授業実践

生徒が発明する公開鍵暗号方式

神奈川県立生田東高等学校教諭　大石　智広

１．はじめに～プログラムで学べること～

この授業は，生徒が公開鍵暗号方式を発明し，なぜそれが解読できないかを，プログラムに触れることで学習する授業である。この授業は，「社会と情報」の中でプログラムを扱うことはできないか，という議論の中から生まれてきた。

「プログラムで学ぶ」のか，「プログラムを学ぶ」のかというキーワードでプログラム教育の目的が語られるが，「社会と情報」という教科であれば「プログラムで学ぶ」が相応しいと考えた。それでは，プログラムで学べるのは，どんな能力や資質だろうか。私は，問題解決力を具体化した「手順化」「検証」を学べると考えている。「手順化」とは，ゴール（解決）までの行動や考えるべきことを細かいステップに分解できる力である。「検証」とは，「手順を実行した結果，ゴールに正しく向かっているか」を確かめる方法を考え，実行する力である。この２つの力は，プログラミング能力とほとんどイコールだ。プログラムを設計し作成する過程は，目的を実現するための手順を書き起こすことにほかならない。手順をコンピュータがわかるように書けば，プログラムになる。そして，デバッグの過程は，どうテストしたら正しく動いていることがわかるか，想定漏れしているケースがないか，など検証の能力をフル活用する必要がある。

このような考えから，プログラムを通して問題解決に必要な力を育む授業の形が見えてきた。問題解決に必要な手順を生徒が考案し，それをプログラムで表現し，実行しながら検証していくという形である。

２．公開鍵暗号方式という題材

「プログラムで学ぶ」題材として選定したのが，公開鍵暗号方式である。公開鍵暗号方式を学ぶ意義は，画期的でかつ社会的に大きな影響を与えていることにある。人類は1970年代まで共通鍵暗号方式と呼ばれる暗号を使ってきた。これは，暗号化にも復号にも共通の鍵を使用するもので，送信側も受信側も同じ鍵を持っている必要がある。この方式の問題点は，通信する相手に鍵を安全に届けなければ暗号通信を行えないことだ。これは，鍵配送問題といわれる。鍵配送問題があるため，鍵を届ける手間と盗まれる危険に加え，初めて通信する相手とは暗号通信できないという欠点を持っている。現在，当たり前に行っているネット通販サイトなどの暗号通信は，じつは鍵配送問題を抱えている共通鍵方式では実現できなかった（利用開始のために実際に会って共通鍵を受け取る必要があったとしたら，誰も利用しなかっただろう）。この鍵配送問題を解決したのが，公開鍵暗号方式である。この発明により，初めての通信から暗号通信を行うことができるようになった。公開鍵暗号方式こそが，今のインターネットを中心とした経済をもたらしたのだ。現代社会の基盤となっている技術の一つであり，学ぶ価値は十分にあると考えた。

一方で，公開鍵暗号方式は非常にシンプルな（わかってみれば）手順でできている。また，公開鍵暗号方式が解読できないのは，素因数分解を高速に行う方法がないという数学的な事実に基づいている。公開鍵を素因数分解すれば秘密鍵を生

成できることは知られているが，巨大な数を使っているため，有効な時間の範囲内で分解できないので解読できないのだ。高校生でも十分に扱えることに加え，これまで当たり前に解いてきた素因数分解が，実は解読できない理由になっている，という事実により数学の奥深さにも触れることができ，生徒の今後の学び続ける姿勢にも影響することができるのではと考えた。

3．　授業のねらいと構成

授業のねらいは以下の3つに整理した。

①公開鍵暗号方式の手順と解読困難性を理解する
②問題解決に必要な手順化と検証を行う
③プログラムに表現することの利点と，検証の必要性を学ぶ

授業は3時間構成とした。それぞれの授業の内容とねらいの関係を，以下の表にまとめる。

時	内容	ねらい
1	公開鍵暗号方式の手順を発明する	公開鍵暗号方式の手順と意義を理解する
2	素因数分解を行う手順を考案・検証する	問題解決の手順化と検証を行う
3	素因数分解を行うプログラムを検証し，実行する	プログラムに表現することの利点と，検証の必要性を学ぶ 公開鍵暗号の解読困難性を理解する

なお，RSA暗号がどのように暗号文を生成しているか，また，どうして公開鍵を素因数分解すると秘密鍵が生成できるような関係になっているのかを理解することは，授業のねらいから外している。これは，対象の高校1年生の数学的知識では理解不能であると考えたことに加え，触れることでかえって，公開鍵暗号方式の手順，解読困難な理由や，その社会的な重要性を理解する妨げになると考えたからだ。

4．授業実践1　公開鍵方式を発明する

導入として，映画『ミッション：インポッシブル』を題材に，暗号を解読してトム・クルーズを救出しよう，という3時間を通した目標を提示している。

(1) アルゴリズムと鍵の概念を理解させる

暗号を理解するためには，アルゴリズムと鍵の関係を理解することが重要である。最初は，宝箱を開ける例を使って，「鍵をさして回すという手順は誰でも知っているが，鍵がなければ開けられない」といった説明を行う。次に，シーザーローテーションを例に説明する。

アルゴリズム	アルファベットを決まった文字数だけずらす
鍵	何文字ずらすか

実際に暗号化と復号を行わせ，暗号化は全員で行い，復号を個別に行わせることで，全員が理解できるように試みている。

(2) 鍵配送問題を解決する必要があること理解させる

シーザーローテーションの欠点という形で，暗号化と復号に同じ鍵が必要なことをあらためて確認する。次に，スパイがたくさんいる世界を想像させ，「鍵を送る」「あらかじめ鍵を渡しておく」という2つの方法に対して，どんな問題が起こりそうか，生徒に予想させる。「鍵を送る」に対しては「途中で盗まれる」といった望んだ答えが出てくるが，「あらかじめ」については教員の補足が必要である。ここでは，twitterやAmazonなどを例に使い，「初めて通信する人と暗号通信できない」ことを確認する。

(3) 公開鍵暗号方式を発明させる

人類が同じ鍵が必要な暗号をずっと使っていたことを説明し，「人類が2000年間発明できなかった鍵を送らなくてよい暗号を発明しよう」と目標を提示する（生徒は失笑する）。

この活動は，最低3人のグループワークで行う。ボブ（受信者），アリス（発信者），トム（スパイ），に役割を分担させる。次に，南京錠，南京錠の鍵，南京錠のかかるケース，手紙を配布する。発明を成功に導くためのポイントは2つある。まず，最初に誰が何を持っているかを確認することである（図1）。

ポイントの2つ目は，生徒の配置である。必ず，ボブ（受信者）⇄トム（スパイ）⇄アリス（発信

図１　持ち物の初期配置

者）の順で座らせる。その上で，ボブとアリスの間で何かを送る時は必ずトムを経由するルールを徹底する。また，トムは見たりコピーしたりすることはできるが，奪ったり破壊したりする操作はできないことを説明しておく（「トムが南京錠を閉めることができるか」という質問はクリティカルである）。

クラスによっては，開始１分以内に見つける班が出てくる。説明や質疑応答を丁寧にしていると，その間に方法を見つけてしまう班が出るので注意が必要である。経験上，ほとんどのクラスで発明できるが，念のためヒントを用意しておいてもよいかもしれない。

(4) 手順を確認し，次の授業へつなぐ

最初に発見したグループに教員がインタビューしながら実演してもらう。その後，教員から手順を文字で示し，改めて手順の確認を行う。各班で再現させてもよいだろう。ここで生徒に納得がいかないところはないか？と発問すると，ほぼ必ず「トムが南京錠から鍵を作れるんじゃない？」という反応が返ってくるので，その方法を次回の授業で考えよう，と次の授業につなげる。

５．授業実践２　公開鍵から秘密鍵を作る手順を考案する

(1) 公開鍵と秘密鍵の関係を理解させる

南京錠と鍵に当たるものとして，素数の積とその因数が使われていることを説明する。そこから，公開鍵を掛け算に分解できれば暗号は解読できると理解させる。ここで，どうやって暗号を作るのかは難しいので説明しない，と補足している。

(2) 公開鍵を掛け算に分解させる手順を考案する

掛け算に分解する手順を個人，グループで考えさせる。ヒントの与え方がポイントで，今年の授業では，１．まず２で割る，２．割り切れなければ３で割る，くらいまでのヒントが必要だった。生徒から出てくる手順は，①１ずつ大きい数で割っていく，②奇数で割っていく，③素数で割っていく，の概ね３つである。発見の状況によって展開は分かれるが，大きな素数が未知であることを理解させ，③以外の①か②の方法のいずれかをそのクラスの採用する手順とする。

(3) 手順が正しく機能するか検証する

(2) で決めたクラスの手順を使って，実際に「公開鍵」を手計算で分解させる。数字は３桁の数字を使い，電卓を利用して行う。また，時間を意識させるため，かかった時間を記録させている。手順を検証した結果を生徒に問うと，「時間がかかる」「間違える」といった声が返ってくるので，それを拾って次の授業に進む。

６．授業実践３　プログラムに分解させる

(1) プログラムに表現することの利点と，検証の必要性を理解させる

コンピュータが与えられた手順を早く・正確に実行できることと，コンピュータがわかるように書いた手順をプログラムと呼ぶことを説明する。また，ゲームのバグを例にとって，プログラムが正確に動作するか「テスト」する必要があることを説明する。

(2) プログラムの検証を行う

公開鍵をセルに入力し，ボタンを押せば素因数分解した結果が表示されるプログラムを教員が用意した（Excel VBA）。ソースは見せるが内容は説明せずに，前回クラスで採用した手順をプログラムとして表現していることだけを説明した。

前回，手計算で行った数字の分解をプログラムに実行させ，正しい答えが出るかテストさせる。

(3) バグとアップデートを理解させる

正しい答えが出ることを確認した後で，「バグがある」と生徒に伝え探させた（小数や１を公開

鍵として入力すると無限ループに入るバグ)。生徒が発見した後に，修正した物を配布し，バグがなくなったことを確認させ，これがアプリのアップデートだというように説明した。この活動はアップデートの意味を理解させる良いアイデアだと思ったのだが，じつは生徒の理解の妨げになっていた。

(4) 巨大な数の分解を実行させる

15桁の数を分解させ，時間を記録させる。本校の環境では 4 秒前後で完了する。なお15桁という数は，Excelのセルに入力できる最大桁数から決めている。

(5) まとめ

実際の公開鍵がもっと巨大であることを生徒に予想させ，実際の桁数が600桁（2048bitを想定）であること，遥かに進化したコンピュータであっても何億年という時間が必要なことを説明する。さらに，今まで考えてきた公開鍵から秘密鍵を作る手順は素因数分解を行う手順であること，素因数分解を早く行う手順がまだ見つかっていないことを説明する。最後に，暗号が解読できないのはなぜかを書かせて授業は終了する。

7．分析

3 回目の振り返りの「暗号が解読できないのはなぜか」という問いに書かれたことから，生徒が暗号の解読困難性を理解できたのかを分析した。ここでの大正解は，「素因数分解を早く行う方法がない」「巨大な数を利用しているため時間がかかる」の 2 つである。分析結果を以下に示す。

時間のみに触れたもの	14人
桁が大きいため時間がかかる	41人
素因数分解を早く解く方法がない	17人
桁の大きさと素因数分解の両方	12人
その他	26人
プログラムが小数を解けないから	9 人

（3 クラス119人の回答を集計）

そのほかは，「解けないようになっているから解けない」といった，理由を示せていないものが多かった。2 つの理由を書くように促すプロンプトはなかったにも関わらず，10%以上の生徒が 2 つの理由を示せている。時間，桁，素因数分解という理由のいずれかを70%の生徒が述べており，多くの生徒に公開鍵から暗号を解読できない理由を伝えることができたと考えている。一方で，寄り道である「バグとアップデート」の活動により，誤った理解を生み出していることもわかった。この部分は，別の機会に潔く譲るべきだろう。

「プログラミングに関してわかったこと」という振り返りには，次のような感想が寄せられた。「自分で計算してみてプログラムのすごさがわかった」「正しく動くとは限らない」「バグがあるからテストする必要がある」という感想が寄せられた。プログラミングで表現することの意義と検証の重要性が伝えられたといえるだろう。

問題解決に必要な「手順化」「検証」の活動を多く取り入れることができたが，生徒の資質として身についているかは不明である。この点は，今後改善していく必要がある。

8．授業の改善案

今回，私が行った授業案のほかにいくつかのバリエーションが考えられる。重視するポイントに合わせて，アレンジすることができる。

シンプル	公開鍵を発明するところまで
ネットワーク重視	SSLの手順を学ぶ 実際の公開鍵を表示させる
プログラミング重視	素因数分解を行うプログラムを作る実習
数学重視	リーマン予想や素数の性質について触れる

9．さいごに

「楽しかった」「スパイの世界を味わえて楽しかった」という感想にまじって，次のような感想を書いてくれた生徒がいた。これから一つでも多く，このような感想を書いてもらえる授業を作り上げていきたい。「私たちは授業で一歩ずつ一歩ずつどうしたらいいか考えていったけれど，きっと人類もこうして一歩ずつやってきたから，今の技術があるんだと思った。」

通巻第 46 号
2018 年 4 月 1 日　発行

©編修・発行　実教出版株式会社
代表者　戸塚　雄弐

発行所　〒 102-8377　東京都千代田区五番町 5
TEL.03-3238-7777
http://www.jikkyo.co.jp/