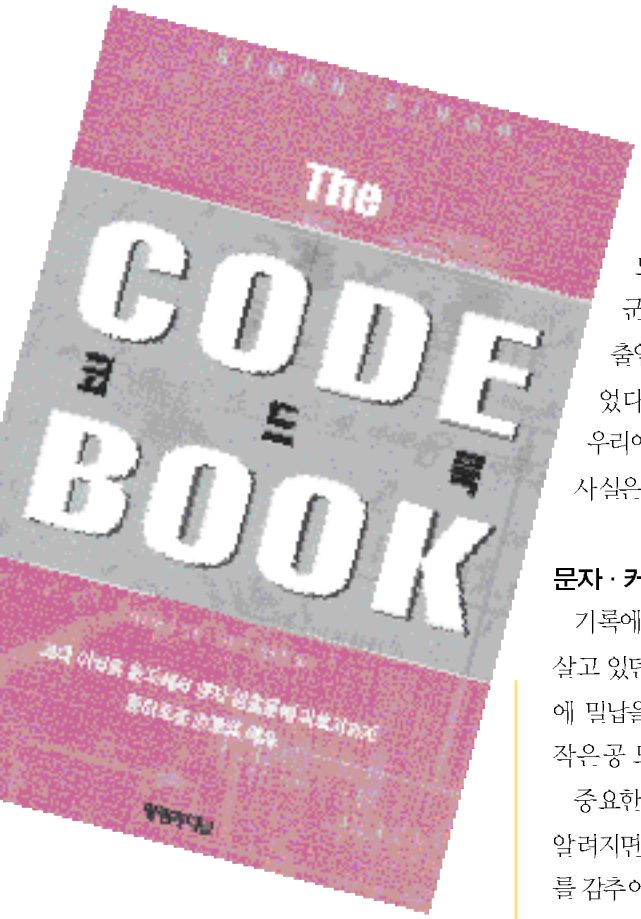
Book

암호의 대중화 … 역기능 우려

사이먼 싱의 코드 북



사이먼 싱 지음 | 이원근, 김희정 옮김
영림카디널 | 2003

암호는 인류가 문자를 사용하기 시작하면서 함께 등장했을 것으로 짐작된다. 발신자와 수신자만이 이해할 수 있는 방법으로 메시지를 전달하는 암호는 처음에는 주로 군사와 정치적인 목적으로만 사용되었을 것이다. 오늘날에도 가장 복잡한 암호 체계를 사용하는 곳은 역시 국가의 안보를 책임지고 있는 군사 분야인 것은 사실이지만 컴퓨터의 작동, 은행에서의 입출금, 보안 시설의 출입, 그리고 인터넷 상거래 등에서도 암호는 절대적으로 중요한 역할을 하게 되었다. 과학과 기술의 발달로 과거 어느 때보다 밝고 투명한 사회로 발전하고 있는 우리에게 어딘가 음침하고 어두운 냄새를 풍기는 암호가 필수품이 되어가고 있다는 사실은 역설적으로 보이기도 한다.

문자 · 커뮤니케이션 정보의 함수관계

기록에 남아있는 최초의 암호는 기원전 480년경 스파르타에서 추방되어 페르시아에 살고 있던 데마라토스가 조국을 잊지 못하고 페르시아의 침략 계획 소식을 적은 나무판에 밀납을 보낸 것이었다고 한다. 고대 중국에서는 전령사에게 글을 적은 얇은 비단을 작은 공 모양으로 만들어 밀납으로 싼 것을 삼키게 하는 방법도 사용했다고 한다.

중요한 메시지의 존재를 감추는 '스테가노그래피'의 군사적, 정치적 효용성이 널리 알려지면서, 이제는 단순히 메시지의 존재를 감추는 정도가 아니라 메시지의 의미 자체를 감추어버리는 '크립토그래피'가 발전하게 되었다. 겉보기에는 평범하게 보이는 문서에 일정한 '암호화' 규칙에 따라서 중요한 정보를 감추어두는 방법이 바로 그것이다. 물론 감추어진 정보를 읽어내기 위해서는 암호화 과정을 거꾸로 반복하는 '복호화' 규칙이 필요하다. 20세기에 들어 컴퓨터가 발전하면서 암호화와 복호화의 과정은 고도로 복잡한 수학의 한 분야로 자리잡게 됐다.

치열한 경쟁속에서 잉태된 암호

사실 인류 역사에서 겉으로 크게 드러난 적은 없으면서도 가장 치열한 경쟁이 끊임없이 이어져왔던 분야가 바로 이와같은 암호학이라고 한다. 암호는 전쟁의 성패와 왕들의 생사를 결정하는 요인이 되기도 했고, 땅 속 깊은 곳에 묻혀있던 우리의 역사와 보물을

찾아내는 열쇠가 되기도 했다.

캠브리지 대학에서 물리학을 공부하고 BBC방송의 프로듀서로 일했던 〈페르마의 마지막 정리〉의 저자이기도 한 사이먼 싱의 〈코드북〉은 그런 암호의 진화 과정과 미래를 낱낱이 소개하고 있다. 암호문에 담겨있는 과학적 규칙에는 암호 작성자의 심리 상태는 물론, 암호를 공유하는 사람들의 사회, 문화, 시대적 배경까지 모두 담아내고 있다. 어마어마한 비밀을 감춰두려는 사람과 어떠한 희생을 감수하고라도 그 비밀을 캐내려는 사람들 사이의 치열한 경쟁은 누구에게라도 흥미로운 주제임은 분명하다.

불특정 다수의 컴퓨터를 통해서 전화 통신이 이루어지고 컴퓨터를 통한 전자우편과 상거래가 일상화되고 있는 오늘날, 정보의 보안을 유지하는 일은 디지털 시대의 성공을 보장하는 핵심 기술임에 틀림없어 보인다. 디지털 시대의 핵심인 인터넷은 오히려 개인의 사생활을 더 쉽게 침해할 수 있는 길을 열어주었기 때문에 'PGP'와 같은 보안 시스템이 꼭 필요하게 되었다.

양화가 악화를 구축해 버린 암호

그러나 암호의 '대중화'는 의외의 문제를 양산하기도 한다. 선의의 정보를 지켜주기 위한 기술이 뜻밖에도 사회의 적이라고 할 범죄와 테러 집단의 정보까지 함께 보호해주는 부작용을 낳게 된 것이다. 지난 1995년 도쿄 지하철에 유독 가스를 살포했던 옴 진리교가 자신들의 정보를 암호화하였음이 밝혀졌고, 세계적으로 암호를 사용하는 범죄 집단의 수는 매년 두배 가량 늘어나고 있다고 한다. 이제 암호의 대중화는 국가 안보에도 심각한 위해 요소로 등장하고 있다.

우리는 오늘날 소리없는 인터넷 세상에서 범죄 예방과 국가 안보가 개인의 사생활 보호와 정면으로 대치되는 상황에 처하게 된 것이다. 범죄 예방과 안보를 위해서 사생활의 비밀을 포기하거나, 아니면 모두를 지켜줄 새로운 기술의 개발을 위해 더 한층 노력해야만 하게 되었다.

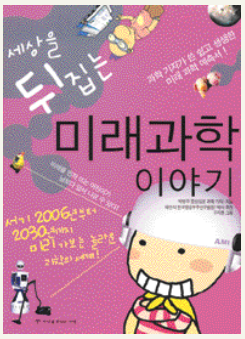
소리없는 전쟁 진행중

얼마 전부터 원자와 분자들로 구성된 미시 세계를 지배하는 양자역학의 원리를 이용한 '양자 컴퓨터'의 가능성이 제기되고 있다. 가공할 만한 연산 능력을 갖추게 될 양자 컴퓨터는 지금까지 알려진 모든 암호화 기술을 한 순간에 초토화시킬 수 있을 것으로 전망된다. 물론 무한한 능력을 가진 우리 인간은 그런 기술의 개발에 성공할 것이고, 그런 기술에 걸맞는 새로운 암호화 기술도 또다시 개발될 것이다. 그러면 또 어떤 사회 문제가 새로 불거질 것인지? 그래서 우리의 삶은 끊임없는 도전의 연속일 수밖에 없는 것일런지도 모르겠다.

글 | 이덕환 서강대 화학과 교수

세상을 뒤집는 미래과학 이야기

박방주 지음 | 채연석 추천 | 구지현 그림 | 9,800원
씨앗을 뿌리는 사람 | 2003



지난 2000여년 사이에 현대 과학과 기술은 우리의 생활을 완전히 뒤바꿔 놓았다. 역사상 처음으로 '평등'과 '인권'을 주장할 수 있게 된 것도 사실은 과학과 기술의 덕분이었다는 역설이 지나칠 만큼. 그런 과학이 지금도 우리의 생활을 하루하루 다르게 바꾸어 놓고 있다. 이미 휴대전화가 일상화되었고, 작은 고깃배까지 인공위성을 이용해서 위치를 파악하는 GPS가 보급되어 있다. 우리의 생활을 근본부터 바꾸어 놓는 과학과 기술의 미래는 과연 어떤 모습일까? 현직 과학 기자의 눈으로 본 '미래 과학의 이야기'를 아동 수준으로 쉽게 풀어쓴 이 책은 어른들이 보기에도 흥미롭기 그지없다.