実験 B「秘密のメッセージ　－暗号の話－」

今井桂子　中央大学　日本応用数理学会
森山園子　日本大学　日本応用数理学会

8 月 8 日（月）【実験・実習】9:00～10:30, 11:00～12:30

タイトル：秘密のメッセージ　－暗号の話－

講師：今井桂子、森山園子

「暗号」というとスパイ映画を思い浮かべますか？なんだか暗いイメージがあるかもしれません。でも、現在の皆さんの暮らしを支える重要な技術になっています。皆さんが毎日使っているスマホに、パスコードを設定していますよね。PC にも ID やパスワードが設定されていると思います。もちろん、クレジットカードには暗証番号やセキュリティコードがあります。これらは、他の人に不正に使われないように、皆さんの個人情報を守っているものです。暗号の歴史を学び、メッセージを安全に伝える方法がどのように変わってきたかを見てみましょう。また、今、社会で使われている暗号の仕組みを、実際に作ってみましょう。暗号を作っても、解読できなければなりませんね。それには、少し数学が必要です。

【メッセージを送る方法】

まずは、遠くにいる相手にメッセージを送る方法です。声は届かないので別の手段が必要になります。古くは、木や火薬に火をつけ、煙をあげることで情報を伝える狼煙（のろし）が用いられていました。狼煙の歴史は古く、中国では紀元前 7 世紀くらいから、日本では約 2 千年前の弥生時代から使用されていたといわれています。実際、中国にある万里の長城（右写真）には 5 千箇所以上の狼煙台が残されています。ただ、狼煙では色を変えるなどでしか内容を表すことが出来ないので、複雑なメッセージを伝えることは難しそうですね。もちろん、手紙を書いて送ると、複雑なメッセージが送れます。でも、秘密にしたいメッセージは途中で奪われるかもしれず、安全に送ることはできないように思います。

【暗号化と復号化】

暗号化とは、伝えたいメッセージをある法則を使って、他の人には意味の分からない情報（暗号文と言います）に変換することです。また、暗号文を元のメッセージに戻すことを復号化といいます。文字情報を第 3 者に分からないようにやり取りする場面を考えてみましょう。最も古典的な暗号の 1 つが「シーザー暗号」です。シーザー暗号とは、各文字を何文字か（K 文字としましょう）ずらしてメッセージを書き換えるものです。もとに戻すときは、暗号文の各文字を反対方向に K 文字分だけずらせばよいことになります。次の図は K=1 のときの暗号化（左図）と復号化（右図）を表しています。たとえば、「ももたろう」を 1 文字ずつずらすと暗号文「めめそれい」ができます。この暗号文「めめそれい」は、もちろん、反対方向に 1 文字分シフトすると、元の平文「ももたろう」に戻ります。シーザー暗号は現代暗号の原型ですが、K を知られてしまうと秘密ではなくなってしまいますし、ひらがなの文字数は 46 なので、K の値を 1 から 45 まですべて試せば解読できて

しまいます。

あいうえおかきくけこさしすせそたちつ．．．

↓

んあいうえおかきくけこさしすせそたち・・・

んあいうえおかきくけこさしすせそたち・・・

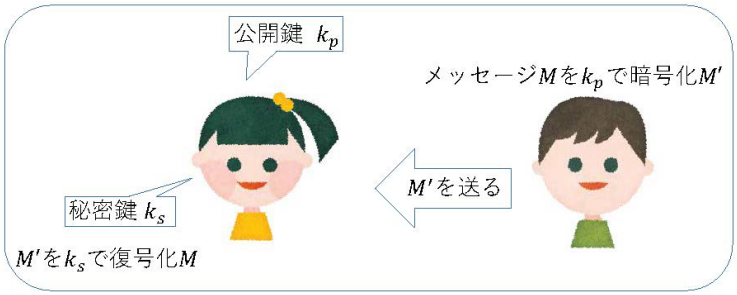
↓

あいうえおかきくけこさしすせそたちつ．．．

共通鍵暗号と公開鍵暗号

シーザー暗号のように送る側と受け取る側で同じルールを使ってメッセージをやり取りする方法と共通鍵暗号方式と言います。共通のルールのことを「鍵」と呼んでいます。長い間、この共通鍵暗号方式が使われてきましたが、この方式では最初に「鍵」を相手に送らなければなりません。また、「鍵」が盗まれると読まれてしまいます。

では、「鍵」を送らなくても良い方法があるでしょうか。「鍵」を送らない方式として公開鍵暗号方式が生まれました。Alice さんに秘密のメッセージを送りたいと思った Bob さんは、Alice さんが公開している鍵を使って、暗号化します。Alice さんは受け取ったメッセージを隠し持っている秘密鍵を使って復号化できます。模式的に描くと左の図になります。こんなことができるなんて不思議ですね。



今、実社会では、RSA 暗号という公開鍵暗号方式が、多くの場面で使われています。今回の実験では、数字をメッセージとしようと思います。電卓を使って自分の公開鍵と秘密鍵を作り、暗号を送りあってみましょう。また、他の人から送られてきた暗号文を復号化して、元に戻ることを確認する実験をします。その仕組みのうらには、フェルマーの小定理という数学が隠れています。数学が安全な社会の構築に役立っていることが分かって頂けたら嬉しいです。

今井桂子（いまいけいこ）

現在、中央大学理工学部情報工学科教授で、中央大学高等学校の校長も兼務しています。夫も大学教員で 25 歳の息子がいます。仕事でも家庭でも沢山のことを掛け持ちしていて忙しくしています。大学、大学院では数学（代数幾何学）を専攻していました。大学では影絵研究会に所属し、幼稚園や保育園で講演を行い、趣味でエレクトーンを弾いたり、スケートやテニスをしたりの日々でした。もちろん、数学に一番多くの時間を割きました。東京大学工学部に就職してから、応用数理、アルゴリズム、特に、コンピュータで図形を処理する方法に興味を持って研究をしています。

森山園子（もりやまそのこ）

現在、日本大学文理学部情報科学科教授をしています。家庭では元気いっぱいな小学生を子育て中です。専門分野を決定するときは、好きだった化学，あこがれだった数学とかなり迷いましたが，90 年代後半に感じた情報の未来にひかれ，大学、大学院では情報科学を学びました。高校時代の勉強不足を悔いていたので，大学時代は家と大学の往復という地味な生活をしていました。情報科学科で学んだ授業「離散数学」との出会いから，研究という世界に足を踏み入れる機会を得ました。幾何学を離散的に見ることに興味を持って研究をしています。