인터넷 암호의 수수께끼

인터넷 암호를 누군가가 가로챈다면 그건 큰일이다. 수학에서 이러한 암호체계를 만드는 기본적인 발상은 곱셈은 쉽지만 나눗셈은 어렵다는 것을 기초로 하고 있다. 그래서 암호는 큰 숫자일수록 풀기가 어렵다는 것이다.

인터넷을 통해 물건을 사려면, 주소와 신용카드 번호 등을 인터넷을 통해 알려 주어야 한다. 이같은 중요한 정보를 누군가가 가로채면 어쩌나 하는 걱정 때문에 조금은 불안하다. 이 때, 남들이 알아볼 수 없게 암호를 만들어 보내는 방법은 없을까 하는 생각을 할 수 있다. 그러나 이 방법은 물건을 파는 회사의 입장에서는 받아들일 수 없는 방법이다. 물건을 사려 하는 사람 각각과 암호를 교환하기 위해서는 암호표와 같은 것을 각각에게 알려 주어야 할 터인데 이것은 말이 안되게 번거로운 일일 뿐만 아니라 인터넷을 통해 암호표를 전달할 때 이 암호표를 누군가가 가로챈다면 그건 더욱 큰 일이 될 것이기 때문이다. 이를 어쩌면 좋을까?

공개열쇠암호체계라는 것이 약 20여년 전에 소개되었다. 이것은 암호를 만드는 방법을 모두에게 공개하되 암호를 푸는 방법은 자기만이 간직하는 방법이다. 이런 방법은 앞서 말한 인터넷을 통하여 물건을 파는 회사 같은 곳에게 좋은 방법이 될 수 있다. 왜냐하면 물건을 사는 사람도 암호를 만드는 방법을 알 것이므로(암호를 만드는 방법은 모두에게 공개되었으니까) 자신의 중요한 정보를 암호로 알리게 될 것이고, 이 정보를 도중에 누군가가 가로챈다고 하더라도 이 사람이 가로챈 것은 암호일 터인데 이 암호를 푸는 방법은 물건을 판 회사만이 알 뿐이니까 암호를 가로챈 사람은 암호를 풀 수가 없을 것이기 때문이다.

그런데 다시 생각해보면 어딘가 이상하다. 암호를 만드는 방법을 아는데 그것을 푸는 방법을 모를 수가 있을까? 암호를 푸는 과정은 암호를 만드는 과정을 거꾸로 하는 과정일 텐데, 한쪽 과정을 알면 그 거꾸로의 과정도 알 수 있는 것이 당연하게 보이니까 말이다. 그렇지만 세상의 대부분의 일이 한 쪽이 쉬우면 다른 쪽은 어렵기 마련인 것이 아닐까? 무슨 공익 광고에도 나오듯이 산불이 숲을 태우는 것은 잠깐이지만 그 숲을 복원하는 데는 수십년이 걸리고, 우리가 경험하고 있듯이 환경을 오염시키기는 쉬워도 그것을 원상복구하는 것은 얼마나 어려운 일인가!

이와 같이, 암호를 만드는 과정은 쉽지만 그 거꾸로의 과정은 불가능하거나 지극히 어렵고 상상을 초월하는 오랜 시간이 걸리는 방법이 있어야 이 공개암호체계는 성공적인 체계가 될 것이다. 수학에서 이러한 암호체계를 만드는 기본적인 발상은 곱셈은 쉽지만 나눗셈은 그렇지 않다는 생각과 같은 간단한 아이디어를 기초로 하고 있다. 예를 들어서 15553의 약수를 계산해보시기 바란다. 시간이 조금 걸릴 것이다. 하지만 103과 151을 곱하는 것은 금방이다. 15553이 아니라 더욱 큰 수를 사용한다면 시간은 더욱 걸릴 것이고, 약수가 몇개 뿐이 없을 경우에는 더욱 어려울 것이라고 추측이 갈 것이다.

주어진 수의 약수를 모두 찾는 효과적인 방법은 아직 개발되어 있지 않다. 그래서 아주 큰 수가 소수(1과 자기 자신만이 약수인 수)인지를 판단하는데는 대형 컴퓨터를 사용해도 상상을 초월할 만큼 오랜 시간이 걸리는 경우가 흔하다. 그러므로 아주 큰 수의 약수들을 모두 안다는 것은 이 암호체계에서 매우 중요한 정보가 된다. 이 암호체계가 국가안보와 같은 것에 관련된 것이라면 그 중요함은 상상이 갈 것이다. ST

高城殷 〈건국대 수학과 교수〉