余り計算で分かる映画『サマーウォーズ』の暗号(実演)

所属　一般科目
担当者　中村 博文、他

映画『サマーウォーズ』*1では、暗号や暗号解読(以下、解読)があたり前に出てきて、解説はありません。しかし、一部のシーンは、世界中で広く使われている実際の暗号*2や、実在の解読の公開問題*3や解読*4と関連しています*5～7。

今日は、**その暗号の原理**と、**解読の公開問題**や**解読**を、一緒に**確認**します。

わり算のあまりの面白い性質を使っています。**あまりが主役**です。

対象　あまりの計算ができる小学生 ～ 大人。

所要時間　**２５分**くらい。　毎時０分と３０分に開始（昼休み以外）。　自由席。

実施人数　**２０人×１０回**。同伴者を含む。各回で部屋の入り口への５分前の先着順。

その他　現代社会を人知れず支えている「計算を使って役立つ働きを持たせる**しかけ**」*8のひとつについて、今日、自分の頭で、その**ひらめきを追体験**してみませんか。

aha!

発展（もしよろしかったら、いろいろ調べて、もう少し きわめてみてください。自由研究になるかは提出先に確認を。）

・データを他の人に分からなくするために、うまく作り変えたデータにしてしまうという方法があります。それが**暗号**です。関連して、元のデータのことを**平文**(ひらぶん)、作り変えたデータを**暗号文**、暗号文を作ることを**暗号化**といいます。暗号文を作るとき、どのように作り変えるかを指示するデータを**暗号鍵**といいます。 暗号文を元のデータ（**平文**)にもどすことを**復号**といいます。元にもどすのも、一種の作り変えです。元にもどすために、どのように作り変えるかを指示するデータを**復号鍵**といいます。暗号鍵とペアになっている復号鍵を使わないと、元の平文にはもどりません。 広く使われるように暗号のしくみを公開する暗号を**現代暗号**と呼んでいます。現代暗号では、外部にもらさないのは復号鍵だけです。 暗号鍵も復号鍵も**数**で表します。守りたい情報も**数**に直して扱います。つまり、**現代暗号の正体は計算**です。

例　*送り手*　平文 2　⇒　暗号化（2×2×2÷33）　⇒　暗号文 8　⇒　復号（8×8×8×8×8×8×8÷33）　⇒　平文 2　*受け取り手*

(21 こかけて÷33 で元にもどるので)　暗号鍵 3, 33　……> *盗聴者*　復号鍵 7, 33

・復号鍵を持たない人が、暗号文などから元の平文を導き出すことを、暗号解読とか**解読**といいます。

・鍵は数ですので、その可能性をすべて試せば解読できます。解読に十分長い時間がかかる暗号を**強い**暗号、反対を**弱い**暗号といいます。試し方の工夫や技術の進歩で、だれかが解読に成功すると、強い暗号ではなくなります。暗号は鍵のけた数をふやすと強さがますため、それで強さを保ち続けている暗号もあります。

・声のほか、途中の電波や光や電気の信号からデータを盗むことも、**盗聴**といいます。暗号で盗聴をふせぐことはできませんが、強い暗号を使えば、もし盗難や盗聴をされて解読を試されても、情報は守られます。

・今日とりあげる**ＲＳＡ暗号***2は、**かけた数**を鍵に使っていて、かける前の数がもし分かると、解読が速いことが知られていますが、かける前の数を求める特別速い方法はまだありません。量子ｺﾝﾋﾟｭｰﾀというのが強敵ですが、実用化は遠そうなため、まだＲＳＡ暗号は大丈夫で、世界中で使われています。

・発信元の確認にも、印鑑やサインの代わりにも使えます:
上の図の矢印を逆にすると、2⇐29⇐2。3つ かけて 元の 2 にもどる 29 を作れるのは、7を知る人だけなので。

・年長の方と調べてみては:色々な暗号と解読、素数、フェルマーの小定理、RSA暗号、素因数分解、拡張ユークリッドの互除法、RSA-129、計算量的安全性、RSA暗号解読ｺﾝﾃｽﾄ、公開鍵暗号、秘密鍵暗号、ﾊｲﾌﾞﾘｯﾄﾞ暗号、https、ﾃﾞｨｼﾞﾀﾙ署名、ﾃﾞｨｼﾞﾀﾙ証明書、量子ｺﾝﾋﾟｭｰﾀ、量子ｹﾞｰﾄ型、Shorのｱﾙｺﾞﾘｽﾞﾑ、ﾂｪﾗｰの公式。備考: aha! はマーチン・ガードナーの著書より。

*1 細田守 原作・監督.出版物は 岩井恭著 角川書店、蒔田陽平著 角川つばさ文庫、ｱﾆﾒｽﾀｲﾙ編集部編:ｻﾏｰｳｫｰｽﾞ絵ｺﾝﾃ細田守 ｽﾀｲﾙなど.
*2 R.L. Rivest, A. Shamir, L. Adelman: “A Method for Obtaining Digital Signature and Public-key Cryptsystems,” MIT-LCS-TM-082,1977.
*3 Martin Gardner:“A new kind of cipher that would take millions of years to break,” Mathematical Games, Scientific American, 237(2),120-124,1977.
かけた数 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
*4 D.Atkins, M.Graff, A.K.Lenstra, P.Leyland:“THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE,”Advances in Cryptology - ASIACRYPT ’94.
*5 いぶき: 映画サマーウォーズの暗号を京大生が解いてみた結果, https://reistenza.com/entame/summer-wars.html *6HKNEET:【本気で考えてみた】サマーウォーズのパスワードの暗号の解き方 2056 桁の暗号は解けるのか?,http://win32programmer.seesaa.net/article/421790350.html
*7 サルにも分かる RSA 暗号,http://www.maitou.gr.jp/rsa/rsa10.php
*8 情報を守る、データで印鑑やサインの代わり、データが少し壊れても直す(例:QR コード)、データの量を減らす、一度に沢山のデータを送るなど。

資料ＵＲＬ
(一応年末まで)

このプリント→
(カラー)

関連スライド→
など

https://www.miyakonojo-nct.ac.jp/g21/sw-rsa-p-pdf.htm　https://www.miyakonojo-nct.ac.jp/g21/sw-rsa-s-pdf.htm