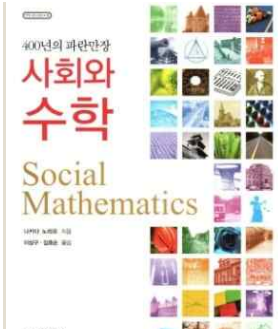


수학사 : 사회와 수학

Week 13

제11장 정보화 사회의 정탐꾼 암호학

1. 암호의 기본과 구성
2. 암호 만들기와 풀기
3. 정보사회와 암호의 활약

이상구(성균관대), sglee@skku.edu

제 11 장

정보화 사회의 정탐꾼
암호학

토용(土俑)으로 밝히는 고대인의 수수께끼

비밀을 지키고 그것을 깨뜨리는 모순

수학 탐방 여행을 서른 번 이상 다녀온 저자는 수학의 역사를 조사하는 일이 고대의 불분명한 부분을 찾아 밝히는'암호해독' 작업과 같다고 느꼈다. 이러한 경험을 통해 '암호'란 동서고금에 광범위하게 존재해왔음을 알았다.

1 암호의 기본과 구성

암호는 어디에 있고, 어떻게 도전할 것인가?

도쿠가와 막부 말기에 교토 미부(壬生)에 군대를 가지고 막부의 죠슈(長州) 낭인의 활약을 제압한 무사조직에서는 첩보나 정탐을 행하는 '감찰' 부서가 있었다. 이 부서는 주로 외부의 움직임이나 정보 탐색을 임무로 했다. 일본 제국주의 군부 헌병과 비슷했다.

규모나 크기는 달라도 일본의 육군 나가노 학교(스파이 양성)나 미국 국무성의 CIA, 구소련의 KGB 등 거의 모든 국가나 사회집단에는 이런 조직이나 기관이 존재한다. 보통 회사에서도 인사부나 인사과라는 부서가 있는데 그런 종류의 역할을 다소 수행한다고 할 수 있다.

이 조직에서 가장 중요한 일이 '외부의 암호해독'과 '부서 혹은 동료 사이의 비밀 유지'로, 전쟁이나 평상시에 한하지 않고 암호가 갖는 역할은 매우 크다.

예전에 미국은 일본과 전쟁한 지 1년도 되기 전에 미육군 신호정보대(SIS)가 일본의 암호해독에 성공하여 일본이 사용하고 있던 암호기 '퍼플(PURPLE) 암호기 B형'(97식 영문자 인쇄기)의 모조품을 완성시켰다고 한다.

그 시점부터 이미 일본의 비밀은 미국에게 읽혀졌고, 전략 전술은 물론이거니와 대소련 공작이나 화평공작의 비밀이 완전히 상대방에게 읽혀졌으니 패전은 시간문제였던 것이다.

평화를 지속하고 있는 것처럼 보이는 현재도 정치, 외교, 기업, 통상의 모든 대외전략에서 암호가 필요하다.

수학 퍼즐 놀이가 암호해독이기도 하다

수학의 즐거움에는 퍼즐을 푸는 것과 비슷한 점이 있다.
'퍼즐을 풀다.' 이것은 그야말로 암호해독이다. 다음 문제에 도전해 보자.

예 1 복면산(覆面算)

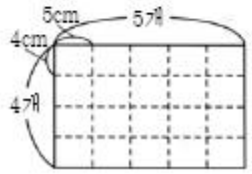
아래의 계산이 성립하도록 각 문자를 숫자로 바꿔라.

$$\begin{array}{r} \text{AM} \\ +\,\text{HO} \\ \hline \text{BUB} \end{array} \left(\begin{array}{r} \text{암} \\ +\,\text{호} \\ \hline \text{법} \end{array} \right)$$

예 2 $x^4+x^2y^2+y^4$을 인수분해하라.

(힌트) $(x+y)^2=x^2+2xy+y^2$

예 3 불가사의 도형. 둘로 잘라서 정사각형을 만들어라.



2 암호 만들기와 풀기

'테루쿠하노루'*라는 살인범

앞에서 제시한 것처럼 수학의 영역 중에는 퍼즐을 다루는 부분이 있다. 퍼즐을 푸는 것 또한 일종의 '암호 해독'이라 할 수 있다.

전 세계에서 일하는 암호 작성이나 해독에 관련된 연구원의 대부분이 수학자인 것은 잘 알려지지 않았다.

아무튼 컴퓨터를 이용하는 수학영역에 '암호학'이 포함되었고, 조만간 교과서에 암호학이 등장할지도 모른다.

사실, 최근의 범죄에서는 범죄자가 암호와 같은 '범행성명'을 제시하는 사례가 많아졌기 때문에 그 대응책이 필요하다.

오래전 예로는 '괴인21면상(怪人21面相)'이 있고 최근에는 '사카기바라(酒鬼薔薇, 술도깨비 장미)'** '테루쿠하노루'가 그 예이다. 연령 미상으로 세상을 놀라게 하고, 그 반응을 즐길 목적으로 저지르는 범죄자, 다시 말해 '사이코패스(유쾌범, 愉快犯)'이다.

그때마다 이 분야의 전문가나 추리소설가 그리고 많은 평론가들이 가능한 범인에 대하여 논하고 추측하지만, 범인의 윤곽은 물론 나이조차도 맞추지 못하고 실망시키는 예가 종종 있다. 이러한 문제들은 '과거의 상식'으로는 풀기 어렵다.

더 논리적인 발상이나 수학적 센스를 가지고 있지 않으면 이러한 해독은 곤란할 것이다. 이것들과 직접 관계가 있다는 것은 아니지만, 매스컴 관계자의 암호에 대한 관심으로 최근 암호해독의 도전이나 스파이 이야기가 신문기사나 TV방송에 많이 나온다.

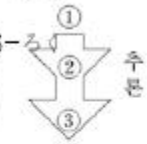
교토 초등학생 살해 사건 '테루쿠하노루'의 해독

(최초의 안)　(10-ten/6-ろく(루)/9-く(루)/8-はち

테 르 그 와 노 르　(하)/-の(노)/(루))

10 6 9 8 - 6　(숫자변환)

도 라 루 에 - 6　(50음에 변환)



(최종안)
'어떤 살인의 책' 중의 각 격언의 맨 끝 글자를 나열한 것.
★ 본인이 자살했기 때문에, 정확한 해석은 알 수 없다

① 「てるくはのる」と「酒鬼薔薇結ぶ点と線」
② 京都 「てるくはのる」の謎を解く「暗号遊び」と「動物虐待」!
③ 犯行声明の「てるくはのる」格言集の文字並べる


暗号解読者に1000万円
NTTが研究者らに挑戦状

(1989. 8. 31　朝日新聞)


WANTED
解読できたら
暗号 賞金1000万円
ソフト会社がコンテスト

(1999. 11. 11　朝日新聞)

① 교토, '테루쿠하노루'의 수수께끼를 풀다. ② '암호놀이'와 '동물학대', ③ 범행성명의 테르그와 노르 교본집의 문자를 병렬.

세계의 암호학자에게 도전. (1990년 3월 6일) - "암호는 화살한 수학적 구조를 가진 미학(美學)"이라고 말하는 암호학자인 전 도쿄공대 츠지이(辻井) 교수는 현상금 2000달러를 붙인 암호를 발표했다.

3 정보사회와 암호의 활약

입소문과 신용금고의 도산

다음은 혼잡한 지하철 안에서 두 명의 젊은 직장여성의 사소한 대화가 큰 사고를 만들 수 있는 예이다.

"너, 취직됐니?"

"응, 저 있잖아, XY신용금고야."

"그래? 네가 근무한다는 그 신용금고 도산될 거야!"

이 얘기를 마지막 문장만 들은 옆 사람이 아는 사람들에게 "XY신용금고가 도산될 것 같으니 빨리 예금을 찾아버리는 것이 좋다."라는 얘기로 확대했고, 그것이 점점 더 확대되어 신용금고 도산소동이 일어나 예금을 찾으려는 사람들로 소동이 일어났다고 한다. 다행히도 견실한 신용금고였기 때문에 일시적인 소동으로 수습되었다는 실화가 있다.

이와 같은 것을 이용해, 직장여성이나 여고생에게 '어떤 정보'를 흘려보내 입소문 을 일으키는 사람이 있다. 이런 것을 마케팅 기법에 접목한 것을 '입소문마케팅'이라고도 한다.

생각해보면

일본 최초의 만화

'조수희화(鳥獸戱畵, 새와 짐승 만화)' 속의 수수께끼

여기서 소개하는 새와 짐승 그림은 예로부터 익살스럽고 세속적인 주제로 일본인들이 좋아하는 두루마리 그림이다. 이는 일본만화의 시초라 하여 중요한 문화유산으로 여기고 있다.

그럼에도 불구하고 작자도 제작 연대도 불명확하고 더욱이 현존하는 4권은 제작 당시의 모습과 전혀 달라져 있다고 말한다.

오랫동안 도바소조(鳥羽僧正, 1053~1140; 고승이면서 풍자화로도 유명한 인물) 작품이라고 알려져 왔으나 최근 동일시대 작품인 '연중행사(年中行事) 족자'와 같은 그림체라는 것이 밝혀지면서, 이 작자는 동일인물로 왕실그림작가 도키와미츠나가(12세기)의 작품이 아닌가 하는 설이 설득력 있다.

아무튼 제작품이 보관되어 있던 교토 고산지[高山寺]가 1547년에 불탔을 때 일부가 떨어져 나갔고 그 후에 몇 번 복원되었으나, 종이 이음새에 상처, 그리고 얼룩이 있어서 500년 후인 현재도 완전히 밝히는 것은 암호해독에 가깝다.

천 년간 일본인이 좋아하고 잘 알려졌던 두루마리 그림이기 때문에 빨리 진실이 밝혀졌으면 좋겠다.