暗号を題材にした数学の教材開発：H25体験ふむふむ数学クラブ「暗号のすうり」の実践報告

福井大学教育実践研究　2014，第39号，pp11－20

実践論文

暗号を題材にした数学の教材開発
― H25体験ふむふむ数学クラブ「暗号のすうり」の実践報告 ―

福井大学教育地域科学部　西　村　保　三
元 福井県立足羽高等学校　大久保　裕　介
元 福井大学教育地域科学部　佐分利　　豊
福井工業高等専門学校　坪　川　武　弘
福井県立高志高等学校　福　田　浩　之
福井大学教育地域科学部　松　本　智恵子
㈱福井村田製作所　山　下　敏　明

本稿は，平成25年度に福井大学で開催された公開講座「体験ふむふむ数学クラブ―暗号のすうり」の実践報告である。この公開講座の狙いは，暗号を題材にして，数学が苦手だったという一般の社会人や中高生を対象に，グループによる体験的活動を通して，数学を楽しみながら学んでもらうことである。またそれを実現するカリキュラムを，高等学校・高等専門学校・福井大学の数学教員による協働によって開発することも目標としている。

キーワード：数学教育，暗号，合同算術，アフィン暗号

1．はじめに

第２次世界大戦中，ドイツ軍が使用したエニグマ暗号を解読するために，イギリスでは数学者アラン・チューリングを中心とする暗号研究班によって1944年に世界初の電子計算機コロッサスが作られた（この事実は1976年まで軍事機密として秘匿された）。このように暗号と数学の関係は，専門家の間では以前から知られていたが，近年のように一般の人の間に広く知られるようになったきっかけとして次の２つが挙げられる。１つ目は，1976年にヘルマンとディフィーらによって公開鍵暗号が発案されたことで，特に1977年に発表されたRSA暗号は，それまであまり役に立たないと思われていた初等整数論に応用の道を開いて注目を集めた。２つ目は，90年代以降，情報通信ネットワークの発展に伴い，通信の暗号化が社会にとって欠かせない重要な技術となったことである。特にインターネットが普及した1990年代後半以降，「暗号の数理」というテーマは，数学のわかりやすい応用として，大学の公開講座や出前授業，中高生・一般向けの数学の講習会や科学雑誌などで頻繁に取り上げられるようになった（今井1998等）。また近年，中学・高校の数学の授業においても暗号の教材化の試みが始められている（大澤2001等）。学習指導要領が改訂されたことで，高校の数学活用の教科書（根上他2012）に暗号が記載されたり，数学Ａに「整数の性質」が入ったことで，数学の授業で暗号を題材として使える機会が増えた。また，教科「情報」においても，新科目「社会と情報」において暗号が取り上げられている（岡本他2013，小原2012）。

福井大学公開講座「体験ふむふむ数学クラブ」では，数学を専門としない一般の方を対象に，体験的なグループ学習によって，暗号の数理を楽しんで学べて，数学が社会で果たす役割を理解してもらえるような教材開発を試みた。本稿では，その実践の報告に沿って，暗号の教材化についての考察を行う。

2．授業実践

本講座は，西村が全体を統括して，テキストの作成から進行までをこなした。事前の打合せで今回は暗号をテーマに公開講座を行うという方向性が決められ，講座の２週間前に講師で集まって，講習内容についてアイディアを出し合った。講師の一人である福田が，2011年に福井県立高志高校で行った課題学習を元に前半部の草稿を作成し，それを参考に西村がテキストの全体を構成した。配布テキストにおける講習内容の流れは以下のようになっている。

第１回（10月19日）
(1) 暗号クイズ
(2) 暗号を作ろう
(3) 暗号の歴史Ⅰ
(4) 暗号と数学
　4i）合同式とシーザー暗号
　4ii）アフィン暗号

第２回（11月31日）
(1) 単文字換字暗号（復習）
(2) 暗号の歴史Ⅱ
(3) 公開鍵暗号
　3i）秘密鍵の共有
　3ii）電子署名
(4) RSA暗号

なお本講習は，各回３時間で，参加者12名を４つの班に分けてグループ学習を行い，各班に１名以上講師がファシリテーターとしてついて支援を行う形式で行った。

第１回

(1) 暗号クイズ

始めに，参加者に暗号のイメージを尋ねたところ，推理小説・スパイ・軍隊など古典的なものが幾つか挙がったが，インターネットや携帯電話など現代的なものは挙がらなかった。そこで，まずは参加者がイメージしやすい古典的な暗号を元にした簡単な暗号のクイズを何題か考えてもらった。

問題１.

①次の暗号文で，今夜の晩ご飯は何か，次の中から選びなさい。

「ばたんたたたごたたはたたたたんたはかたたたれたーた　たぬきより」

ア）オムライス　イ）たぬきうどん　ウ）カレー　エ）ラーメン

②ある暗号を使うと，「好き」は「シカ」，「きく」は「カキ」という風に表されます。この暗号で「アサ」と表されるものを次の中から選びなさい。

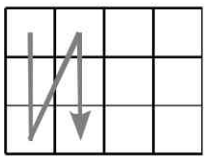
ア）草　　イ）石　　ウ）熊　　エ）梨

③ある暗号で，「虫」は「7・3　3・2」，「鳥」は「4・5・9・2」という風に表されます。この暗号で「7・1　7・4」と表されるものを次の中から選びなさい。

ア）音　　イ）琴　　ウ）豆　　エ）種

④宝の隠し場所を記した紙片を手に入れた（図１）。これに書かれた宝の隠し場所を，次の中から選びなさい。

ア）倉の中　イ）公園の砂場　ウ）池の中　エ）山の上



「このをうすほえなれんば。」

図１：暗号クイズ

答え.

①ウ　「たぬきより」とあるので，「た」を抜いて読む。

②イ　平仮名を１つ後にずらして読む。

③ウ　１桁目は，あ行＝１，か行＝２，・・・，ま行＝７・・・

２桁目は，あ段＝１，い段＝２，・・・，お段＝５を表す。

④イ　方眼の矢印に沿って文章を書いて，横向きに読む。

上記の暗号クイズは，子供向けのなぞなぞでよく見かける易しいものばかりだが，各グループで話し合いをさせて，参加者同士打ち解けあうきっかけ作りを意図している。

暗号クイズの答えを確認する流れで，暗号の原理をシャノンによる模式図（図２）を使って簡単に説明した。暗号とは，送信者から受信者へ，第三者（盗聴者）にわからない手段で情報を伝える手段である。それには，送信者が伝えたい文ｘを暗号文ｙに変換（暗号化）して送信し，受信者はそれを元の文ｘに戻して（復号化）内容を理解する。暗号・復号化する方法は鍵Ｋで決まり，鍵は通信を行う２人だけの秘密として共有される（Stinson 1996，三谷・佐藤2007など）。

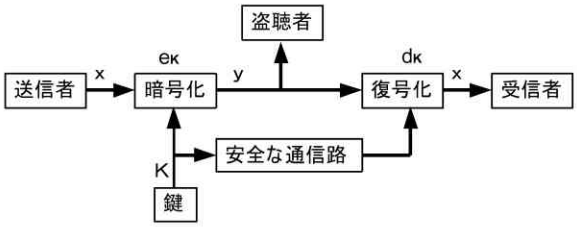


図２：暗号系のモデル

【基本用語と記号】

平文（ひらぶん）ｘ：元の文（例えばx_iを文字として$x=x_1x_2\cdots x_n$）

暗号文ｙ：暗号化された文（例えばy_iを文字として$y=y_1y_2\cdots y_n$）

鍵Ｋ：暗号・復号化するための秘密の鍵

暗号化関数e_k：鍵Ｋによって決まる変換の規則　$e_k(x)=y$

復号化関数d_k：鍵Ｋによって決まる暗号化の逆変換　$d_k(y)=x$

※暗号化関数は，平文と暗号文の一対一対応である。

(2) 暗号を作ろう

次に簡単な暗号に慣れてもらうために，各グループで相談して独自の暗号文を作ってもらい，それを他のグループが解読するというゲームを行った（図３）。ただし難しすぎないように，平文は五七五の俳句か，有名人の名前とし，ヒント（鍵）を付けることにした。それぞれの班から出てきた暗号は，全て暗号クイズ①～④を少し変形したものであったが，実際に暗号を作ろうとすると，「ん」や小さな「ゃ・ゅ・ょ」，濁点や句読点をどうするかなど，意外と考えなければならない点に気付いて，各班で独自の工夫を凝らしていた。この活動は皆，ゲーム感覚で楽しそうに取り組んでいたが，暗号クイズと同じような内容の導入に時間を掛け過ぎて，以降の時間が少なくなってしまったのが反省点である。

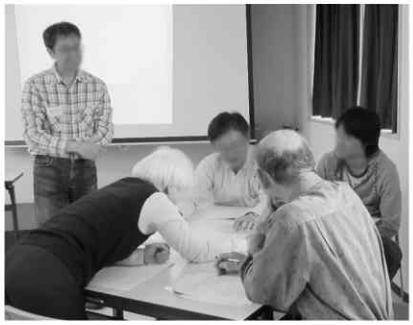


図３：暗号を作ろう

【参加者が作った暗号の例】

3, 4, 7, 21, 11, 16, 28, 17, 23　鍵＝＋3，人名（ローマ字）

この暗号文は平文を＋3したものと考えると，平文は

0, 1, 4, 18, 8, 13, 25, 14, 20

ローマ字を表しているということなので，アルファベット順に0=A, 1=B, 2=C, …, 25=Zだとすると，ABESINZOUとなる。この暗号は，シーザー暗号そのものである。鍵は＋2の方が1=A, 2=B, …となり自然だが，0から始めたのは，テキストの後のページに書かれている符号表（表１）を使ったとのことだった。

(3) 暗号の歴史Ⅰ

各班の作った暗号を説明した後，これまでに登場したような古典的暗号の歴史を簡単に紹介した。古典的な暗号化の方法を大別すると，暗号クイズ①のように余計な文字を挿入する「挿入式」，②③のように文字を置き換える「換字式」，④のように文字の並びを替える「転置式」の３種類がある。②はローマのカエサルが使ったとされることから**シーザー暗号**と呼ばれる。③はさらに古く，ポリュビオスが紀元前２世紀頃に使っているが，暗号というより符号の１種である。④は，紀元前5世紀にスパルタで使われていた「スキュタレー暗号」と同じものであるが，ＴＶドラマ『ハードナッツ！』でも同じものが登場したばかりだったので，参加者から「最近ＴＶで観た！」という指摘があった。このように，古典的な暗号には挿入式や転置式などもあり，フィクションの世界では，しばしば取り上げられているが，今日では暗号と言えばもっぱら換字式を指し，挿入式や転置式は，補助として用いられる程度である。それを踏まえて，この講座でも以降は換字式暗号のみを扱うことを断った。換字式暗号の中でも，シーザー暗号のように，文字を１文字ずつ別の文字に置き換えるものを「単文字換字暗号」と呼ぶ。単文字換字暗号は，推理小説などでもしばしば登場し，エドガー・アラン・ポー原作『黄金虫』(1843)はその最も古く有名な例である。黄金虫は，コナン・ドイル『踊る人形』(1903) や江戸川乱歩『二銭銅貨』(1923) など，多くの小説に影響を与えたことなどを紹介した。

(4) 数学と暗号

4i) 合同式とシーザー暗号

暗号を数式化するために，まず文字を数字に置き換える規則（符号という）を表１のように決めることにした。

表１：アルファベットの符号

文字	A	B	C	D	E	F	G	H	I	J	K	L	M
数字	0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

平文を３文字後にずらすシーザー暗号（A→D, B→E, …）を考える。暗号化の規則は，y=x+3だが，x+3が25を超えると循環的に0に戻って，26=0, 27=1, 28=2, …と考える。これを

$$y=x+3 \mod 26$$

と表す。ここで，a mod pは，aをpで割った余りを意味する。この場合の鍵Kは3であるが，一般に鍵Kのシーザー暗号の暗号・復号化関数はそれぞれ次式で表せる。

$$e_K(x)=x+K \mod 26$$

$$d_K(y)=y-K \mod 26$$

例．MATHEMATICSをシーザー暗号（K=3）で暗号化する。

平文	M	A	T	H	E	M	A	T	I	C	S
x	12	0	19	7	4	12	0	19	8	2	18
x+3	15	3	22	10	7	15	3	22	11	5	21
暗号文	P	D	W	K	H	P	D	W	L	F	V

暗号文は，PDWKHPDWLFV

空白の暗号・解読化の表を印刷したワークシートに，各自で好きな英単語を適当な鍵を使ってシーザー暗号で暗号化してもらい，それを他の人に鍵を伝えて解読するという作業を行った。

定義１．整数aとbをそれぞれpで割った余りが等しいとき，すなわち a mod p = b mod pのとき，aとbは法pで等しいといい，a≡b (mod p) と表す（“≡”の式を**合同式**という）。

命題２．a≡c (mod p)，b≡d (mod p)のとき，次式が成立する。

(i) a+b≡c+d (mod p)，　(ii) ab≡cd (mod p)

注意．$Z_p=\{0, 1, 2, \cdots, p-1\}$と表すと，上の命題から，集合$Z_p$が法pの和と積に関して，**環**と呼ばれる構造をもつことがわかる。

合同式の概念は難しくなく，時計（午後１時＝13時）やカレンダー（曜日は法7，干支は法12等）など日常でも当たり前に使われている。しかし，この説明に“mod”という数学記号を使うと参加者の拒否感が強くなるようだった。命題２は，合同式の計算において，足し算と掛け算は通常通り行えることを意味しており，簡単な曜日計算を例として見せた。特に，合同算術の掛け算の性質を理解するために，法7と法10の掛け算の表をワークシート上に各自で作ってもらった（表２・表３）。

表２：法7の掛け算表

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

表３：法10の掛け算表（0の段は除く）

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
9	9	8	7	6	5	4	3	2	1

さらにそれぞれの掛け算の表に注目して，各$a\in Z_p$に対して，その逆元a^{-1}すなわち$ab\equiv 1 \pmod p$となる元$b=a^{-1}\in Z_p$を見つけるという課題を出した。この計算は，ワークシートの掛け算表の下に，逆元の表を用意して，そこに各自で書き込んでもらった（表４・５）。逆元の意味をすぐに理解できない参加者もいたが，各班のファシリテーターが支援した。

表４：法7の掛け算における逆元

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

表５：法10の掛け算における逆元

a	1	2	3	4	5	6	7	8	9
a^{-1}	1	×	7	×	×	×	3	×	9

表４・５の観察から，aに逆元があるのは，１以外にpとの共通の因数を持たないとき（**互いに素**という）であることは，容易に予想できる（逆は明らかであろう）。この事実は，証明はせずに定理として紹介して，認めてもらうことにした。

定理３．整数aがpと互いに素のとき，かつそのときに限り，$ab\equiv 1 \pmod p$を満たす整数bが存在する。bは法pにおいて唯一つに決まり，b mod pを法pにおけるaの逆元と呼んで，a^{-1}と表す。

定理３より，aとpが互いに素のときに限り，法pの演算においてaによる割り算が行えることがわかる。特にpが素数のときは，Z_pは0を除く任意の元で割り算が行える，**体**と呼ばれる構造をもつことに注意する。

4ii）アフィン暗号

法pの演算に少し慣れたところで，シーザー暗号を少し複雑にした暗号として，**アフィン暗号**を紹介した。表１に示したアルファベット26文字の符号を使い，法はp=26とする。整数の組a，bに対して，次の変換を考える。

$$e(x)=ax+b \mod 26$$

この暗号ではK=(a,b)が鍵になる。特にa=1のときがシーザー暗号である。この暗号が復号化できるためには，関数$y=ax+b \mod 26$がZ_{26}の一対一対応になっていなければならない。これにはaに逆元があることが必要で，定理３から，aが26と互いに素でなければならないことがわかる。このとき，復号化関数は，

$$d(y)=a^{-1}(y-b) \mod 26$$

で与えられる。26と互いに素な数は，1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25の12通りあるので，鍵の組み合わせは12×26＝312通り（自明な１通りを含む）である。

例．a=3，b=2 でMATHEMATICSをアフィン暗号化する

平文	M	A	T	H	E	M	A	T	I	C	S
x	12	0	19	7	4	12	0	19	8	2	18
3x+2	12	2	7	23	14	12	2	7	0	8	4
暗号文	M	C	H	X	O	M	C	H	A	I	E

暗号文：MCHXOMCHAIE

復号化関数は，$3^{-1}=9$だから，$d(y)=9(y-2) \mod 26$となる。

上の例題と同様のワークシートを使って，各自で適当な英単語をアフィン暗号化して，それをグループ内の他の人に暗号文と鍵を教え合って，同様のシートで解読するという課題を出した。もちろん，解読のためには鍵aの逆元を知る必要があり，法26の逆元表を完成させるという課題にも同時に取り組んだ（表６）。この課題の最中に終了時刻となり，これらの課題を仕上げることを宿題として課した。

表６：法26の掛け算における逆元

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

【アフィン暗号の解読】

この部分は，今回の講習において配布テキストで準備はしていたが，時間がなく説明の大半を省略した内容である。単文字換字暗号では，文字の現れる頻度を統計的に分析することで，幾つかの文字の見当が付く。通常の英文の場合，アルファベットは頻度が高い順に，e・t・a・o・i・n・s・・・とされている。例えば，前の例の暗号文MCHXOMCHAIEにおいて，OはEを表し，HはTを表していると見当がついたとする。$e(x)=ax+b \mod 26$という変換で，$e(E)=0$，$e(T)=H \Leftrightarrow e(4)=14$，$e(19)=7$であるから，

$$\begin{cases} 4a+b\equiv 14 \pmod{26} \\ 19a+b\equiv 7 \pmod{26} \end{cases}$$

という連立１次方程式が得られる。下式から上式を引いて，

$$15a\equiv -7\equiv 19 \pmod{26}$$

ここで，$15\times 7=105\equiv 1 \pmod{26}$より$15^{-1}=7$を両辺に掛けて，

$$a\equiv 19\times 7=133\equiv 3 \pmod{26}$$

$$b\equiv 14-4\times 3=2 \pmod{26}$$

暗号化の鍵a=3，b=2が解けたので，他の文字も全て解読される。

第２回

(1) 単文字換字暗号（復習）

まずは前回の復習として，用語の説明と表１の符号表

を再掲し，宿題であった表６の解答を示して，アフィン暗号・復号化の課題をもう一度繰り返した。ここで，講師の山下が作成したExcelファイルを使って暗号・復号化の計算をプロジェクターで写して，参加者全員で確認した（図４）。Excelを使うと，暗号化の計算をその場で確認できるので，とても有効であった。

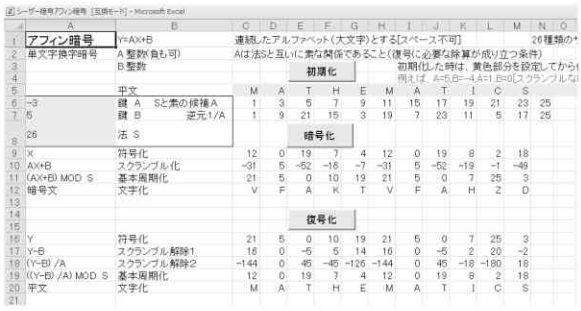


図４：Excelによる暗号の表計算

アフィン暗号の計算によって，合同式に少し慣れたところで，息抜きと称して，アフィン暗号の応用である，次の数当てマジックを演じた。客の選んだ数に色々な計算をさせて，その答えを聞いて客の数を当てるマジックだが，暗号化の鍵（計算）が公開されており，公開鍵暗号の導入にもなっている。

【数当てマジック】
①客に0～9までで,好きな数を決めさせ,電卓に打たせる。
②37倍させる。（ [×] [3] [7] [=] と打たせる）
③53を加えさせる。（ [＋] [5] [3] [=] と打たせる）
④答えの１の位の数を尋ね，演者は客の数を当てる。
〔方法〕①で選んだ数をｘとすると，客の行う計算は y=7x+3 mod 10 である。逆変換は，x=3y+1 mod 10 となり，④で客が宣言した数を３倍して１加えた数の１の位が客の数である。また，演者が電卓を使えるなら，①で２桁の数を選ばせて，④で下２桁を答えさせてもよい。その場合，客の計算は y=37x+53 mod 100 で逆変換は x=73y+31 mod 100 となる。

＜その２＞
①客に1～9までで,好きな数を決めさせ,電卓に打たせる。
②34倍させる。
③47を加えさせる。
④答えの各桁の数を加えさせる（例.149なら1+4+9＝14）。
⑤答えが１桁になるまで④を繰り返させ，その数を答えさせる。
〔方法〕④⑤の操作は，9による剰余を求めている。客の計算は y=7x+2 mod 9 であり，逆変換は x=4y+1 mod 9 となる。

(2) 暗号の歴史Ⅱ
前回の古典的暗号の歴史の続きとして，現代的な暗号の歴史を簡単に紹介した。

(i) ヴィジュネル暗号（多表式暗号）
15世紀に考案された暗号で，文字列を何文字かのブロックに区切って，ブロック毎にそれぞれの文字を異なる暗号表で変換する。例えば，CIPHER を暗号化の鍵とし，これを数字で置き換えて K=(2,8,15,7,4,17)とする。平文を６文字ずつのブロックに区切って，１文字目は２，２文字目は８，３文字目は15，・・・ずらすシーザー暗号を考えると，例えば平文 MATHEMATICS は OIIOIDCBXJW に暗号化される（図４と同様のExcelファイルで実演した）。同じ文字でも異なる文字に暗号化され，解読は非常に難しい。暗号化の鍵の組み合わせはこの場合，26^6＝３億通り以上となる。このように，文字を幾つかのブロックに区切って暗号化する方法を**ブロック暗号**という。当然，ブロック長が長いほど解読は困難になり，ブロック長が平文以上に長く，使い捨てされる場合は，解読は原理的に不可能である（バーナム暗号）。ただしその場合は，非常に長い鍵を通信者の間でどう管理するかという問題が生じる。

(ii) エニグマ
1918年に開発され，ドイツ軍によって第２次世界大戦中に使用された機械式の暗号機（図５）。タイプライターと同様の機構で文字を印字するが，歯数の異なる複数のローターが，１文字打つ度に回転して，長い周期の多表式暗号を自動生成する。復号化も同じ要領で行い，ローターの設定を合わせて暗号文をタイプすると平文が印字される。ドイツ軍が使用したものは，歯車が８枚あり，周期は100億以上であった。あるシステムで暗号の鍵を自動生成していく暗号はストリーム暗号と呼ばれ，携帯電話などでも似たシステムが使われている。

図５：エニグマ暗号機

(iii) DES
1976年に世界で初めて決められた暗号化の標準規格（Data Encryption Standard）で，コンピュータの発達に伴って国際的に広く使われた。フェイステルが考案したブロック暗号の１種で，ブロック長は64bit，鍵長は56bit である。暗号化は，排他的論理和という足し算を使って，ブロックの後半部分に鍵の一部を加えて，ある方法で転置したものをブロックの前半に加えるといった作業を16回繰り返す。DES の暗号は，鍵の総数が現代の

コンピュータにとってはそれほど多くない（2^{56}＝7.2京通り）という理由で，今日では安全とはみなされていない。そこで，鍵を３つ使ってDESを３重に掛ける3DESが多く使われている。また2001年には新しい暗号標準規格であるAES（Advanced Encryption Standard）が決められた。ここでは，パソコンのメールソフトの暗号化設定の画面をプロジェクターで写して，3DESが実際に使われていることを見せた。

(iv) 公開鍵暗号

1976年にヘルマンとディフィーらによって考案された新しい暗号システムである。これに対して，従来の暗号システムは，共通鍵暗号と呼ばれる。本講座の後半では，公開鍵暗号について解説していく。

(3) 公開鍵暗号

3i) 秘密鍵の共有

これまでの暗号システム（図１）では，通信者の間で秘密鍵を共有していなければならない。例えば２人が，以前からの知り合いであれば，２人だけの共通の秘密を使ってそれを暗号の鍵とすることができる。しかし，初めて知り合った人同士ではどうすればよいだろうか？例えば，インターネットで買い物をする場合に，クレジットカードのナンバーを相手先に伝える場合などである。

問題２．インターネットの掲示板で，ＡさんはＢさんと個人的に連絡を取り合いたいと思いました。掲示板は誰でも見られるので，下手に連絡先を書くわけにはいきません。みんなが見ている掲示板のやり取りで，Ｂさんだけにメッセージを伝えるにはどうしたらよいでしょうか？

ヒント：暗号化の鍵として，例えば100以下の数の中から１つを２人だけの秘密として選ぶことができればよい。

この問題を各グループで話し合って考えてもらったが，さすがによいアイディアは出てこなかった。そこで，講師による説明という形ではあるが，アフィン暗号を応用した次の方法を紹介した。

①100以下の大きな素数としてp=97を固定する。以下の計算は全て法97で行う。
②整数kを2から96の間で任意に決める。例えばk=41とする。ここまでのやり取りは公開の場で堂々と行われる。
③ＡさんとＢさんは，自分だけの秘密の数a,bを決める。例えばa=43，b=52とする。
④２人は自分の決めた数とkを掛けて，結果を公開する。
　Ａさんは ak＝43×41＝1763≡17 (mod 97)
　Ｂさんはbk＝52×41＝2132≡95 (mod 97)
⑤２人は相手の結果と自分の秘密の数を掛け算して，結果を秘密の鍵Kとする。秘密の鍵はK＝abk mod pである。
　Ａさんは 95×43＝4085≡11 (mod 97)
　Ｂさんは 17×52＝884≡11 (mod 97)
⑥以上で，２人は共通の秘密K=11を共有できたので，これを鍵として暗号通信を行えばよい。
⑦他の人は，２人がk=41をもとに法p=97の演算でak＝17と bk=95を元にK=abkが共通鍵として決められたことはわかるが，そこからKを求めるには，例えばK=17×95×41^{-1}という計算しなければならず，法97における41^{-1}がわからないと求められない。41の逆元は，41×2＝82，41×3＝26，41×4＝67，・・・と順に当てはめていけば求まるが，pが大きいと大変である。

上記はヘルマン・ディフィーの鍵共有アルゴリズムの原理をこの講座のために単純化したもので，マコーミック2012の４章の解説を参考にした。実際には，掛け算ではなく累乗が使われているという違いはあるが，基本原理は同じである。以上の説明の後，次の課題を各グループで行ってもらった。

課題．上の鍵共有法を用いて，グループの公開のやり取りで２人だけの秘密の数を決めてください。他の人は，２人が決めた秘密の数を当ててください。

前の例の鍵共有法のポイントは，41による掛け算は易しいが，割り算すなわち41^{-1}を求めることは難しいことにある。しかし，41^{-1}は次のような“ずるい”方法を使えば簡単に求められる。

①K=41と任意の数kを決める。簡単のためkも素数から選び，k=29とする。
②Kk－1を素因数分解する。
　Kk－1＝41×29－1＝1188＝2・2・3・3・11
③Kk－1の任意の約数pについてKk≡1 (mod p)なので，適当な大きさのpを法として選ぶ。よい候補がなければkを替えてやり直す。例えば，p=99とすると，法99で41^{-1}＝29である。

このように，法pを後で決めるのであれば，逆元は簡単に求められる。そして，法99で41^{-1}=29であることは上記の計算をした人にしかわからないので，問題１では，Ａさんはもっと直接的にＢさんに「秘密の数xを2～98の範囲で決めて，アフィン暗号化y=41x mod 99して教えてください」と言っても他の人にはxはわからないことになる（これは先の数当てマジックと同じである）。

例えば，Ｂさんはx=52に対して，41×52＝2132≡53

(mod 99)と計算してy=53を伝え，Aさんは復号化の鍵41^{-1}=29を使って，　29×53＝1537≡52 (mod 99)と計算して，x=52を得る。このように，暗号化と復号化に異なる鍵を使うことで，暗号化の鍵を公開して使えるようにしたのが，公開鍵暗号の原理である（図６）。そのためには，暗号化の鍵がわかっても復号化の鍵を求めることが難しいことに加えて，受信者だけには暗号・復号化の鍵のセットをうまく求めることができる抜け道があることが必要である。

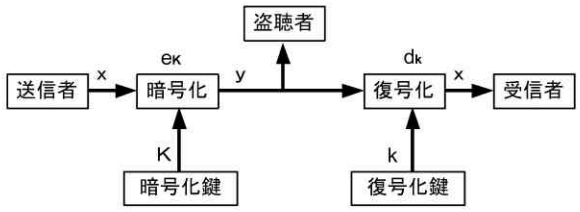


図６：公開鍵暗号のモデル

上の説明の後，実際に自分だけの公開鍵Kと法p，復号化鍵kを作って，できた公開鍵を使ってグループ内で暗号のやり取りを行う課題を出したが，上記の説明を十分理解できなかった参加者が多く，この課題は難しかったようだ。

3ii）電子署名

公開鍵暗号の主な用途は，次の２点であることを補足した。

①暗号化の鍵を，盗聴の危険のある通信で相手に送る。

②電子署名を行う。

まず①について，メッセージ自体を公開鍵暗号で送ってもよいが，一般に，共通鍵暗号に比べて公開鍵暗号は計算量が膨大になるという欠点があるので，実際の通信では鍵だけを公開鍵暗号で送って，秘密鍵を共有したあとは，DESなどの 共通鍵暗号を使ってやり取りするのが一般的である。②の電子署名の原理は，配布テキストには下のように書いて準備していたが，今回の講座では時間の関係で説明を省略した。

例．AさんがBさんにx=36を送りたい場合

①Aさんが知っている復号化鍵k=29を使ってx=36をアフィン暗号化してyとする。y=29×36＝1044≡54 (mod 99) よりy=54

②本文x=36に署名y=54を添付して，X=36・54を新たな本文としてBさんに（必要なら暗号化して）送付する。

③X＝36・54を受信したBさんは，Aさんの公開鍵K=41で署名y=54を復号化する。41×54＝2214≡36 (mod 99) これは本文x=36と一致する。

④Aさんの公開鍵K=41で復号化してx=36になるような暗号化は復号化鍵$k=K^{-1}$を知っているAさんにしかできないので，この通信はAさんからのものだと確認できる。

注意１．上の例では本文のx=36をそのまま暗号化しているが，長い文章だと，署名部分は本文の適当な要約（例えば数字10個ごとにそれまでの合計）で十分である。これを**ハッシュ値**という。

注意２．上記の説明だけでは，公開鍵K=41自体が他人のなりすましである可能性を防げないので，実際には信頼できる第三者機関である「認証局」を設けて，Aさんの公開鍵K=41を登録して，その公開鍵が確かにAさんのものであると証明する。

(4) RSA暗号

(3)では，アフィン暗号を使って公開鍵暗号の原理を説明した。これは，暗号化鍵Kから復号化鍵$k=K^{-1}$が一見簡単にはわからないのがポイントであった。しかし実は高校の数学Aで習う「ユークリッドの互除法」というアルゴリズムがあり，Kの逆元$k=K^{-1}$は高速で求められるので，アフィン暗号では公開鍵暗号としては不十分であることを説明した。

例．法97において41^{-1}を求める方法

ユークリッドの互除法を使って97と41の最大公約数を求める。

$$97=41\times2+15$$
$$41=15\times3-4$$
$$15=4\times4-1$$

最後の1は，97と41の最大公約数が1であることを示している。

今の計算を逆にたどる。

$$\begin{aligned}1&=4\times4-15\\&=(15\times3-41)\times4-15\\&=15\times11-41\times4\\&=(97-41\times2)\times11-41\times4\\&=97\times11-41\times26\end{aligned}$$

従って，$41\times(-26)=97\times(-11)+1\equiv1$ (mod 97) すなわち，$41^{-1}=-26\equiv71$ (mod 97) が求まった。

そこで，実際に使われている公開鍵暗号の例として，RSA暗号を紹介した。RSA暗号についての詳しい説明は，配布プリントには記しておいたが本稿では省略する。講座ではその歴史的経緯と，関連する大きな数の素因数分解の困難さ，フェルマーの小定理，素数判定アルゴリズムなどを「お話」として紹介するだけに留めた。

３．アンケート結果

福井大学COC推進室が実施した参加者のアンケート結果（第１回・第２回）を図７～９に示す。回答数は第１回7／10名，第２回8／8名である。まず図７に示すように，参加者の年代は，第１回に参加した大学生１名を除いて，大半が60～70代と，高い年齢層に偏っている。講習内容の難易度についての質問については，大半が（や

や）難しかったと答えており，参加者に合っていたかは疑問である。例えば，身近な話題としてインターネット通販を例に挙げても，経験したことがない参加者が多く，暗号通信を身近なものとして感じてもらえなかったこともあった。しかし，講座への満足度の質問（図９）では，やや満足が半数，残りが満足か大変満足で，内容が難しかった割には，満足度は高かった。

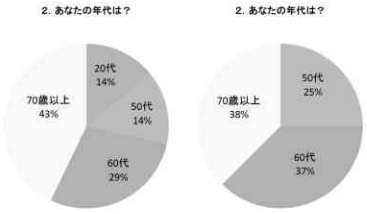


図７：参加者の年齢分布

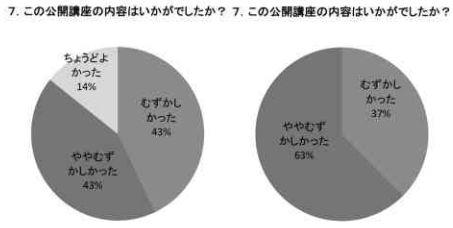


図８：難易度の感想

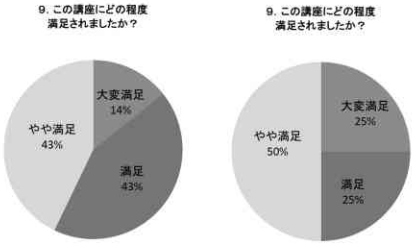


図９：講座の満足度

＜自由記述欄＞

・「余り」を数式表現上“＝”と書かれると，抵抗大！（ex. 3×9＝27＝1 mod 26など）合同式が理解しづらい。（60代）
・みなさんで教え合っている様子がよかった。（20代）
・「mod」とか「41^{-1}（mod 99）」の定義は初めて聞いた。（60代）
・普段使う言葉と違い，modを理解するのに多少手間取った（60代）
・とても興味深かったです。もう一度家でやってみます。（70代）
・日常で使用していない為，納得しづらい課題でした。（50代）
・むずかしかったけど，楽しかった。（60代）

自由記述欄からは，合同式を普段目にしないことへの戸惑いと，難しかったけど楽しかったという感想が述べられており，図８・９のアンケート結果を裏付けている。

４．まとめ

ネットワークの発達に伴い，暗号が生活に必須なものとなった現代において，暗号の数理は，数学のわかりやすい応用を示す格好の題材である。しかし，中学高校の数学の授業において，暗号の教材化は意外に難しく，大澤2001の先行研究などにおいても，生徒に暗号の原理を，実感を伴った形で理解させることはできなかったと報告されている。その原因の１つに，授業者に「暗号の数理＝RSA暗号＝フェルマーの小定理」という意識が強すぎて，その部分の数学的説明に力を入れるあまり，暗号の本質が伝えきれていない面があると我々は考えた。RSA暗号の理解にはそれなりの予備知識が必要であり，単に「法ｎでｘをａ乗してから，さらにｂ乗すれば，フェルマーの小定理でｘに戻る」という原理だけでは，シーザー暗号の「法ｎでｘをａずらしてから，さらにb=n−aずらせばｘに戻る」の原理と同じことで，公開鍵暗号という本質が説明できていない。そこで，本講座ではRSA暗号は基本的に扱わず，アフィン暗号を中心に，合同式の計算から始めて，公開鍵暗号の本質が理解できるようなカリキュラムを考えた。アフィン暗号の場合，公開鍵Ｋを掛けるという暗号化関数に対して復号化の秘密鍵はK^{-1}であるが，これが一見簡単に求められないことを，「落とし戸付き一方向性関数」として利用している。続いて，実際にはユークリッドの互除法というアルゴリズムを使えば，K^{-1}が簡単に求まるという話で，数学の有用性が伝えられる。そこで実際には掛け算ではなく累乗が使われているという流れで説明すれば，（本講座ではそこまで説明しなかったが）RSA暗号も実感を伴って理解できるであろうと考えた。累乗を掛け算に置き換えて公開鍵暗号のシステムを単純化して説明するアイディアは，マコーミック2012を参考にした。その他，暗号の数理のわかりやすい説明と体験型の授業方法は，三谷・佐藤2007，一松1980および小原2012を，また暗号のやや専門的な説明はStinson 1996などを参考にした。

今回の講習では，暗号を題材にした教材開発の面では，うまくいったと思うが，内容の難易度は参加者に合っていたとはいえなかったように思う。しかし，暗号の学習を通じて，参加者に数学の有用性と楽しさを感じてもらうという本講座の目標はほぼ達成できたと考えている。

引用文献

D. R. Stinson著，櫻井幸一監訳(1996)，暗号理論の基礎，共立出版.
三谷政昭，佐藤伸一（2007），マンガでわかる暗号，オーム社.
一松信（1980），暗号の数理，講談社ブルーバックス.
ジョン・マコーミック著，長尾高弘訳（2012），世界でもっとも強力な９のアルゴリズム，日経BP社
今井秀樹（1998），誰もが使える暗号を目指して，数学セミナー3月号，pp. 16–21.

大澤弘典（2001），暗号の教材化についての一考察，日本数学教育学会誌83(7) pp. 10-17.
小原格（2012），見てわかる，体験してわかる暗号化の授業，ICT・Education 49，pp. 16-21.
根上生也，桜井進，佐藤大器，清水克彦，妹背浩也，中本敦浩（2012），数学活用，新興出版社啓林館，pp. 108-111.
岡本敏夫，山極隆（2013），高校社会と情報，実教出版，pp. 64-69.

A curriculum development of mathematics based on cryptography, the report of "Mathematics of Cryptography" Fumufumu H25

Yasuzo NISHIMURA, Yusuke OKUBO, Yutaka SABURI, Takehiro TSUBOKAWA, Hiroyuki FUKUDA, Chieko MATSUMOTO, Toshiaki YAMASHITA

Keywords: mathematical education, cryptography, modular arithmetic, affine cipher