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 21 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）は 11 月 26 日(土) 10:30 から 12:00 科学館 視聴覚室で行われます

今回の高大連携講義「暗号の科学」は、神戸大学工学部電気電子学科の森井昌克先生が担当されます。森井先生とは筆者のＨＰ「物理の小道」の運用の中で知り合いになった先生です。ＨＰの中で行われていた素数を求めるプログラミングコンテストの関係で、素数について扱われていた先生のＨＰに筆者が書き込みをしたのが始まりでした。今年度、森井先生が神戸大学工学部に赴任されたことで、高大連携講義をお願いした結果、快く引き受けてくださいました結果実現したのが今回の講義です。

暗号と素数の関係は非常に深いもので、現在の暗号化技術には素数理論が使われています。インターネットなどの通信において 「暗号技術」 は大変重要な技術の一つです。通信径路を情報が伝達される間において通信内容が傍受されたり、改変されたりする恐れがあるからです。重要な情報は暗号化されて伝達されるのが常識です。「信頼性・隠匿性」を確保するためには必須の技術となります。

通信と暗号は切っても切れない関係、忠臣蔵では「討ち入り」の「山」と「川」。

「信頼性・隠匿性」を確保するための暗号技術とはどのようなものでしょうか。次回 11 月 26 日に行われる高大連携講義の「暗号の科学」は暗号がどれほど重要なものなのか、現実の通信でどのように使われているのかについて、研究先端の話題を取り上げていただけるものと思っています。先生とのメール交換の中で、暗号についての歴史の話や、その技術など分かりやすい暗号技術についての講義となる予定です。

文を暗号文に変えること「encrypt」、暗号文を元の文に戻すこと「decrypt」

通信手段にはいろいろあります。古くは「文書（手紙）」でした。相手に届けるためには、情報を伝達する人がいます。伝達する人が文書の中身を見るかもしれません。また、書き変えるかもしれません。それを防ぐにはどうすればよいのか。推理小説作家がいろいろな手段を考案しています。元の文書をある特定の法則性を使って、他人が見ても分からない文書に変換するのです。これを「暗号化（encryption）」といいます。受け取った文書をその特定の法則性を使って、元の文書に戻すのです。これを「復号化（decryption）」といいます。それぞれ動詞形では「encrypt」と「decrypt」といいます。

暗号とはどんなもの？　原始的な暗号化の例を挙げると？

暗号化とは、「文字を変換するルール」を考えることです。数個の単語だけであれば 忠臣蔵の討ち入りのときの 「山」＝「お前は味方か？」、「川」＝「味方だ！」というように適当な語句を対応させるだけで終了です。長い文章の場合、全文字を対応させるのです。「あ」を「い」に、「い」を「う」にと１つずらすという簡単なルール（規則性）で文章を変えるだけでも立派な暗号といえます。「50 音順に１文字ずらす」という「暗号化」の仕組みで作った暗号文は、原文「きみがだいすきです。」　→　暗号文「くむぎ、ぢうせくどせ。」となります。見た目はまったく分からない文章のようですが、専門家にとっては簡単に解読されてしまう暗号文なのです。

この暗号は暗号文を多数集めると簡単に見破られてしまいます。理由は、文字の頻度差があるからです。例えば、文末などの文字は「た」、「す」などの特定の文字が多く出現します。ここまでの文章でも文末の文字のほとんどは「す」になっていますね。だから、暗号文の「せ」は「す」だろうと推察されてしまうのですね。これが糸口となって暗号化のルールを見破られてしまい暗号文とは言えなくなります。

「簡単な規則性」でも暗号文が解読されないようにするにはどうすればよいのか、そこで「科学（数学）」が登場するのです。いわゆる 「暗号の科学」 です。

コンピュータや通信の分野では、文字に番号を付けています。これを文字コードといいます。日本語文字は文字数が多いのでここではその番号を説明しません。ローマ字の文字コードは「ASCII」という名前がつけられた文字コードです。アルファベットのＡは 65 番、Ｂは 66 番、（以下同様）。小文字のａは 97 番、ｂは 98 番、（以下同様）となりますね。このように文字を暗号化するための準備は文字を数値化することから始めるのです。（志）