女子中高生のための関西科学塾 2024
実習「秘密を守るには？ 現代の暗号とその数理」

大阪公立大学大学院理学研究科
菅　徹
松澤　陽介

1. はじめに

「女子中高生のための関西科学塾」は，理工系分野に興味を持つ女子中高生を対象に，大学での実験・実習体験，理系女子学生との交流会，理工系分野で活躍する女性研究者・社会人による講演会，企業見学などを企画，開催する活動です．それらの企画を通じて，

- 理工系の学術分野のおもしろさを伝えること
- 理工系を好きな仲間が大勢いることを知らせること
- さまざまな理工系の仕事があることを知らせること

（関西科学塾ホームページより抜粋）を活動の目的としています．現在，京都大学，大阪大学，神戸大学，奈良女子大学，大阪公立大学の 5 つの大学のうち 1 つがその年の幹事校として運営の中心を担い活動を行っています．「女子中高生のための関西科学塾」に関するさらなる詳細が本誌掲載の細越裕子先生による記事で紹介されていますので是非ご覧ください．

19 回目となる 2024 年度の「女子中高生のための関西科学塾」は A〜F の 6 つの日程で企画があり，そのうち C・D・F の 3 つの日程で，各大学における実験・実習が行われました．筆者らの所属する大阪公立大学での実験・実習は，C 日程の 10 月 27 日に中学生向けの企画として行われました．実験・実習名の一部を挙げてみると，「地震波を解析して，地面の下を解析してみよう！」「実践 PCR！ 遺伝子で身元を突きとめる」「顕微鏡の目：隠された生物の不思議を探る」などがあり，筆者らも（おそらく読者も）思わず参加してみたいと思うものばかりです．数学に関する実験・実習も毎年のように行われており，2024 年度は本稿で紹介するものの他にも，11 月 24 日（D 日程）に奈良女子大学で開催された高校生向けの実習「数学の定理を感じてみよう」が行われています．

タイトルにもある「秘密を守るには？ 現代の暗号とその数理」は C 日程に大阪公立大学で行われた実習です．筆者の一人である松澤は，講師として実習の内容の発案からすべてを担当しました．もう一人の筆者である菅は関西科学塾実行委員として実習のサポートをしました．大阪公立大学大学院の学生の溝口史華さんと山下裕理さんにも TA として実習

のサポートをしていただきました．本稿の残りでは，実習内容の紹介から実際の実習の様子までの詳細を報告したいと思います．

2. 実習内容を決めるにあたって

関西科学塾の講師を私（松澤）は 2023 年度から 2 年連続で担当させていただきました．2023 年度の関西科学塾は私にとっては一般向け公開講座の講師を務める初めての機会でした．高校生の頃に高エネルギー加速器研究機構主催の Belle Plus や，数理の翼といったサイエンスキャンプに参加し，大学生になってからはそういったイベントの TA を何度か務めたこともあり，その意味でも中高生向けの公開講座の講師を引き受けることは自然なことでした．また，かつてサイエンスキャンプや公開講座から多くの影響を受けた身としていずれは自分もそのような場を提供したいという思いも常々持っていました．

2023 年度の関西科学塾では円周率をテーマに選びました．関西科学塾は実習をするということが大きな特徴なのですが，数学をテーマに中学生でも理解でき楽しめる実習のネタを考えるのはなかなか難しい課題でした．この年はランダムな整数のペアが互いに素になる確率に円周率が現れることを利用してその値を計算するという実習を行いました．ランダムな数のペアは，120 面体サイコロを振ることで生成したのですが，これにより（課題の本質とは関係ないのですが）実習にちょっとした遊びが加わって参加者もより楽しめたのではないかと思っています．この実習のアイデアは私がたまに見ている数学系 YouTube チャンネルの Stand up math から拝借しました．

その後 2024 年度の講師も引き続き引き受けることになった際，2023 年度と同じ内容にするという選択肢もあったのですが，せっかくなので別の話題を選んだ方が面白いかと思い，最終的に暗号について取り上げることにしました．純粋数学からの話題ではなく，敢えて応用数学とも言える暗号をテーマに選んだのにはいくつか理由がありました．

まず一つには，私のポスドク時代の受け入れ教員だったシルバーマン先生が暗号の専門家でもあったということがあります．私は数論力学系と呼ばれる分野の研究を主に行なっており，その関係でアメリカのブラウン大学においてシルバーマン先生の下でポスドクをしていました．ここ 20 年ほどの暗号業界における最大の課題の一つは耐量子暗号の開発だと思いますが，その有力候補とされている NTRU という暗号システムは実はシルバーマン先生を含むブラウン大学の 3 人の数学者によって 1990 年代に提案されたものです．数年前，それまで耐量子暗号の有力候補と目されていた楕円曲線の同種写像ベースの暗号に対して攻撃手法が見つかり，その後 NTRU が急速に注目を浴び始めました．そのような話をシルバーマン先生とする機会があり，それが暗号をテーマに何かやってみたいと思う一つのきっかけとなりました．

もう一つの理由，こちらの方がずっと大きな理由なのですが，それは，近年数学が社会

の中で果たす役割が非常に大きくなってきているという状況を伝えたかったというものです．かつてハーディは『ある数学者の生涯と弁明』で “数学に実用的な使い道は殆どない” と書いていますが，この主張は現代においては正当化は困難でしょう．もちろんハーディが本当に伝えたかったメッセージは，数学者が味わい深いと感じる類の定理や証明には実用的価値では測れない重さがあるということだったと思いますし，その点は時代によって変わるものではないでしょう．しかし，現代では楕円曲線がインターネットの通信セキュリティを支えていますし，深層学習をはじめとする AI の開発にも種々の数学の知識は不可欠です．日常生活で用いられる技術に高度な数学がダイレクトに用いられることはもはやめずらしいことではなくなってきていると言えると思います．私が中高生だった頃，正直なところ数学についてこのような感覚を持っていませんでした．他の自然科学や工学の基礎として間接的には数学が実用的な益を持っているとは認識していましたが，ここまで直接的に社会インフラに関与しているとは思っていませんでしたし，もしかしたら当時から比べても近年は急速に数学の果たす役割が大きくなってきているのかもしれません．このような状況を踏まえて，数学の代表的な応用先の一つである暗号をテーマに選び，数学が社会において果たしている役割を感じてもらえればと思った次第です．

3. 実習内容

暗号をテーマに選んだ当初は，上で触れた経緯もあったので耐量子暗号やその候補である NTRU について紹介できればと思っていました．しかし，NTRU を説明するためには格子や有限体上の多項式環などを避けて通ることはできないので，中学生相手に実習まで行うのは少し難しすぎるという至極当然の結論に至り，結局 RSA 暗号を取り上げることにしました．

さらに，RSA 暗号の数学的内容というよりは，それを用いた実際のメッセージのやり取りや解読を体験するという部分に焦点を当てることにしました．というのも，この関西科学塾には中学 1 年生もそれなりに参加するので，RSA 暗号の数学的側面をしっかり解説するにはそれなりの時間が必要になってしまいます．関西科学塾では実習を行うことを主眼としているので，そこに時間はあまりかけたくないという事情がありました．もちろん数学の定理をみんなで考え議論し証明するというのは，実は数学の実習としては王道と言っても良いと思うのですが，今回は実社会でどのように数学が使われているかを伝えることがテーマだったのでその部分は諦めた形です．

実習にあたっては，参加者を二つのグループに分けて，RSA 暗号を使ってグループ間でメッセージをやり取りしてもらうことにしました．実習の前半では，それぞれのグループで RSA 暗号の秘密鍵・公開鍵を生成し，それを用いて公開鍵暗号のプロトコル通り，相手グループの公開鍵を使ってメッセージを暗号化し送信することを行います．さらに，実習

の後半では，メッセージを自分の公開鍵で暗号化し，それを相手グループに解読させることも行います．すべての計算を手で行うのは仮にできても時間がかかりすぎるので，各グループには計算用のパソコンを１台ずつ与えて利用してもらいます．

RSA 暗号を使ってメッセージのやり取りをするには，文字と数字の対応を決めておかなければなりません．実際に実用化されている RSA 暗号での文字と数字の対応がどうなっているのか私もちゃんとは把握していないのですが，実習ではこの部分は単純化して，右図のように五十音と数字などを 1 から 65 の数字に対応させる表を作りそれに従って数字と文字を変換してもらうことにしました．

文字	番号	文字	番号
あ	1	む	33
い	2	め	34
う	3	も	35
え	4	や	36
お	5	ゆ	37
か	6	よ	38
き	7	ら	39
く	8	り	40
け	9	る	41
こ	10	れ	42

鍵生成やメッセージのやり取りに先立って，最初に RSA 暗号の原理を説明しておく必要がありますが，そこでは以下のような方法を取ることにしました．まず RSA 暗号は以下の性質を持つ自然数の組 (n, e, d) だと紹介します：すべての整数 m に対して

$$m^{ed} \text{ を } n \text{ で割った余り} = m \text{ を } n \text{ で割った余り} \quad \cdots \quad (*)$$

が成立する．この設定で，RSA 暗号によるメッセージ送受信のプロトコルと，その正当化まではきっちり説明します．さらに，このような組を生成するアルゴリズムが大切なわけですが，以下のような一般的に用いられているものをそのまま紹介することにしました：

Step 1 素数 p, q を選ぶ．

Step 2 $n = pq$ とする．

Step 3 e を $1 < e < (p-1)(q-1)$ および $\gcd(e, (p-1)(q-1)) = 1$ となるように選ぶ．

Step 4 $de + l(p-1)(q-1) = 1$ となる整数 d, l を見つける．（「ユークリッドの互除法」で求めることができる．）このとき，(n, e, d) は RSA 暗号を実現する組となる．

このアルゴリズムがなぜ RSA 暗号を与えるのかの説明にはフェルマーの小定理や中国式剰余定理かそれと同値な何かは必要だと思います．今回はその点は省略し，実際にこの方法で作った RSA 暗号でメッセージのやり取りを行なってもらうことで，正当性を体感してもらうことにしました．

また，暗号なので解読の困難さが最も重要なわけですが，公開されている n, e から秘密鍵 d を求めるには p, q を知らなければならなさそうであること，そして p, q を知るには n を素因数分解しなければならずそれは n が大きい場合大変そうであることを実習の最後に説明することにしました．実習では p, q として高々数桁くらいの素数しか用いることがで

きないと予想されるため，実用的に用いられる素数のサイズを感じてもらうために Mac のターミナルで RSA 暗号を生成しそこで用いられている素数 p, q を見せて実習の締めとすることにしました．せっかくなので実際に紹介した素数を書いておきます．

$p = 172712311076899717673696031523866656535852985898618819379408652403$
$777580945592971996072441326899903491495462055569382394181803607427709$
$059009698602743768338899388649859604517688317115443458941372419318695$
$626840179454699724274894578819560031180457886676485825042192660337238$
$590276934540727728266772360983202213$

$q = 142663793485506807084012852246511904649527124591694566975632221863$
$230444467970177376670114337338327635969175714019230657250802180953835$
$273872289062104943304933261598824895971511450114054176186984597247233$
$770587567517870975805269820563686966819314585758219936883043308146423$
$974944622620831231398740758113878961$

4. 実習開始！

今回の実習で設定していた募集人数は 15 人でしたが，それに対し参加希望者は満員となりました．実習ではまず最初に暗号が現代社会においてどのような場面で使われているのか，どのような暗号があるのか，などの基本的な事柄について説明しました．その後，グループに分かれての実習のために，RSA 暗号がどのような手順で作られるのか，どのように解読されるのかについて解説し，グループ作業にうつりました．

まずはグループごとに，前節で述べた **Step 1**，つまり素数 p, q を選ぶところから始めて，**Step 2** から **Step 4** までをたどって順に n, e, d を求めていきます．そして公開鍵である n, e を相手グループに渡します．次に，渡された公開鍵を使って暗号文を作る作業に入ります．最初に五十音を数字に対応させる表を使って，各グループで考えた短い文章を 1 文字ずつ数字に変換します．変換された数字の 1 つを m とします．ただし p, q をある程度大きくとっておいて m が $n = pq$ 未満になるようにしておきます．相手グループからもらった公開鍵 n, e を用いて，$c = m^e$ を n で割った余りを計算します．この c が，考えた文章のうちの 1 文字を表す暗号となります．

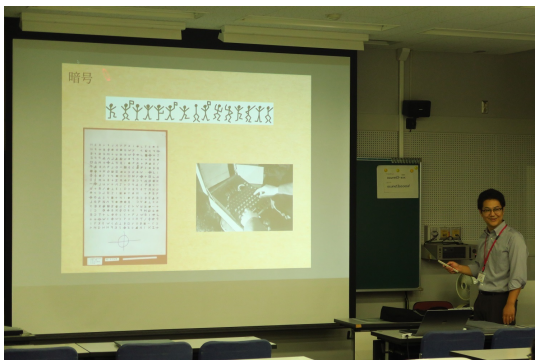
グループ作業では，1 枚の大きな紙をグループ全員で共有して数字を書きこんでいきます．作業が始まって間もなくは多少の緊張も見受けられましたが，1 文字ずつ暗号化していく過程でどんどん緊張がほぐれ，作業を楽しんでいる様子が感じられました．作業が進む

につれて，計算機を使って数値を計算する係，求めた数値を紙に書く係など，中学生が自主的に役割分担を行っていく様子に感心してしまいました．

実習の前半のクライマックスである，暗号文の解読に入ります．上の手順で作成した暗号文を相手グループから受け取り，それを暗号化する前の文章に戻してどのようなメッセージが送られてきたのかを明らかにします．受け取った暗号文は，上で求めた $c = m^e$ が複数個（その個数が暗号化する前の文章の文字数）集まって構成されています．自分のグループで持っている秘密鍵 d を使って，$c^d = m^{ed}$ を n で割った余りを計算します．前節に述べた性質 $(*)$ と m が n 未満であることから，この余りは m に一致し，暗号化する前の文字が解読されたことになります．

暗号文が解読されたときには，最初の緊張感を忘れるほどの盛り上がりとなっていました．手で計算する場面もたくさんありましたが，時間がかかりすぎる場面ではところどころパソコンあるいは参加者が持っているスマホの計算機を使って計算したので，どちらのグループも解読自体にそれほど時間はかかりませんでした．そこで再び暗号文の作成と解読を行いましたが，2 回目以降になると暗号化するメッセージの文章を考える段階から和気あいあいと作業を行っていました．

盛り上がりを見せたまま，実習は後半戦に入りました．前半では相手グループの公開鍵を使って暗号文を作成しましたが，今度は自分のグループの公開鍵を使って暗号文を作成し，その暗号文を相手グループに解読して（つまり秘密鍵が分からない状態から暗号を破って）もらいます．その場合，まずは秘密鍵を求める作業が必要になります．秘密鍵 d が **Step 1** から **Step 4** の手順で作られていることを前提としているので，公開鍵の一つである n を素因数分解して p, q を求めた後に，**Step 3** と **Step 4** から秘密鍵 d を求める作業が新たに加わる形です．既に作業手順に慣れたどちらのグループもあっという間に解読し，時間の許す限りメッセージを送っては解読する作業を楽しんでいました．



暗号に関する説明の様子

実習の様子

RSA 暗号を暗号たらしめる一番の肝となる素因数分解をパソコンを使って行ったので，実習中には暗号を破る難しさについての体感は少なかったかもしれません．しかし，計算機がなかったら？ という問いに対しては，実習中に現れた 4，5 桁程度の整数の素因数分解でも大変そうだという表情が読み取れましたし，前節に記載したような大きな素数を用いた場合は途方もない計算が必要だということも理解してもらえたと思います．同時に，計算機を用いてもなお，素因数分解が暗号の鍵となるほど困難なことであるという点について関心をもってもらえたように思います．

5. 実習を終えて

延べ 3 時間弱，中学生にとっては長い実習であったにも関わらず，それが短かったと思わせるほどの盛り上がりだったように思います．第 3 節でも述べたように，**Step 1** から **Step 4** で性質 $(*)$ を満たす組 (n, e, d) が得られる理由については説明を省略せざるをえませんでした．しかし，暗号文が正しく解読されていくのを繰り返し経験することで，それが確かに機能しているというのを体感してもらえたと思います．必ずそうなるとは分かっていることでも，実際の数値を当てはめたときに理論値と同じものが出るとやはり「本当にそうなった！」という感動を覚えるものです．そのような体験をしたことで，今回説明できなかった数学的背景について興味をもってくれたのなら良いなと思います．

例年，実験・実習中に保護者の方々が教室を参観してまわるツアーを行っています．2023 年度は，教室に参観に来た際，たまたまプロジェクターにリーマンゼータ関数のオイラー積表示に関する式が映されていました（整数のペアが互いに素になる確率に円周率が現れる理由を説明する過程で出てきました）．当然その実習の中で内容が一番難しい場面で，保護者の方々を引率していた実行委員の先生に「これは…中学生は理解できるのでしょうか」と（冗談半分に）言われてしまい，120 面体サイコロを振って実際に円周率の近似値を求めるグループ作業のタイミングで参観が行われていれば！ と少し感じてしまいました．2024 年度の今回は，ちょうどグループ作業中に参観が行われました．しかしここでもたまたま，各自がもくもくと手計算を行うタイミングで，盛り上がりを十分に伝えられないまま次の教室へと保護者の方々は移動していきました．今ついさっきまでみんなで話し合いながら楽しそうに作業していたんですよ！ と大きな声で言いたくなりましたが，できませんでした．やはりちょうど良いタイミングとはなかなか難しいな…と思いました．しかしきっと参加者本人たちがどんな実習だったのか，実際に感じたものを直接保護者の方に伝えてくれたと信じています．

実習が盛り上がったのは，ひとえに TA を務めてくれた溝口史華さんと山下裕理さんのサポートがあったためです．参加者はそれぞれ別々の中学校から応募しているため，自分以外のほとんどの参加者とは当日初めて会うことになります．グループ作業を行う際，当然

誰もが多少の人見知りをしてしまいます．TA の 2 人が最初に「じゃあまずはみんなで一緒に素数を選んでみよう！」「とりあえず 2 桁くらいの素数で何がいいか考えてみようか」とうまく誘導してくれたおかげで，たちまち緊張がほぐれていくのを感じました．TA の 2 人をきっかけにして，参加者の中でもリーダーシップのある子が発言をすると，それに呼応するように他の子も意見を述べ始めます．そうなるとあとは上で述べた通り，「じゃあこんな風にしたらどうだろう」「じゃあ私はこれを担当する」といった具合いに自主的な動きが生まれていきました．TA の 2 人は，そのような自主的な動きを尊重しつつ，全員が作業に参加できるように声掛けを行うなど場面に応じて適切に対応してくれました．2 人のサポートなしにはこれほどスムーズにグループ作業は進まなかったでしょう．

溝口史華さん（左）と山下裕理さん（右）

実習を行う側が先入観を持つことは避けたいことではありますが，理系分野の中でもとりわけ数学というのは女子学生から不人気なのではないかという心配は多少なりともありました．ところが蓋を開けてみると多くの応募があり，そして参加者のみなさんが目を輝かせて実習に取り組んでいました．今回の実習によって，関西科学塾の目的の達成に，そして数学教育の発展に，微力ながら一役買うことができたのであればと願っています．

謝辞

実習に関する紹介記事の掲載をご提案くださいました『数学通信』編集部の方々に感謝申し上げます．大阪公立大学の関西科学塾実行委員の先生方には本原稿に対するコメントをいただきました．誠にありがとうございました．実習の開催のために，関西科学塾実行委員の皆さまをはじめ，多くの方々にお力添えをいただきました．この場を借りて御礼申し上げます．