중에서 가장 높은 금액을 부른 사람을 낙찰자로 선정하는 것입니다.

그렇다면, '논스'는 도대체 왜 사용하는 것일까요? 그냥 '입찰가'의 해시 값만 전송해도 입찰가를 숨기는 데는 아무런 문제가 없을 텐데요. 이는 지문 내용만으로 명확하게 알기는 어렵지만, 조금만 생각해보면 쉽게 알 수 있습니다. 만약 '입찰가'의 해시 값만을 게시판에 게시한다고 해봅시다. 이 경우 해시 값을 역으로 계산하여 원래 데이터를 바로 알아내는 것은 불가능하지만, 모든 숫자를 일일이 계산해보면 게시판에 올라온 것과 같은 해시 값을 찾을 수는 있을 겁니다. 자세히 설명해볼게요. 사실 경매에 올라오는 물건들의 가격대는 어느 정도 정해져 있습니다. 예를 들어 중고 휴대폰이라면, 보통 2~30만원 선에서 가격이 형성되겠죠. 이때 어떤 불굴의 의지를 가진 사람이 200,000원부터 200,001원, 200,002원, ... 299,999원 등을 모두 해시 함수 G에 넣어 계산해볼 수 있을 겁니다. 그러면 중간중간 나오는 해시 값들이 게시판에 게시된 것과 똑같을 수 있겠죠? 이런 방식으로 각 참여자가 얼마를 불렀는지를 알 수 있게 되고, 이는 위에서 말했던 문제를 낳게 됩니다. 따라서 '논스'라는, 게시자만 알 수 있는 임의의 숫자를 포함하고, '입찰가'를 직접적으로 변환한 값이 아닌 이 '임의의 숫자'를 더한 값을 변환해 게시하도록 하는 방식으로 경매를 진행하는 것이죠!

조금 어렵다고 느낄 수도 있지만, 핵심은 하나입니다. 우리가 읽고 있는 이 내용도 결국 '사례'에 해당하니, 제시된 '원리'와 붙여서 읽어줘야 한다는 거예요. 제시된 원리는 '해시 함수'의 특징, '일방향성', '충돌회피성'의 정의 등입니다. 하나하나

일대일로 대응시키면서 읽으면, 얼마든지 해낼 수 있는 경지예요. 어렵다고 넘어가지 말고 최선을 다해서 이해해봅시다.

몰랐던 어휘 정리하기

30 ③

선지	①	②	③	④	⑤
선택률	5%	5%	79%	8%	3%

① '해시 함수'라는 개념을 이끌어내기 위해 들었던 '비트코인' 예시를 통해 쉽게 지울 수 있겠죠.

② 기억이 나지 않으면 자연스레 '해시 함수'의 정의를 확인하셔야 합니다! 입력 데이터에 대응하는 '하나의 결과 값'을 나타내는 게 '해시 함수'예요. 두 개의 서로 다른 해시 값을 도출하지는 않겠죠.

③ 지문 속에 명확한 근거는 없지만, 적용되는 '해시 함수'가 달라질 경우 당연히 '해시 값'도 달라지겠죠? 해시 함수도 결국 '함수'이므로, 적용되는 식이 다를 테니까요. 혹은 함수가 다를 때도 '해시 값'은 항상 일정하다는 내용은 지문에선 알 수 없기 때문에 틀렸다고 해도 될 것 같습니다만, 여러모로 조금 아쉬움이 남는 선지입니다.

④ '문자열의 길이!' 우리가 '고정값'으로 체크해뒀던 내용입니다. H와 같은 특정한 해시 함수에서 해시 값의 문자열의 길이는 고정되어 있다고 했어요.

⑤ 2문단에서 체크했던 정보죠? 그림을 통해 이해하려는 노력까지 곁들였으면 더욱 쉽게 지울 수 있었겠네요.

31 ①

선지	①	②	③	④	⑤
선택률	69%	5%	5%	9%	12%

① '일방향성'의 정의 그 자체를 묻는 선지네요. '해시 값'을 바탕으로 '입력 데이터'를 복원할 수 없다는 것이 핵심이었죠?

② '일방향성'은 '복원'에 대한 내용입니다. '문자열의 길이'가 고정된 것과는 아무런 상관이 없어요.

③ 특정 해시 함수에서 나오는 해시 값의 '문자열의 길이'는 항상 고정되어 있다고 했습니다. 고정값을 다시 한번 건드리고 있죠? '충돌회피성'은 데이터의 충돌쌍을 찾는 것과 관련된 내용이지, '문자열의 길이'와는 아무 상관이 없어요.

④ 이렇게 도출한 '해시 값'이 같은 경우, 즉 '충돌'하는 경우에 그 쌍을 찾기 어렵다는 것이 '충돌회피성'의 내용입니다. 충돌하는 원인 그 자체가 '충돌회피성'은 아니에요! 개념의 정의를 디테일하게 체크할 것을 요구하는 선지였어요.

⑤ 역시 정의를 디테일하게 묻고 있는 선지입니다. '충돌'의 정의는 '같은 함수'에 서로 다른 데이터를 넣었을 때 같은 해시 값이 나오는 경우입니다. 그런데 여기선 '다른 함수'에 적용한 상황을 묻고 있네요. 여기에 ㉠, ㉡은 '충돌'이 발생하는 상황 그 자체와는 아무런 관련이 없으니 총체적으로 틀린 선지였어요. 정의 체크의 중요성! 몇 번이고 강조해도 지나치지 않습니다.

32 ②

선지	①	②	③	④	⑤
선택률	6%	72%	7%	7%	8%

– [가]에서 설명한 '온라인 경매'를 실제로 해보자는 것이네요. 지문의 해당 부분에서 과정을 다시 체크해봅시다.

1) 각 입찰 참여자는 자신의 입찰가를 감추기 위해 논스의 해시 값과, 입찰가에 논스를 더한 것의 해시 값을 함께 게시판에 게시한다.
2) 해시 값 게시 기한이 지난 후 각 참여자는 본인의 입찰가와 논스를 운영자에게 전송한다.
3) 운영자는 최고 입찰가를 제출한 사람을 낙찰자로 선정한다.

결국 A와 B는 처음에 각각 r과 m, 그리고 s와 n을 게시판에 게시하고, 이 기한이 지난 후 각각 a와 논스, b와 논스를 운영자에게 전송하겠네요. 운영자는 여기서 최고 입찰가를 제출한 사람을 선정하는 것이구요. 대충 이 정도로 흐름을 잡아 두고 선지 판단해 보도록 합시다.

① a, 즉 진짜 '입찰가'는 해시 값 게시 기한이 지난 후에 전송하는 겁니다!

② 게시 기한 전에는 해시 값만 볼 수 있습니다. 그런데 이 해시 값을 만든 '해시 함수'는 '일방향성'을 만족한다고 했기 때문에, 운

영자는 '해시 값'을 '입력 데이터'로 복원할 수 없겠죠. 그럼 최고가 입찰자도 당연히 알 수 없겠네요!

③ m과 n이 같은데 r과 s가 다르면, a와 b는 당연히 다르겠죠. 해시 값은 입력 데이터 당 하나밖에 나오지 않기 때문에, r과 s가 다르다는 건 '논스'의 원래 값도 다르다는 것이고, '논스'가 다른 상황에서 '입찰가+논스'를 같게 만들려면 '입찰가'는 당연히 다를 것이니까요.

④ r과 s는 입찰가와는 아무 상관없는 '논스'의 해시 값이에요. 또한 '일방향성' 때문에 이 '논스'도 정확히 알 수 없으니 누가 높은 가격으로 입찰하였는지는 절대 알 수 없겠죠.

⑤ B가 m과 r을 알아도 '일방향성' 때문에 그것의 입력 데이터를 알 수는 없기 때문에 게시판이 굳이 비공개로 운영될 필요는 없겠네요. 봐도 뭘 알 수 있는 게 없으니까요.

정답률이 그리 낮지는 않았지만, 지문을 제대로 이해하고 문제를 완벽하게 해결하기는 쉽지 않았습니다. 단순히 '맞혔다'가 아닌 '완벽하게 뚫었다'라는 느낌이 들 때까지 공부해보도록 합시다. 제가 쓴 해설 정도면 충분해요.

| 핵심 point |

① 화제 check : 독서 독해의 처음이자 끝. 첫 문단에서 잡은 '화제'를 마지막 문단까지 놓지 않아야 합니다.
② 재진술 인식 : 같은 말이라도 다르게 표현되는 경우가 많습니다. 이 '같은 말'에 민감하게 반응하면, '정보량'을 줄이면서 읽을 수가 있습니다.
③ 고정값 : 고정된 값이 제시되면 확실하게 체크해두셔야 합니다. 다른 개념들과 비교될 때의 '기준'이 되기도 하고, 일단 문제에 나오니까요!
④ 사례–원리 연결 : 모든 사례는 어떠한 원리를 이해시키기 위해 존재합니다. 독해 속도를 늦추면서 확실하게 '이해'하고 넘어갑시다.
⑤ 〈보기〉 정리 : 〈보기〉 문제를 해결할 때, 선지를 판단하기 전에 반드시 〈보기〉의 내용을 어느 정도 정리하는 것이 중요합니다.