RSA에 사용된 수학 이론

다음은 RSA 암호제작과 해독의 구조를 수학적으로 설명한 것이다.

(1) 앨리스는 값이 큰 두 개의 소수를 선택하고 이를 각각 p, q라고 정한다. 이 두 소수는 값이 엄청나게 큰 것이어야 하지만, 여기서는 편의를 위해 $p = 17$, $q = 11$이라고 가정하자. 앨리스는 이 두 숫자를 비밀에 부쳐야 한다.

(2) 앨리스는 이 두 숫자를 곱해서 N을 얻는다. 이 경우 $N = 187$이다. 앨리스는 숫자 하나를 더 선택한다. 여기서는 이 숫자가 $e = 7$이라고 가정해 보자. (e와 $(p-1) \times (q-1)$은 서로소가 된다. 그러나 이 부분은 전문적이어서 그 설명은 생략.)

(3) 앨리스는 이제 전화번호부와 맞먹는 공개 열쇠 열람부에 e와 N값을 공개한다. 암호제작에 이 두 숫자가 필요하기 때문에 앨리스에게 암호를 보내고 싶어 하는 사람은 모두 이 숫자를 알아야 한다. 이 두 숫자는 앨리스의 공개 열쇠에 해당한다. (e는 앨리스의 공개 열쇠의 일부를 구성함과 동시에 다른 모든 사람의 공개 열쇠의 일부가 될 수 있다. 그러나 p와 q의 값에 따라 변화하는 N값은 모두 달라야 한다.)

(4) 메시지를 암호화하기 위해서는 그 내용을 숫자 M으로 변화시켜야 한다. 예를 들어 원문을 ASCII 이진수로 변화시킨 뒤, 이렇게 해서 얻은 숫자들을 다시 십진수로 변환하여 사이퍼 텍스트 C로 암호화 한다. 이때 사용되는 공식은 다음과 같다. 즉,

$$C = M^e \pmod{N}$$

(5) 밥이 앨리스에게 키스, 즉 X라는 글자 한 자만을 보내고 싶다고 해보자. ASCII에서 X는 $1011000_{(2)}$으로 표현된다. 이 이진수를 십진수로 표현하면 88이다.

$$M = 88$$

(6) 이 메시지를 암호화하기 위해서 밥은 공개 열쇠 열람부를 참조해 앨리스의 공개 열쇠 $N = 187$, $e = 7$이라는 것을 확인한다. 이 두 숫자를 알면 앨리스에게 보내는 메시지를 암호화하는 데 필요한 공식을 얻을 수 있다. M의 값이 88이므로 공식은,

$$C = 88^7 \pmod{187}$$

(7) 위 함수를 계산기로 계산하는 것은 쉬운 일이 아니다. 계산기의 문자판이 이렇게 큰 수를 모두 표기할 수는 없기 때문이다. 그러나 모듈러 함수의 지수를 계산하는 쉬운 방법이 있다. $7 = 4 + 2 + 1$이므로,

$$88^7 \pmod{187} = \left[88^4 \pmod{187} \times 88^2 \pmod{187} \times 88^1 \pmod{187}\right] \pmod{187}$$

$$88^1 = 88 = 88 \pmod{187}$$

$$88^2 = 7{,}744 = 77 \pmod{187}$$

$$88^4 = 59{,}969{,}536 = 132 \pmod{187}$$

$$88^7 = 88^1 \times 88^2 \times 88^4 = 88 \times 77 \times 132 = 894{,}432 = 11 \pmod{187}$$

밥은 이제 암호문 텍스트 $C = 11$을 앨리스에게 보내면 된다.

(8) 모듈러 함수의 지수는 일방 함수이기 때문에 $C = 11$을 거꾸로 계산해서 원문 메시지를 알아내기는 무척 어렵다. 따라서 이브로서는 이 암호 메시지를 가로챈다 하더라도 해독할 수 없다.

(9) 그러나 앨리스는 자신만이 가지고 있는 특별한 정보를 이용해서 암호를 해독할 수 있다. 이미 알고 있는 p와 q의 값을 이용해 암호 해독 열쇠, 즉 자신의 개인 열쇠인 d값을 구하면 된다. d를 계산하는 방법은 다음과 같다.

$$e \times d = 1 \pmod{(p-1) \times (q-1)}$$

$$7 \times d = 1 \pmod{16 \times 10}$$

$$7 \times d = 1 \pmod{160}$$

$$d = 23$$

(d값을 계산해 내는 것은 단순한 과정이 아니지만, 유클리드의 알고리듬이라고 알려져 있는 방법을 사용하면 쉽게 해결할 수 있다.)

(10) 메시지를 해독하기 위해서 앨리스는 다음 공식을 이용한다.

$$M = C^d \pmod{187}$$
$$M = 11^{23} \pmod{187}$$
$$M = \left[11^1 \pmod{187} \times 11^2 \pmod{187} \times 11^4 \pmod{187} \times 11^{16} \pmod{187}\right] \pmod{187}$$
$$M = 11 \times 121 \times 55 \times 154 \pmod{187}$$
$$M = 88 = X(\text{ASCII에 의해서})$$

리베스트, 샤미르, 애들먼은 특별한 1차 함수를 만들어서 특수한 정보, 즉 p와 q값을 아는 사람만 뒤집어 계산할 수 있도록 했다. 각각의 함수는 p와 q값을 선택하고 이 두 수를 곱해서 N을 얻는 방법을 통해 개인화할 수 있다. 이 함수를 이용해서 모든 사람은 어떤 특정 개인의 N값을 사용해 그 사람에게 보내는 암호문을 작성할 수 있지만, N값을 만들어 낸 p와 q값을 알고, 따라서 해독 열쇠인 d를 아는 사람만이 이 암호문을 해독할 수 있다.