高大連携通信

発　行　兵庫県立神戸高等学校総合理学コース部
第 16 号 平成 17 年（2005 年） 11 月 28 日(月)
「高大連携通信」作成に際して 2003 年から、フリーソフト OpenOffice.org を使って全て作成されています。（感謝）

高大連携講義「暗号の科学」（神大・工 森井昌克 先生担当）
11 月 26 日(土) 10:30 から 12:00 科学館 視聴覚室で行われました

テレビ、新聞、雑誌などマスコミで大活躍中の森井昌克先生から、森井研究室で現在行っている研究内容について解説するところから始まる講義であった。その中の一部である「暗号」について今回は取り上げいただいた。

「暗号」は生活の中に定着!

コンピュータの通信、携帯電話の通信、銀行のキャッシュカードなど、生活の全ての分野で暗号技術を抜きに語ることが出来ない。個人の問題だけでなく、国家レベルから、企業レベルまで全ての分野で暗号技術は使われている。

国家レベルでは外交情報、企業レベルでは危機管理技術、研究情報など、個人ではプライバシー保護など、情報の漏洩が大きな問題を引き起こすことも多い。そのため、情報を暗号化して漏洩を防ぐ研究が必要になるのだ。一般社会では、暗号技術は表には見えないように利用されており、情報通信の裏側で利用者に意識しないうちに暗号技術が使われている。情報通信では、デジタル化の裏側で暗号技術とコンピュータの２つによって支えられているのだ。

映画の「U571」での暗号から始まり、現在の情報・通信での暗号へ

U517 という映画の話が登場する。世界大戦中のドイツの潜水艦の名前だが、ドイツの暗号「ENIGMA（エニグマ）」の話から始まった戦争中の暗号の話だった。このように暗号が登場するのは戦争での機密通信が大きく目立つ。また、言葉遊び、推理小説などの「遊びの分野」でも登場する例は多い。現在での暗号利用はコンピュータを介した通信・情報の分野で多くなっている。その代表的な例として、「情報セキュリティの技術」がある。情報ネットワークのアクセス管理（分かりやすくいえばパスワード認証などの個人認証）や通信内容の漏洩を防ぐための暗号化技術などである。また、「暗号」そのものを話題にした小説には、万葉集、聖書などを題材にしたものがある。その多くは、その文献に未来を予言しているとの記述があるというものだ。しかし、科学的な分析をすればそれほど意味のあるものではないようだ。20 世紀末に大流行した「ノストラダムスの大予言」 がその代表で、後から解釈した話であって、暗号と評価できるものではないのだそうだ。

現代の暗号技術 ～ データの機密性、完全性、信頼性をいかに守るか ～

インターネットで使われている電子メールには「データの機密性（他人に見られない）」はありえない。インターネットそのものは通信経路が公開されているのでこれを完全に守りきれることは不可能なのだ。「データの完全性（情報内容が改変されない）」も同様で、「データの信頼性（メール送信者が正しい）」に至ってはスパムメール（迷惑メール）が示す通りに簡単に偽装は可能だ。

暗号とは数学の 「関数（暗号化関数）」、「逆関数（復号化関数）」であるだけなのだから、暗号化関数と、復号化関数をどのように決めるかに暗号技術が決まる。情報は文字列であるのだが、文字を符号化（文字コード）して情報を数値化して関数の変数とする。関数値が暗号文ということになる。

「シーザー暗号」の仕組みから、現代の暗号化技術への発展

暗号化関数を $C=f(M,K_e)$ とする。シーザー暗号は関数が文字コードを１文字ずらすというもの。暗号の鍵 K_e は文字をずらす文字数になる。しかし、文字をずらすという場合の数（アルファベットなら 26 しかない）が少なすぎてすぐに暗号を解読できてしまうので、これでは、暗号といえなくなる。

でも、暗号の鍵 K_e の数を圧倒的に増やせば、全ての場合の数をこなすことが時間的に不可能となるので解読不可能になってしまうはずだ。このような発想で暗号を作れば、最新鋭のスーパーコンピュータでも解読しても、暗号の鍵は 128 ビットサイズで十分に解読不可能とされている（予想外のアルゴリズムにより解読されるかもしれないが...）。したがって、暗号化の関数が知られていても解読されない「暗号」が作れることになる。

解読不能とされてきた暗号でも、暗号化アルゴリズムの欠点から解読されてきた！

世界大戦中に使われた暗号技術は暗号器という特殊な暗号化関数を仕込んだ機器を利用していた。その暗号器を入手してアルゴリズムの欠陥をを突いて全て暗号を解読されたケースは多い。

現代の暗号化技術では、暗号化関数の逆関数を見つけることが不可能とされる関数を使っている。暗号化関数を公開しても解読が不可能なのだ（逆関数も見つけることができないとは限らないのだが...）。

いろいろと異なる暗号化関数が使われると非常に不便なので暗号化アルゴリズムは共通にして広く利用されるようにするべきである。現在、インターネットで利用されている RC4 という暗号がある。暗号化のアルゴリズムは知られてしまっているが、解読は非常に難しい。そのため現在でも使われているのだ。

暗号アルゴリズムは完全公開しないと、暗号アルゴリズム作成者がトラップドア（ある操作で暗号解読できる仕掛け）を組み込むケースが予想される。特定の人がそれを利用して通信を傍受することが出来てしまう。これでは暗号化の意味がなくなる。アルゴリズムは公開されて万人に検証可能な方が良いとのことだ。

「もの」から「情報」へ！　現在は、大きな転換期となっている！

農業革命は栽培の進展で食糧生産を飛躍的に高めてきた。産業革命においては機械化による物品の大量生産に成功した。現在の第３の革命 「情報革命」によって、情報という形のないものの効率化に成功しつつあるとの話は、筆者（志）にも良く分かる。森井先生がいうには物の「所有」から、「利用」への転換が訪れるとのことだ。事実、「お金」の世界では、お札、硬貨という物の形がある「お金」から脱して、情報に変身した「お金」の利用が当たり前となっている。クレジットカード、キャッシュカード、携帯電話マネーなど上げればきりがない。千両箱を蔵にため込む時代ではない。音楽の世界でもその革命が近い。携帯音楽プレーヤー 「iPod」の爆発的なヒットだ。これにより、物である「CD」に変わり、ネット配信での「音楽情報」へと流通する形態が大きく変わりつつある。CD の棚を眺めるのではなく、iPod に何曲収まっているかになりつつある。このように「情報」が「物」と同様に価値あるものとして流通する時代になってくるのは間違いないようだ。

高大連携講義で得たものは何だろうか？

筆者は 2002 年から毎年見てきた神戸高校の高大連携講義だが、どの分野の講義も大変楽しみにしている。また、その講義から得たものも多い。特に専門外の分野である生物学や生命科学に関するものが面白い。

最近の高校生は目先の受験のみに目が向きすぎのようだが、筆者（志）が高校生の頃は、受験など気にせずにいろいろなことに挑戦してきた。高校三年生のときには、授業で日本史があり、そのため歴史に興味を持ち（受験科目は地理！）、中央公論社の日本の歴史、世界の歴史という 10 数冊はある大部（図書館にあります！）に挑戦し読破したり、東洋文庫という緑の小型全集（これも図書館にあるようです）にも興味を持って楽しんだりもした。南総里見八犬伝（原文）を読破したのも同じ時期だった（これは受験に関係しているが...）。

受験とは関係ないものほど、現在まで人生の上で大変有意義なものとして役立った。専門科目は大学に進学してからいくらでも学べる機会がある。専門以外の科目こそ勉強しておくことがよい。３年生にいまさらのお薦めだが、１、２年生は十分に時間があるはず。一度挑戦してみてはいかがでしょうか（志）

神戸高校高大連携講義は 2002 年から始まって現在に至っています。高大連携講義の記録「高大連携通信」の既刊分には、行われた全連携講義についての情報が記載されています。ホームページ「物理の小道」(http://tachiro.client.jp) にて閲覧することができます。