
# 인터넷 통신의 안전성 보장하기

암호에 관한 수학 없이는 누구도 인터넷상에서 안전하게 쇼핑하거나, 지불하거나, 업무를 수행할 수 없습니다. 수 세기 전에 증명된 대수적 사실들에 기반을 두고 있지만, 오늘날의 복잡한 암호 기법들이 구축된 것은 지난 25년 안의 일입니다.

공개키 암호화 방식은 사용자로 하여금 복호화 키는 숨기면서도 암호화 키를 모두가 사용하도록 공표할 수 있게 해줍니다. 그러한 알고리즘 중 하나인 RSA는 현대 브라우저에 쓰이는 암호화의 배경이 되고 있습니다. 최근에 미국 국립 표준 기술국은 앞으로 전자 통신에 쓰일 것으로 고급 암호화 표준(AES)을 채택하였습니다. 이 새로운 표준은 순열, 모듈 연산, 다항식, 행렬, 유한체를 이용하여 자유롭지만 안전하게 정보를 전송할 수 있게 합니다.

더 알아보기: "Communications Security for the Twenty-first Century," Susan Landau, *Notices of the American Mathematical Society*, April 2000.

Translation courtesy of volunteer members of the Korean Mathematical Society.