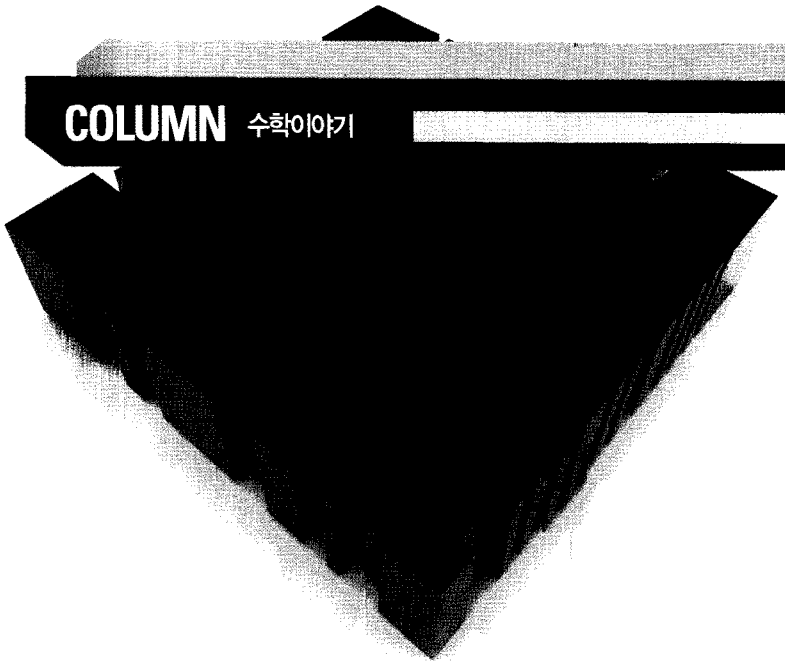


수학, 현대인의 사생활 보호 지킴이

오늘 갑자기 당신의 컴퓨터가 바이러스를 먹어 작동이 안 되고, 휴대폰이 고장 났다고 가정해 보자! 전자결제와 휴대폰 불통으로 당신은 안절부절못하며 더구나 불쾌지수까지 높은 장마철에 왕짜증을 내게 된다. 컴퓨터와 휴대폰이 우리 삶 속에 너무 깊숙이 들어왔기 때문이다.

그런데 편리한 물건의 그늘에는 늘 위험의 요소가 있는 법. 이른바 정보의 도둑질 해킹이 그것이다! 사생활을 지켜주는 나만의 정보를 잘 유지 · 관리하려면 패스워드(비밀번호) 관리를 철저히 해야 한다. 개인적으로도 주의해야하지만 기업과 관공서 또한 예외가 아니다. 텔레뱅킹이나 인터넷뱅킹을 할 때, 이메일을 열어볼 때, 인터넷 쇼핑으로 결제를 할 때 다양한 영역에서 필요한 패스워드의 원리는 무엇일까. 수학의 분야에서 정수론의 이론을 기초로 발달한 '암호수학'의 힘을 빌려야 설명이 가능하다.

글_ **계영희** 고신대학교
유아교육과 교수
yhkye@kosin.ac.kr
글쓴이는 이화여대 수학과 졸업 후 한양대학교에서 석사학위를, 홍익대학교에서 박사학위를 받았다. 현재 고신대학교 종합인력개발원 원장, 한국수학교육학회 이사, 한국수학사학회 부회장 등을 겸임하고 있다.

암호의 원조, 케사르

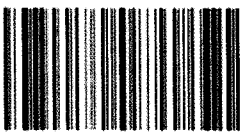
2004년 전자 · 전기공학의 전문학술지 '스펙트럼'에서, 암호학은 향후 10년을 이끌어 갈 10대 기술로 선정되었다. '역사학의 아버지'라고 불리는 고대 그리스의 헤로도투스의 기록에 의하면, B.C. 5세기경 그리스는 페르시아와의 전쟁 중에 문서를 비밀리에 전달하기 위해 희한한 방법을 사용했다. 스파이를 안전하게 침입시키기 위해서 머리를 삭발한 후에 메시지를 쓰고, 머리카락이 다시 자라기를 기다렸다가 보냈다는 것이다. 스파이가 잡혀서 몸을 수색당한다고 해도 증거자료가 밝혀질 염려가 없기 때문이었다. 물론 화급을 다투지 않는 고대사회에서나 있음직한 방법이다. 그러나 이 방법은 메시지 자체를 숨기는 것으로 엄밀히 말하면 암호는 아니었다. 메시지를 들키더라도 의미를 감추는 것이 곧 암호이기 때문이다.

암호의 시조는 클레오파트라와 드라마틱한 삶을 살았던 로마의 케사르이다. 그는 알파벳 글자를 세 자리씩 밀려 쓰는 방법으로 암호문을 만들었다. 알파벳의 'a, b, c, …'를 'D, E, F, …'로 바꾸었다. 'love'는 'ORYH'가 되어 읽어본들 도통 뜻을 알 수가 없게 된다. 케사르의 암호를 해독하려면 모두 몇 가지 방법이 있을까? 알파벳의 수가 26이므로 모두 25가지이다.

난공불락의 암호기계, 에니그마

1918년 독일의 발명가 슈르비우스는 새로운 암호기계를 발명했다. 그는 암호작전에 늘 실패하던 독일정부에 '에니그마'를 채택하도록 설득하여, 1925년에 대량 생산된 에니그마가 독일군에 보급되었다. 에니그마는 제2차 세계대전 초반까지 영국을 비롯한 연합군을 위협하는 난공불락의 암호기계였다.

그런데 적은 내부에 있는 법. 조국인 독일을 배반한 한스 틸로 슈미트가 역사에 등장을 한다. 가난하고 고독했던 그는 형에 대한 시기심

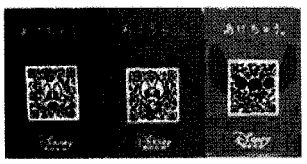


▸▸ 1차원 바코드

▸▸ 2차원 코드 중 하나인 QR코드

▸▸ 자이

▸▸ 부르주아



▸▸ 디즈니

과 자신을 버린 조국에 대한 반감으로 에니그마의 비밀정보를 프랑스에 팔아넘겨 돈을 거머쥐고 만다. 연합군은 에니그마의 정보를 획득했지만 한스의 정보만으로 암호를 해독하기에는 역부족이었다. 에니그마의 기계도 없었고, 수많은 경우의 수를 실험하고 연구해야만 해독이 가능했다.

그러나 또 한 번의 반전이 일어난다. 수학자 20명으로 구성된 폴란드의 암호해독반은 한스가 건네 준 복사물을 가지고, 애국심에 끓어오르는 열정과 창의력으로 암호해독에 매달렸다. 가장 뛰어난 사람은 23세의 레예프스키였다. 그는 모든 비밀통신에는 반복되는 것이 있으며, 반복은 일정한 패턴을 낳는다는 것을 알아차렸다. 패턴은 암호해독가들에게 해독의 발판이 된 것이었다.

연합국을 구한 수학자, 튜링

전쟁이 계속되는 동안 에니그마도 끊임없이 발전하였으므로 폴란드의 레예프스키가 개발한 암호해독기 '봄브' 역시 계속 발전했다. 영국의 암호해독국은 처음엔 언어학자와 고전학자들만 참여시키다가 후에는 수학자, 과학자, 체스 전문가, 십자말풀이 마니아까지 동원하여 각 건물에서 팀을 이루면서 연구하도록 했다. 가장 큰 공헌을 세운 인물은 수학자 튜링이었다. 에니그마를 해독하는 그의 아이디어는 전자식 암호해독기 '콜로수스'개발의 기초가 되었다.

전쟁이 끝난 후에도 암호학은 여전히 국가전략의 중요한 부분이며, 또 인터넷이 발달하면서 우리 생활과 밀접하게 그 위력을 발휘하고 있다. 1977년 리베스트, 세미르, 아델만 등 미국의 세 명의 수학자가 개발한 암호방식 RSA는 MS 윈도, 넷스케이프, 브라우저 등 많은 SW와 연동이 가능하고 편리하여, 국제표준화기구(ISO)에서 암호의 표준으로 삼았다. 이 알고리듬은 140자리 이상의 두 개의 큰 소수를 선택한 후 곱하고 추가 연산을 하여 공개키와 개인키를 구성하는 원리이다. 여기서 공개키란 우리가 흔히 아이디라고 부르는 것으로 다른 사람이 알아도 좋은 열쇠이며, 개인키란 비밀이 보장되어야 하는 나만의 패스워드를 말한다. 인터넷에서 사용하는 정보를 암호화하고, 복호화하는 데는 수학의 소인수분해의 원리가 사용된다.

생활 속의 암호, 바코드와 QR코드

복잡한 연산으로 만든 공개열쇠의 암호화에도 불구하고 해커들의 침입은 우리 사생활을 위협하고 있다. 그렇다면 해독이 불가능한 암호통신은 존재하지 않는 것일까. 1980년대 초 천재 물리학자 파인만이 제시한 해법은 바로 양자컴퓨터이다. 양자컴퓨터는 반도체 칩 대신에 액체가 계산을 하는데 기존의 컴퓨터가 수백년이 걸려야 해결하는 암호를 56비트 양자컴퓨터로는 불과 몇 분 만에 풀 수 있다고 예언을 했다. 지금은 액정으로 만든 모니터를 사용하고 있지만 컴퓨터 본체까지 액정으로 만들어진다면 가능하다는 이야기이다.

물건의 제조사와 상품명에 관한 정보를 효율적으로 관리하기 위해 사용되는 바코드, 우리의 주민번호, 도서의 ISBN에는 모두 공개암호에 해당하는 패리티 검사를 사용한다. 패리티 검사는 정보전달에 오류가 생겼는지를 체크하기 위해서인데 원리는 수학의 잉여류이다.

최근 스마트폰과 함께 폭발적으로 사용되는 QR코드를 알아보자. 1994년 일본 덴소웨이브사가 개발한 2차원 QR코드는 1차원의 바코드가 20자 정도의 간단한 정보를 제공한다면, 수백 배의 정보량을 제공한다. 문자 외에 음성과 영상, 위치정보까지 척척 알려주기 때문에 최근엔 마케팅에 필수품으로 등장하면서 독특한 디자인으로 옷을 입고 있다. 온라인과 오프라인을 자유자재로 넘나들면서 매체와 매체가 호환되는 재미있는 QR코드로 개인 명함을 편집하려면 단돈 1만 원이면 된다고 인터넷에서 우리를 유혹하고 있는 시대이다. ST