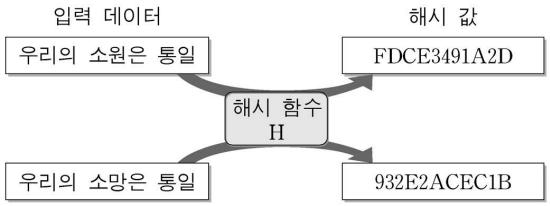
[16～18] 다음 글을 읽고 물음에 답하시오. -2016.09A

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 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.

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.