통신 수학

세상에 타전하는 수학자들의 디지털 메시지

글 _ 조용승 이화여자대학교 수학과 교수 yescho@joins.com

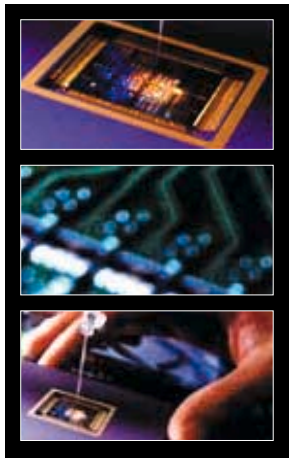

벨

디지털이라는 단어를 빼놓고는 살 수 없는 세상이 됐다. 통신 역시 '디지털 통신'이 대세가 된지 이미 오래다. 하지만 '디지털 혁명'이라고 불릴 만한 통신의 디지털 시대를 연 것이 수학자들이라는 사실을 아는 사람은 얼마나 될까.

삼각함수에서 시작된 디지털통신 혁명

프랑스의 수학자 푸리에(Baron de Fourier, 1768~1830)는 1822년, 모든 주기적인 현상을 삼각함수의 선형결합으로 나타낼 수 있다는 이른바 '푸리에 정리'를 발표했다.

얼핏 순수수학의 발견으로 그쳤을 지도 모를 이 이론이 빛을 보게 된 것은 120여 년이 지난 1948년, 미국 벨 연구소의 클라우드 섀넌이 '통신이론의 수학적 원리'라는 논문을 발표하면서부터였다.


통신관련 칩

정보이론의 기념비적인 업적으로 꼽히는 이 논문의 발표로 아날로그 통신 시대는 막을 내렸고, 디지털 혁명의 싹이 움트기 시작했다. 지구 반대편의 사람들과 얼굴을 보면서 통화할 수 있게 된 것도 푸리에라는 수학자의 이론 덕택인 셈이다.

이 논문이 발표되었던 20세기 중반만 해도 통신케이블을 사용하여 1천800개 정도의 신호를 보낼 정도의 수준밖에 되지 않았다. 사람들이 '20세기 최고의 발견'이라는 찬사를 아끼지 않았던 통신혁명은 그렇게 시작되었다. 수학의 발전이 곧 통신기술의 발전을 의미한다는 사실을 알게 된 것도 그 때부터였다.

그 후 반세기가 넘는 세월 동안 통신수학은 발전을 거듭했고, 지금은 사람 머리카락만한 굵기의 광통신케이블에 640만 개의 통신정보를 보낼 수 있게 됐다. 기술의 격세지감을 느낄 법한 얘기다.

로그이론+지수함수+3차방정식+… = 예금 인출, e-메일 교환 등

그렇다면 통신 분야에서 수학의 역할은 무엇일까. 수학은 통신시스템에서 발생하는 무작위적인 현상을 확률론을 기반으로 정밀하게 분석하는 몫을 담당한다. 그 결과는 통신망의 성능을 분석하는데 활용된다. 뿐만 아니라 통신 시스템의 최적화를 위한 알고리듬 개발과 소프트웨어 설계 · 구현을 통한 원천 핵심기술 개발에도 수학은 중요한 역할을 한다.

역설적인 이야기로 들릴 수도 있겠지만, 다른 사람이 통신내용을 아무나 알 수 없도록 비밀을 유지하는 '암호'의 발전도 역시 수학의 공로였다.

게임이론과 함께 현대 수학에서 빼놓을 수 없는 암호이론은 영국의 수학자 튜링(Alan Turing, 1912~54)이 악명 높은 독일군 암호체계 에니그마를 해킹하면서 급격하게 발전했다. 그

벨연구소의 연구원

초고속 광검출기

러나 영국이 주축이 된 연합군의 승리에 결정적인 역할을 했던 그는 전쟁이 끝난 뒤 독이 든 사과를 먹고서 자살했다. 세상은 그가 사망한지 12년 뒤에 수학의 노벨상이라 불리는 '앨런 튜링 상'을 만들어 전쟁 영웅의 삶을 기렸다.

암호이론은 순수수학자들이 로그이론, 로그함수, 지수함수 등의 이론을 이해하고, 이를 삼차방정식과 타원에 적용한 뒤에야 실생활에 쓰일 수 있게 됐다. 우리가 은행예금을 인출하고, 신용카드를 사용하고, e-메일을 주고받을 수 있는 것도 바로 이 암호이론 덕분이다.

수학교육이 국력 좌우하는 21세기

전자상거래의 핵심 기술로 꼽히는 '공개키 암호'의 원리도 대수방정식의 해법과정에서 발견한 군론(群論)과 소인수분해 이론을 응용한 것이다.

공개키 암호시스템은 타인이 메시지를 암호화할 때 사용하는 공개키와 암호문을 원래의 메시지로 복원할 때 쓰는 비밀키를 각각 사용하는 암호시스템을 말한다. 공개키 암호시스템은 전송에 의존하는 데이터의 보안에 반드시 필요한 기술로 많은 수학적 이론이 응용된다.

이 공개키 암호 기술 분야에서는 우리 나라가 세계 최고 수준의 기술 경쟁력을 갖고 있다. 지난 2000년 한국과학기술원 수학과 교수팀이 한국전자통신연구원 부설 국가보안기술연구소와 공동으로 공개키 암호 원천기술을 세계 최초로 개발한 것이다. 이 기술은 곱셈과 덧셈 등 연산의 순서를 바꿔 다른 값이 나오도록 하는 '비가환군'에 근거했다. 미국에서 개발돼 가장 널리 쓰이는 공개키 일종인 RSA(Rivest Shamir – Adleman)시스템보다 2배 이상 빠른 이 기술은 공개키 암호론이 시작된 지 20여년 만의 획기적인 수학이론으로 평가받고 있다. 특히 암호화 및 복호화 속도가 매우 빠르고 구현하는 알고리듬의 크기가 작아 스마트카드나 전자화폐와 같은 소용량 장치에도 무리없이 적용할 수 있다.

벨연구소 내부

우리 나라는 미국과 함께 공개키 암호시스템의 원천기술을 확보한 단 두 나라 중 하나가 되었다. 우리 나라가 전자상거래 및 정보보호분야에서 미국과 함께 시장을 주도하게 될 것은 당연해 보인다.

21세기는 정보통신 분야의 신기술이 국력을 좌우하는 시대다. 그 정보통신 국력을 뒷받침하는 학문이 바로 수학이다. 소련이 미국보다 먼저 인공위성을 쏘아 올렸을 때 미국 사회가 '수학교육의 부재'에서 원인을 찾았던 이유를 지금 한국 사회는 곰곰이 되씹어 봐야 할 때다. ST

글쓴이는 미국 시카고대학교에서 박사학위를 취득하였으며, 현재 이화여대 수학과 교수로 재직중이다.