Bulletin of Nagano Women's Junior College Vol.14 21—43, 2016

暗号学習プログラムの提案と実践

長野女子短期大学
久保田　賢　二

要　旨

ネットワークが進展した現代において、暗号技術の習得が必要である。しかし、暗号技術の理解のためには複雑な数学的課題があり、学生の学習意欲を維持しながら暗号の基本原理を習得することが難しい。そこで、授業の中に体験型学習であるコンピュータ・サイエンス・アンプラグドを取り入れたり、シーザー暗号方式で暗号化と復号を体験したりして、学生の学習意欲を維持しながら暗号原理を学習する学習プログラムを提案する。また、その学習プログラムを短期大学生に実践した様子、結果を報告する。

キーワード：

暗号、コンピュータ・サイエンス・アンプラグド、共通鍵暗号方式、公開鍵暗号方式、シーザー暗号、換字式暗号、排他的論理和、一方向性関数、素因数分解問題、ＲＳＡ、モジュロ演算

１．はじめに

Webページの閲覧、電子メールのやり取り、オンラインショッピングおよびネットバンキングなど、インターネットの普及により情報化が進み、私たちの生活はたいへん便利になった。しかしながら、ネットワークの利用に際し、他人に知られたら困る情報、あるいは知られたくない、秘密にしておきたい情報がある。たとえば、クレジットカード番号、銀行の口座番号、個人情報などである。さらに、これらの情報を盗聴されることから守るだけでなく、なりすましや情報の改ざんを防止する必要もある。すなわち、情報を秘密裏に正しい相手に送るための「情報秘匿」と、情報の送り手と受け手が正しい相手であることを証明する「認証」の機能が必要である。これらの「情報秘匿」と「認証」の役割を持つものが、暗号である。ネットワークが進展した現代において暗号の仕組みや基本原理を理解することが求められている。

しかし、暗号の仕組みや技術の背景には、複雑な数学的課題が存在していることが多く、学生の学習意欲を維持しながら暗号原理の理解を促すことは難しい。

そこで、授業の中に体験型学習であるコンピュータ・サイエンス・アンプラグド[(i)(ii)](以下、「アンプラグド」という）を取り入れたり、シーザー暗号方式の仕組みを理解した後、実際に暗号化と復号を体験したりして、学生の学習意欲を維持しながら暗号原理の理解を促す学習プログラムを提案する。アンプラグドでは小学校高学年以上の児童・生徒を対象とした学習プログラムが多い。今回の学習は暗号をテーマとしている。そのため素因数分解やべき乗といった内容を含むため、小・中学生を対象とするのではなく、高校生以上の生徒・学生を対象とした学習プログラムとなっている。

２．暗号方式の学習

暗号方式には、共通鍵暗号方式と公開鍵暗号方式がある。共通鍵暗号方式は、情報の送信者と受信者が同じ秘密の鍵を使って暗号化と復号を行う方式である。公開鍵暗号方式は、情報の送信者と受信者が別の鍵を使って暗号化したり、複合したりしている。たとえば、送信者が公開された鍵を使って暗号化して情報を送信し、受信者は暗号化した鍵とは別の秘密の鍵を使って復号するのである。

ここでは、第一に共通鍵暗号方式のシーザー暗号と換字式暗号を体験しながら暗号の基本原理を理解した後、共通鍵暗号方式での重要な演算である排他的論理和について学習する。第二に共通鍵暗号方式とは発想の違う暗号方式である公開鍵暗号方式の代表であるＲＳＡの基本原理を学習する。

２．１　共通鍵暗号方式

⑴　共通鍵暗号方式とは

共通鍵暗号方式を視覚的に理解するため、平文の文書１枚、道具箱１個、錠前とその錠前を開ける鍵２個を用意した。「平文」（ひらぶん）とは通常私たちが使っている文のことであり、暗号化されていない文のことである。

いま、太郎君が花子さんに手紙を送ることとする。手紙の内容を他人に知られないようにするために、手紙を道具箱に入れて錠前をかける。この錠前を開ける鍵は、太郎君と花子さんしか持っていない。道具箱は運ばれて、花子さんに届き、花子さんは自分が持っている鍵で錠前を開け、道具箱の中の手紙を受け取ることができる。

ここで暗号方式と比較すると、太郎君が道具箱に手紙を入れて鍵を掛けることが「平文を暗号文に換える」ことに相当する。そして、花子さんが道具箱を鍵で開けて、手紙を取り出すことが、「暗号文を平文に復号する」ことに相当する。また、太郎君が持っている鍵と花子さんが持っている鍵でしかこの錠前を開けることができない。暗号化するときの鍵と復号するときの鍵が同じなので、この暗号方式を共通鍵暗号方式という。（図１参照）共通鍵暗号方式には、シーザー暗号や換字式暗号が含まれる。

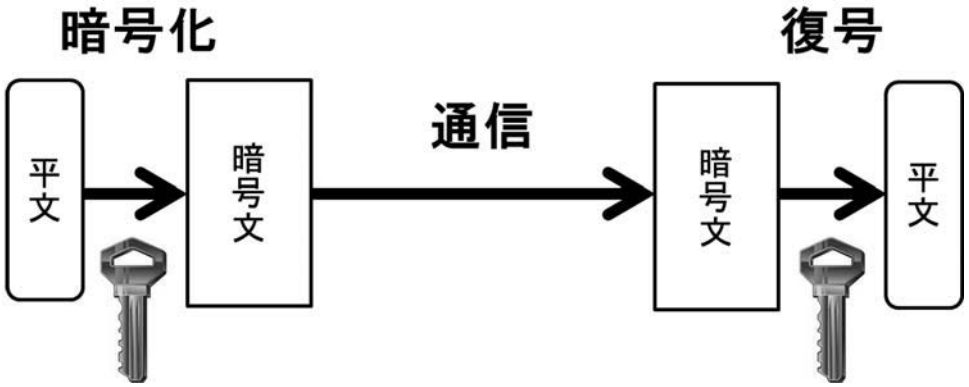


図 1　共通鍵暗号方式

2．1．1　シーザー暗号

学生は共通鍵暗号方式の一つであるシーザー暗号方式で平文の暗号化と、暗号文の復号を実際に行ってみて、共通鍵暗号方式を体験して理解する。

⑴　シーザー暗号とは

シーザー暗号は平文の文字をアルファベット順に何文字かずらして暗号化するものである。たとえば、「NAGANO」（平文）を文字ごとに 3 文字後ろへずらすと、NはQに、AはDにと換えることができ、すべてを換えると「QDJDQR」（暗号文）となる。復号は暗号文の文字を 3 文字ずらして元に戻すことで行うことができる。（図 2 参照）

⑵　学習の目的

- シーザー暗号の仕組みを理解する。
- 暗号で使われる用語を理解する。
- シーザー暗号を実施することから共通鍵暗号方式の仕組みを理解する。

⑶　授業の実践

まず、上記⑴のとおりシーザー暗号方式の仕組みの説明を行った。

シーザー暗号方式の仕組みが理解できたら、次に学生は付録 1（別紙 1）のようにあらかじめ準備した単語を暗号化してみる。更に、あらかじめ準備した暗号文（単語）を復号してみる。

学生が暗号化と復号を実行することができるようになったら、学生自身が単語を考えてその単語を暗

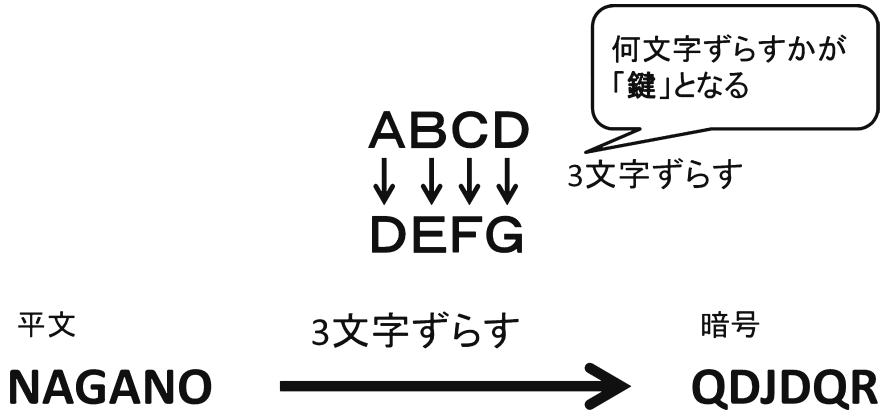


図 2　シーザー暗号の暗号化

号化する。このときずらす文字数は3文字とする。そして隣の学生に、暗号化した単語と、暗号化の鍵となる3文字ずらしたことを伝える。隣の学生はその暗号文を復号する。

これらを体験すると学生は、アルファベット順に「何文字」ずらしたかが暗号化のときと復号するときの「鍵」になっていることがわかる。すなわち、暗号化の鍵と復号の鍵が共通であることがわかる。このようにシーザー暗号の仕組みを理解するとともに、シーザー暗号は共通鍵暗号方式の一つであることも理解する。

さらに、情報の正規の受信者でない者が通信路上で暗号文を取得することを「盗聴」という。盗聴した暗号文を平文に戻すことを「解読」という。（図3参照）ここで、シーザー暗号方式の暗号文を解読することを考える。暗号化の鍵は「何文字」ずらすかであるから、アルファベットは26文字なので、アルファベット順に1文字ずつ文字をずらしたものを25通り作成するとそのうちのどれかに意味のある文が現れる。これで解読が可能である。このようにシーザー暗号は解読が容易なので、別の方式が考え出された。それが換字式（かえじしき）暗号である。

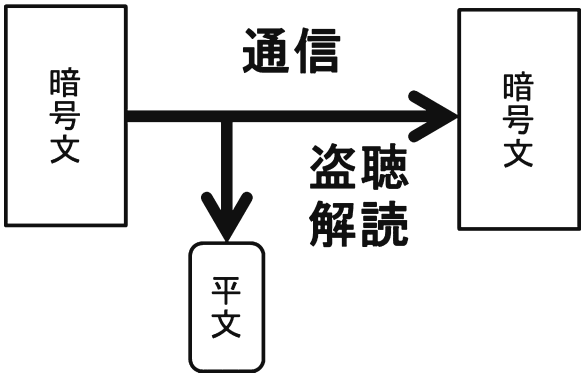


図3　盗聴と解読

2．1．2　換字式暗号

⑴　換字式暗号とは

換字式暗号とは、平文と暗号文の各文字を1対1で異なる文字に対応させる方式の暗号である。たとえば、アルファベット26文字を図4のように対応させて変換すると、平文「ＮＡＧＡＮＯ」は、「ＦＱＵＱＦＧ」となる。この暗号方式では、図4の変換規則が暗号化の鍵となる。

⑵　学習の目的

- ●換字式暗号の仕組みを理解する。
- ●暗号で使われる用語を理解する。
- ●換字式暗号を実施することから共通鍵暗号方式の仕組みを理解する。

⑶　授業の実践

まず、換字式暗号方式の仕組みの説明を行った。換字式暗号は平文の文字を換字式暗号の変換規則に従って暗号化するものである。たとえば、「ＮＡＧＡＮＯ」（平文）を図4に示す変換規則で変換すると、ＮはＦに、ＡはＱにと換えることができる。すべての文字を換えると「ＦＱＵＱＦＧ」（暗号文）となる。復号はこの変換規則に従って変換を戻すことで、行うことができる。

換字式暗号方式の仕組みが理解できたら、次に学生は付録2（別紙2）のようにあらかじめ準備した単語を暗号化してみる。更に、あらかじめ準備した暗号文（単語）を復号してみる。

これらを体験すると学生は、図4の「変換規則」が暗号化するときと復号するときの「鍵」になっていることが分かる。すなわち、暗号化の鍵と復号の

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

QWERTYUIOPASDFGHJKLZXCVBNM

図4　換字式暗号の変換規則例

鍵が共通であることがわかる。このように換字式暗号の仕組みを理解するとともに、換字式暗号は共通鍵暗号方式の一つであることも理解する。

ここで変換規則（鍵）が何通りあるか考える。アルファベットは26個あるので、Ａは26通り変換しうる文字があり、次の文字Ｂは25通りの変換候補があり、次の文字Ｃは24通りの変換候補があり…と徐々に減っていって最後のＺは１通りの変換候補となる。したがって、変換候補のパターンは

$26\times25\times24\times\cdots\cdots\times3\times2\times1\fallingdotseq4\times10^{26}$

となる。（相異なる26個から26個取る順列の数になる。）

一般的に鍵の数が多いほど解読が難しくなると考えられるが、文字を別の文字に変換する方式では鍵の数に限界がある。たとえ換字式暗号の鍵が約4×10^{26}通りあっても、現代の高速なコンピュータによる解析で解読できてしまうからである。そこで、暗号文や鍵を解読されないために、文字を文字コード（０と１のビット列）に変換して、更にそれらを数学的に処理することで解読されにくい暗号ができるのである。この数学的な処理の一つとして、「排他的論理和」という演算がある。共通鍵暗号方式を理解するために欠くことのできない演算である。

２．１．３　共通鍵暗号

⑴　排他的論理和とは

共通鍵暗号方式では、平文の文字を文字コード（０と１のビット列）に変換して、暗号化ではそれらの０と１のビット列に何らかの演算を施して０と１の並びがランダムになるようにしている。０と１の並びがランダムであれば、解読が困難になるからである。しかし、ただランダムな並びにしてわからなくすればよいわけではない。復号ではこのランダムな状態の０と１の並びを暗号化と同じ鍵を使って平文に戻さなければならないからである。

それでは、この処理にはどんな演算が使われているのだろう。

この演算には「排他的論理和」（以下、「ＸＯＲ」という）が使われている。ＸＯＲとは、コンピュータが行う論理演算の一種である。次のように行われる。

１ビットのＸＯＲは次のようになる。

０　ＸＯＲ　０＝０（０と０のＸＯＲは０になる）
０　ＸＯＲ　１＝１（０と１のＸＯＲは１になる）
１　ＸＯＲ　０＝１（１と０のＸＯＲは１になる）
１　ＸＯＲ　１＝０（１と１のＸＯＲは０になる）

長いビット列のＸＯＲをとるときは、同じ桁のビット同士のＸＯＲをとる。仮に、０１１０１１０１というビット列にＡという名前をつけ、０１０１０１０１というビット列にＢという名前をつけたとする。するとＡとＢのＸＯＲは次のようにビットごとにＸＯＲを計算して得られる。

```
        ０１１０１１０１    ・・・Ａ
ＸＯＲ  ０１０１０１０１    ・・・        Ｂ
--------------------------------------------
        ００１１１０００    ・・・Ａ ＸＯＲ Ｂ
```

次に、得られたビット列００１１１０００にもう一度ビット列ＢでＸＯＲをとる。

```
        ００１１１０００    ・・・Ａ ＸＯＲ Ｂ
ＸＯＲ  ０１０１０１０１    ・・・        Ｂ
--------------------------------------------
        ０１１０１１０１    ・・・Ａ
                                （Ａに戻った）
```

すると、得られたビット列は０１１０１１０１で元のビット列Ａと同じになる。

Ａ　ＸＯＲ　Ｂの結果に対して、さらにＢとのＸＯＲをとるとＡに戻るのである。なぜなら、ＸＯＲ演算ではＢとＢの同じ数同士の演算は必ず０になるからである。いわば、Ｂ同士が打ち消しあったのである。

すなわち、同じ鍵を使うＸＯＲ演算で暗号化と復号の処理ができるのである。

- 平文Ａを、鍵ＢでＸＯＲ演算して、暗号文「Ａ　ＸＯＲ　Ｂ」を得る。（暗号化）
- 暗号文「Ａ　ＸＯＲ　Ｂ」を、鍵ＢでＸＯＲ演算して、平文Ａを得る。（復号）

ここで、鍵Ｂの選び方によって強い暗号を作ることができるのである。

実際の共通鍵暗号方式では、換え字処理と転置処理（文字やブロック単位で文字の位置を変える）と

ＸＯＲ演算の組み合わせで処理が行われている。

⑵　学習の目的

●ＸＯＲ演算処理により、０と１の並びがランダムな状態になったものが、またＸＯＲ演算により元の０と１の並びに戻ることを理解する。

⑶　授業の実践

(a)　暗号化

表計算ソフトで図５の「ビット列Ａのパターン」と「かぎＢのパターン」を作りＸＯＲ演算の結果を求める。付録３（別紙３）の手順に従って表計算ソフトを操作する。図５の「ビット列Ａのパターン」は、マス目が16×16で構成され、マス目には０と１が入力されている。１の値はマス目の中でアルファベットのEの形になるように並べている。また、Ｅの形がわかるように赤色に塗ってある。「かぎＢのパターン」は、最初の１行目は０と１が交互に入力され、２行目は１と０が交互に入力されている。これらの２行が繰り返され、16行を構成している。「ビット列Ａのパターン」と「かぎＢのパターン」のそれぞれのビットごとに排他的論理和をとった結果が「暗号文」のパターンとなっている。元の「ビット列Ａのパターン」は「暗号文」ではランダムな０と１の並びになっていることを知る。Ｅの形を見つけることはできない。

ＸＯＲ演算処理は、ＩＦ関数とＡＮＤ関数を使って求めた。（別紙３参照）

(b)　復号

得られた「暗号文」に同じ「かぎＢパターン」のＸＯＲ演算を求め、元の「ビット列Ａのパターン」に戻ることを確認する。（図６参照）

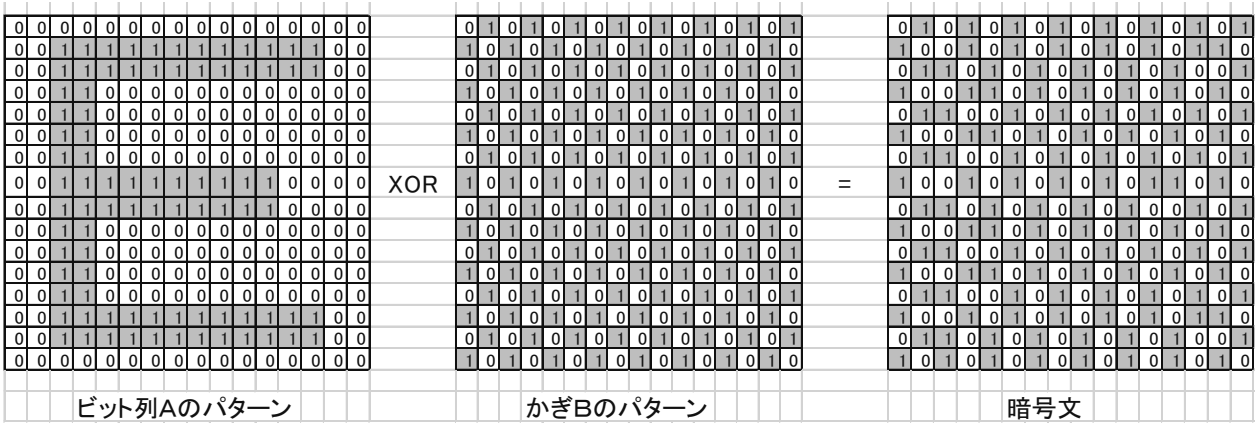


図５　ＸＯＲ演算による暗号化

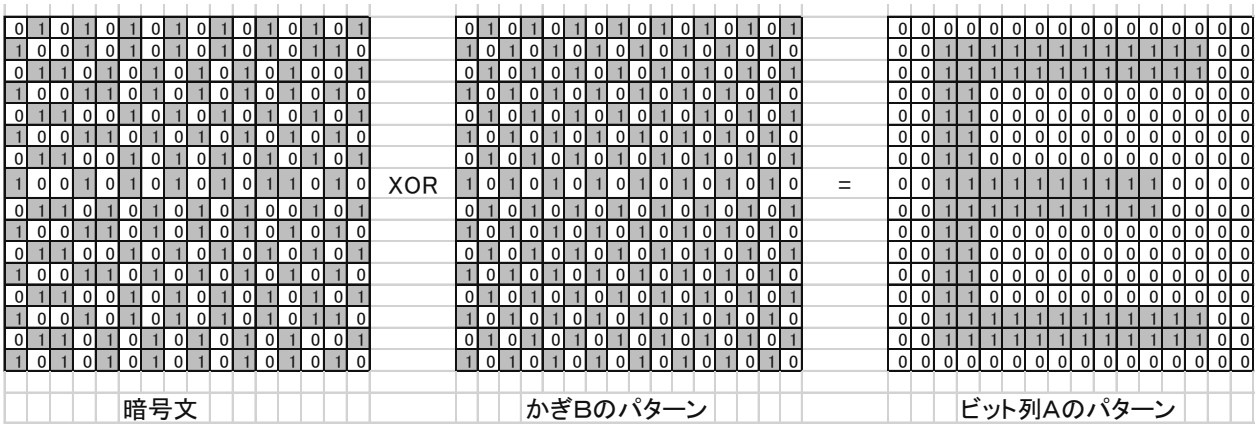


図６　ＸＯＲ演算による復号

０と１の並びがランダムな暗号文から、元のビット列Ａのパターンに戻っていることが視覚的にわかる。

（Ｅの形が見てとれる）

２．２　公開鍵暗号方式

⑴　公開鍵暗号方式とは

共通鍵暗号方式の特徴は、以下のとおりである。

- ●第三者に知られないように共通鍵を情報の正規の受信者に送ったり、保管したりしなければならない。
- ●計算量が少なく高速に暗号化と復号が行えるため、大量のデータの通信に適している。
- ●多数の鍵とその管理が必要となり、不特定多数との通信に適さない。

この特徴の中で、「共通鍵を秘密裏に相手に送らなければならないこと」が一番の問題となっている。遠方にいる相手に直接共通鍵を秘密裏に渡すのには限界があるからである。

そこで、従来の暗号方式と発想を変えて、次のような暗号方式が考え出された。暗号化の鍵と復号の鍵を別にするのである。今、鍵Ａと鍵Ｂがあるとする。

- ●鍵Ａで暗号化した暗号文は、鍵Ｂでしか復号できない。
- ●鍵Ｂで暗号化した暗号文は、鍵Ａでしか復号できない。

ここで、鍵Ａを公開し（公開鍵）、鍵Ｂは秘密にしておく（秘密鍵）。公開された鍵Ａから鍵Ｂは推測できないし、鍵Ａで暗号化した暗号文は鍵Ａで復号できない。このような暗号方式を「公開鍵暗号方式」という。この暗号方式では鍵を公開しておくため、共通鍵暗号方式の問題点であった「共通鍵を秘密裏に相手に送らなければならない」という問題は解決される。また不特定多数との通信にも適する。

それでは、鍵を公開しても暗号文は解読されないのだろうか。

公開鍵暗号方式の原理として、「一方向性関数」がある。一方の向きに計算ができて答えを出すことができても、反対の向きに計算するのが極めて困難な性質を「一方向性」といい、そのような働きを持つ関数を「一方向性関数」という。一方向性関数の問題として、素因数分解問題と離散対数問題がある。

「公開鍵で平文を暗号文に変換することは容易であるが、暗号文を平文に解読することは困難である」という一方向性の性質を利用したものが公開鍵暗号方式である。

この一方向性の性質を学習するため、アンプラグドでは「アイスクリームワゴン問題」を使って学生に説明している。また、アンプラグドを活用した公開鍵暗号学習プログラムの情報科教育への適用例もある。[(iii)]

⑵　学習の目的

- ●アイスクリームワゴン問題を作成することは容易であるが、この問題を解くことは難しいことから、一方向性問題の性質を理解する。

⑶　授業の実践

⑷　アイスクリームワゴン問題

複数の黒丸とこの黒丸を結ぶ線からできている地図を学生に渡す。（付録４の別紙４参照）黒丸は交差点を表し、線は道を表している。今、どこかの交差点にアイスクリームワゴン車を１台止めたい。アイスクリームを買うお客様は一つ隣りの交差点まで歩いていけるとすると、少なくとも何台のアイスクリームワゴン車が必要であるか、また、どこに車を配置したらよいかという問題である。

この問題を解くには、アイスクリームワゴン車をどこかの交差点に置き、その車に買いに来られる範囲の交差点を線で囲む、次に別の交差点にアイスクリームワゴン車を置き、その車に買いに来られる範囲の交差点を線で囲む、ということを繰り返していき、すべての交差点をどこかのアイスクリームワゴン車の範囲に入れればよい。しかし、アイスクリームワゴン車が一番少ない台数で、すべての交差点からお客様はアイスクリームを買いにこられるかとなると、今解いた解が最適解かどうか分からない。総

当りで交差点にアイスクリーム車を置いて解いてみなければならない。この問題を解くことは難しいことがわかる。

ところが、この問題を作るのは容易である。別紙５のとおり、次の３ステップで問題を作ることができる。①交差点の親子を作る。②子同士をつなぐ。③親と子の区別をなくす（親を黒く塗りつぶす）。

このように、問題を作ることは容易であるが、問題を解くことは難しいという「一方向性」という性質について学生が理解したところで、次のように実際の公開鍵暗号方式で使われている一方向性関数について説明した。

⑹　一方向性関数

一方向性関数問題には、素因数分解問題と離散対数問題がある。

(i)　素因数分解問題

桁の大きな２つの素数を掛け合わせて積を求めることは容易であるが、２つの素数を掛け合わせた数（合成数）から元の２つの素数を求めることは困難である。このように合成数から元の２つの素数を求めることを「素因数分解問題」という。

たとえば、35を素因数分解すると、５×７とすぐにわかる。桁の小さな素数をすでに暗記しているため素因数分解が暗算でできるのである。ところが、１０００１の素因数分解はいくつになるかと聞かれてもすぐには答えられない。素因数分解で公式があてはまって解けるものはほんの一部で、公式があてはまらないものがほとんどだからである。これを解くには、１０００１の約数の候補である$\sqrt{10001}$以下の素数２，３，５，７，・・・の中から一つずつ約数の候補を探すのである。それらを試していくうちに１０００１＝73×137であることがわかる。このように２つの素数の合成数の桁数が増えると素因数分解はさらに困難になるのである。

この素因数分解の困難さを利用した暗号方式に「ＲＳＡ」がある。

(ii)　離散対数問題

次のような合同式において

$$a^{x} = y \pmod{p} \qquad \text{(2.2-1式)}$$

ｐ、ａとｘがわかっている場合にｙを求めることは容易であるが、ｐ、ａとｙがわかっていてもｙの対数ｘを求めることは困難である。これを離散対数問題という。この離散対数問題は、Diffie-Hellman鍵交換や公開鍵アルゴリズムのひとつであるElGamal方式で使われている。

２．２．１　ＲＳＡ

⑴　ＲＳＡとは

ＲＳＡは公開鍵暗号方式の一つである。ＲＳＡは平文を数値（文字コード）としてとらえ、それに数学的な処理をすることにより暗号化する暗号方式である。暗号化は次の式で表現することができる。

暗号文＝平文^{E} mod N

ここで、暗号文と平文は数値である。

ＲＳＡの暗号化は、「平文（数値）をE乗してmod Nをとる」ことである。「mod Nをとる」とは、「Nで割った余りを求めること」（モジュロ演算）である。（「mod Nをとる」ことを、「Nを法とする世界」ともいう）言い換えると平文（数値）をE回掛けて、その結果をNで割った余りを求めると暗号文が求まる。そして、EとNがわかれば誰でも暗号化を行うことができるので、EとNの組が公開鍵である。

ＲＳＡの復号は、暗号文（数値）を次の式で数学的に変換して平文を求める。

平文＝暗号文^{D}mod N

ここで、暗号文と平文は数値である。

ＲＳＡの復号は、「暗号文（数値）をD乗してmod Nをとる」ことである。言い換えると暗号文（数値）をD回掛けて、その結果をNで割った余りを求めると平文が求まる。ここでNは暗号化のとき使った数と同じである。DとNの組が秘密鍵になる。DとNを知っている人だけが、復号できる。

それならなぜEとNがわかっても、暗号文が解読できないのだろうか。

それは、Nは素数Ｐと素数Ｑの掛け合わせた数で、

Nの桁数が大きくなるとNからPとQを求めることが困難であること(素因数分解問題)、PとQが求まらないと秘密鍵Dを求めることができないからである。秘密鍵Dは次式で求めることができる。

D＝［m×{(P－1) と (Q－1) の最小公倍数}＋1］／E (mは任意の整数) (2.2-2式)

この式からわかるように、Eの値がわかっていても素数PとQがわからなければ最小公倍数を求めることができないので、Dを求めることができない。以上のＲＳＡの暗号の仕組みをもっと理解するために、P，Q，Eに具体的な数値を入れて考えてみよう。

たとえば、P＝3とQ=11を選び、「N＝33を法とする世界」を考える。この世界に存在する全ての数は、0から32までだけである。33で割って余りを出すからである。

この世界に存在する全ての数のべき乗を求めると、図7のようになる。

この図7を見ると、1から32までの数はべき乗するたびに予想のつかない数に変わっているが、11乗または21乗するとまた元の数に戻っている。

このように2つの素数（PとQ）をかけた数（N）を法とする世界では、全ての数が自分自身の数に戻るべき乗数が必ず存在する。(この例では11乗と21乗である。) そしてそれが何乗になるかは次の式で求められる。

m×{(P-1) と (Q-1) の最小公倍数}＋1 (2.2-3式)

mは任意の整数である。

たとえば、P＝3、Q=11の場合、P－1＝2、Q－1＝10の最小公倍数は10だから、m＝1とすると1×10＋1＝11、m＝2とすると、2×10＋1＝

この世界の数 \ べき乗	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13
14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14
15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32

図 7　33を法とする世界

21となり、11乗と21乗でどの数も元の自分自身の数に戻ることができる。

次に、たとえば公開鍵のＥを３と設定する。そして、相手に伝えたい平文の数値を９，15，21とする。これらの数値を３乗して、33を法とする世界の数を求めると、図７より３，９，21となることがわかる。この３，９，21が暗号文の数値である。

さらに、３，９，21を７乗すると図７より、元の数値９，15，21になることがわかる。これが暗号文を復号したことになる。すなわち、33を法とする世界では、平文を３乗して暗号文を求めて、その暗号文を７乗すると平文に戻ることになる。この復号するときのＤ＝７乗は素数ＰとＱから（2.2-4式）の通り求めることができる。しかし、Ｎを素因数分解できなければＰとＱを求めることができない。

秘密鍵Ｄを求める式を考える。Ａという数値を暗号化するときにＥ乗（公開鍵）し、復号するときＤ乗（秘密鍵）したとすると、元の数値Ａに戻らなくてはならないので、秘密鍵Ｄは次の式から求まる。

$$(A^E)^D = A^{[m\{(P-1)と(Q-1)の最小公倍数\}+1]}$$

$$ED = m\{(P-1)と(Q-1)の最小公倍数\}+1$$

$$D = m[\{(P-1)と(Q-1)の最小公倍数\}+1]／E \qquad (2.2\text{-}4式)$$

ここで、素数ＰとＱを与えられたときＮ＝Ｐ×Ｑを求めることは簡単であるが、Ｎ（Ｐ×Ｑ）の値を与えられたとき、Ｎの桁数が大きければ素数ＰとＱを求めることは困難である。また、平文の文字の数値を何乗かしてＮを法とする世界の数を求めること（暗号化）は容易であるが、ＰとＱの値がわからなければ、秘密鍵Ｄを求めることができず、あと何乗すれば元の平文の数値に戻すこと（復号）ができるかわからない。

このように法とする数Ｎと公開鍵Ｅを公開しても、ＰとＱを使って秘密鍵Ｄを求めた本人以外は秘密鍵を知ることはできない。この素因数分解の難しさが、公開鍵暗号方式の解読に対する安全性になっている。

⑵　学習の目標

- 公開鍵暗号方式の代表であるＲＳＡの仕組みを理解する。
- 表計算ソフトを使って「15を法とする世界」を計算する。

⑶　授業の実践

⑷　表計算ソフトを使って「15を法とする世界」の数を求める

素数ＰとＱに具体的に小さな値を入れ、Ｎを計算し、「Ｎを法とする世界」の表を作成する。ある数値を何乗かすると元の数と同じ数が現れることを確認する。そしてＰとＱの値から何乗すると元の数と同じ数が現れることを計算する。

学生は、Ｐ＝３、Ｑ＝５，Ｎ＝15として「15を法とする世界の数」を、表計算ソフトを使って求めてみる。ｍｏｄ関数を利用する。

すると結果は図８のとおりとなった。

ここで、図８を見ると、５乗と９乗のとき、元の数に戻っていることがわかる。何乗のときもとの数に戻るか計算をしてみよう。2.2-3式から、Ｐ－１＝２、Ｑ－１＝４なので、最小公倍数は４となる。したがって、ｍ×４＋１が元の数に戻る乗数である。（ｍは任意の整数）ｍ＝１ならば５であるし、ｍ＝２ならば９である。

⑸　公開鍵を３に設定し、秘密鍵を求める

さらに公開鍵をある数に設定して、秘密鍵を求める。たとえば、公開鍵Ｅ＝３とするとＤを求める式（2.2-2式）から、Ｄ＝（ｍ×４＋１）／３となり、ｍ＝２のとき秘密鍵Ｄは整数となり、Ｄ＝３と求ま

15 を法とする世界　P=3、Q=5

		べき乗									
平文の数値		1	2	3	4	5	6	7	8	9	10
	1	1	1	1	1	1	1	1	1	1	1
	2	2	4	8	1	2	4	8	1	2	4
	3	3	9	12	6	3	9	12	6	3	9
	4	4	1	4	1	4	1	4	1	4	1
	5	5	10	5	10	5	10	5	10	5	10
	6	6	6	6	6	6	6	6	6	6	6
	7	7	4	13	1	7	4	13	1	7	4
	8	8	4	2	1	8	4	2	1	8	4
	9	9	6	9	6	9	6	9	6	9	6
	10	10	10	10	10	10	10	10	10	10	10
	11	11	1	11	1	11	1	11	1	11	1
	12	12	9	3	6	12	9	3	6	12	9
	13	13	4	7	1	13	4	7	1	13	4
	14	14	1	14	1	14	1	14	1	14	1

図 8　15を法とする世界

る。つまり、今回の例では公開鍵をＥ＝3とすると、秘密鍵はＤ＝3となる。

(c)　平文を暗号化する

たとえば、2，7，13を平文の数値として、暗号文を求める。Ｅ＝3すなわち3乗してｍｏｄ15をとると、図8から暗号文は8，13，7となる。

(d)　暗号文を復号する

つぎに、この暗号文（8，13，7）を復号する。秘密鍵Ｄは上記(b)項の計算で、3と求まったから、8，13，7を3乗してｍｏｄ15をとると、図8から2、7、13となって、平文に復号できたことがわかる。

学生は以上のとおり、表計算ソフトを使って図8を作成し、平文の数値に対し公開鍵Ｅのべき乗を行い、ｍｏｄ15を取り、暗号文を求めた。さらに、秘密鍵Ｄを計算し、暗号文の数値を秘密鍵Ｄのべき乗を行い、ｍｏｄ15を取り、復号して平文を求めた。ここで、数値をべき乗してｍｏｄ15を取ることは容易であるが、Ｎを素因数分解して素数ＰとＱの値を求めなければ秘密鍵Ｄの値を知ることは困難である。Ｎ＝15の場合は、素数ＰとＱはＰ＝3、Ｑ＝5とわかるが、Ｎの桁数が大きくなると素数ＰとＱを知ることは難しい。これが素因数分解問題という一方向性関数を利用した暗号方式ＲＳＡである。

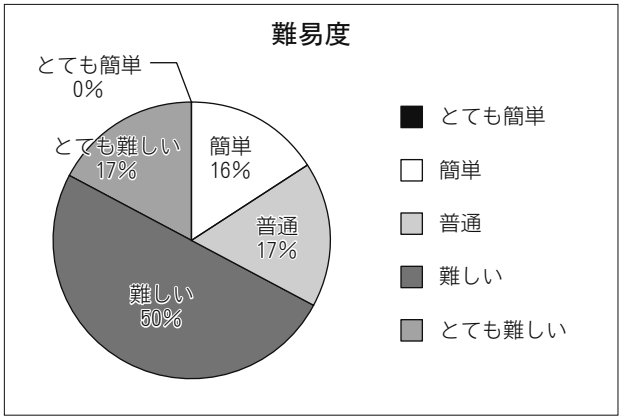
3．学習の実践評価

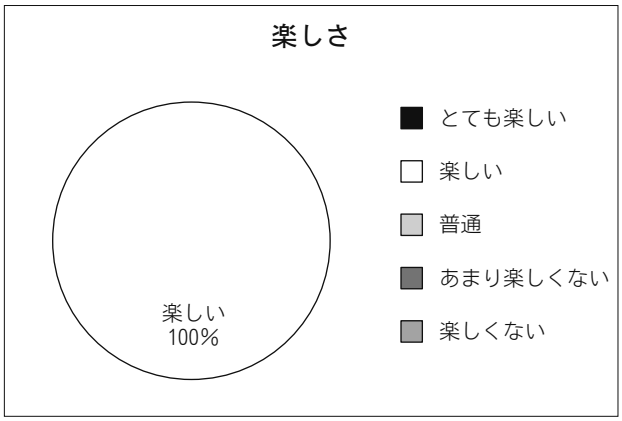
今回の「暗号」学習プログラムを長野女子短期大学の学生と実践してみた。

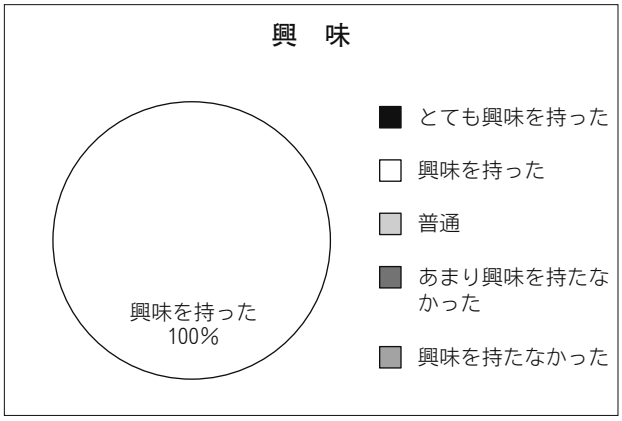
2．2．1(3)の授業は時間の都合上実施ができなかったが、他の項目は実施できた。講義内容の難易度、楽しさ、興味の度合いについて学生が4段階評価を行った。また、感想は自由記述とした。

3．1　結果

授業の最後に実践結果の評価をするために、アンケートを実施した。授業の難易度、楽しさ、興味の度合いについて図に示す。







難易度については、16%の人が「簡単」、17%の人が「普通」50%の人が「難しい」、17%の人が「とても難しい」であった。楽しさについては、100%の人が「楽しい」を選び、興味については100%の人が「興味を持った」を選んだ。「暗号」というテーマは、難しい数学的な要素を含むので、67%の人が難しいと感じながらも、今回の学習プログラムで学生は、楽しく、興味を持って学習ができた。

4　おわりに

ネットワークの進展に伴い、秘密にしておきたい情報をネットワーク経由でやり取りすることが多くなった。これからの私たちには、情報を秘匿し、相手を認証する技術、すなわち「暗号」についての知識が必要である。しかし、暗号技術を学習するには数学的要素が必要であり、学生の学習意欲を維持しながら暗号原理を学習していくことが難しかった。そこで今回の学習プログラムを提案した。アンプラグドを取り入れたり、シーザー暗号方式で暗号化や復号をしたり、表計算ソフトで「Nを法とする世界」をのぞいてみたりして、暗号の基本原理を学習した。学習した学生の約7割が「難しい」と感じたが、全員が「楽しい」、「興味を持った」と回答しているので、所期の目的は達成できたと考える。

暗号技術を理解するにあたり、2つの文献を参考にしてきた。[iv][v] 暗号技術は奥が深い、今回は情報の暗号化と復号について学習プログラムを作成したが、「認証」については触れていない。今後の課題と考えている。

参考文献

（ｉ）Tim Bell, lan H. Witten, Mike Fellows: Computer Science Unplugged.
＜http://csunplugged.com/＞
（ii）兼宗進監訳、『コンピュータを使わない情報教育　アンプラグド・コンピュータ・サイエンス』
イーテキスト研究所
（iii）間辺広樹、兼宗進、並木美太郎、
アンプラグドを活用した公開鍵暗号学習プログラムの情報科教育への適用、
情報教育シンポジウムSSS2010
（iv）『暗号技術入門　秘密の国のアリス』
結城　浩　著　ソフトバンククリエイティブ
（ｖ）『暗号理論　図解雑学』
伊藤　正史　著　ナツメ社

付録１

暗号学習プログラム　別紙１

氏名＿＿＿＿＿＿＿＿＿＿＿＿

１．シーザー暗号

（１）暗号化

次の文字をアルファベット順に１文字後ろにずらして、暗号化しなさい。

①ＴＯＫＹＯ　＿＿＿＿＿＿＿＿＿＿＿＿

②ＮＡＧＯＹＡ　＿＿＿＿＿＿＿＿＿＿＿＿

（２）復号

次の文字をアルファベット順に１文字前にずらして、復号しなさい。

①ＯＢＨＢＯＰＫＰＴＩＪ　＿＿＿＿＿＿＿＿＿＿＿＿

②ＴＰＤＤＦＳ　＿＿＿＿＿＿＿＿＿＿＿＿

（３）自分で言葉（平文／ローマ字）を決めて、それをシーザー暗号化しなさい。そして、自分で決めた暗号文を次のページに書き、隣の人にその暗号文を渡して復号してもらいなさい。ずらす文字数は３文字とする。

平文（ローマ字）	暗号文

（４）隣の人からもらった暗号文を復号しなさい。

暗号文	平文（ローマ字）

---------- 切り取り線 ----------

次の暗号文は、私がシーザー暗号で作ったものです。これらの暗号文を復号してください。ただし、暗号化の鍵は３文字後ろにずらしたことです。

暗号

付録２

暗号学習プログラム　別紙２

氏名＿＿＿＿＿＿＿＿＿＿＿＿

１．換字式暗号

平文と暗号文の各文字を１対１で異なる文字に対応させるものを「単一換字暗号」という。たとえば、英語のアルファベット 26 文字を図１の変換規則のように変換すると、

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓
Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

図 9　換字式暗号変換規則

平文　HELLO

↓

暗号文　ITSSG

（１）次の文字を上記の変換規則に従って、換字式で暗号化しなさい。

平文	暗号文
NAGANOEKIDEMATE	
ZENKOJIGOKAITYOU	

（２）上記図１の変換規則に従って、換字式暗号化された暗号文を復号しなさい。

暗号文	平文
ZGANG	
IGAAQORG	

付録３

暗号学習プログラム　別紙３

排他的論理和（ＸＯＲ）

１．学習の目的

- ある特定の並びを持った０と１のビット列（ビット列Ａのパターン）が、かぎＢのパターンとのＸＯＲ演算処理により、０と１の並びがランダムな状態（暗号文）になることを理解する。(図１参照)

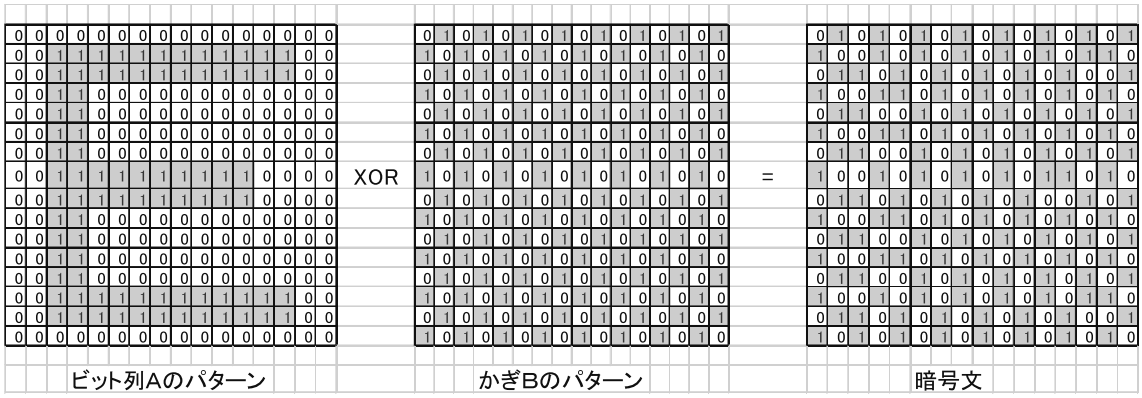


図 10　ＸＯＲ演算による暗号化

- その０と１の並びがランダムな状態であったもの（暗号文）が、かぎＢのパターンとのＸＯＲ演算により元の０と１のビット列（ビット列Ａのパターン）に戻ることを理解する。(図２参照)

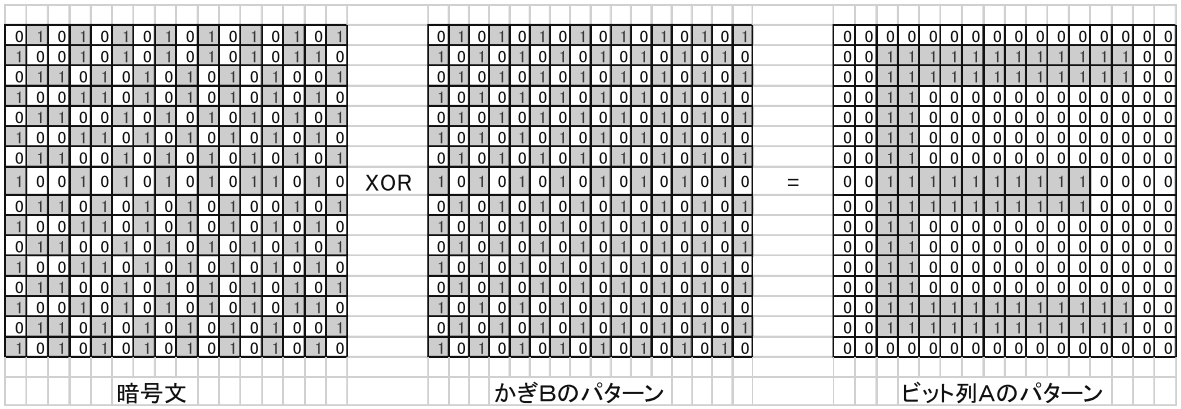


図 11　ＸＯＲ演算による復号

２．表計算ソフト（Ｅｘｃｅｌ）によるＸＯＲ演算の実行

Ｅｘｃｅｌを起動し、次の操作を実行する。

２．１　ＸＯＲ演算による暗号化

（１）列幅をそろえる

①開いたブックのＳｈｅｅｔ１において、全セル選択ボタンをクリックする。

②Ａ列とＢ列の境界をドラッグして、１８ピクセルの幅に設定する。

③Ｑ列，ＡＨ列、ＡＹ列を選択し直して、７２ピクセルの幅に設定する。

（２）ビット列Ａのパターンの作成

①Ａ１：Ｐ１６のセルを選択して、実線（細線）で格子を描く。

②図１のビット列Ａのパターンのようにに Ａ１：Ｐ１６のセルに０と１を入力する。

③Ａ１：Ｐ１６のセルを選択して、「ホーム」、「スタイル」グループの「条件付き書式」をクリックする。

④「セルの強調表示ルール」を選択し、「指定の値に等しい」をクリックする。

⑤「次の値に等しいセルを書式設定」のボックスに１を入力する。

⑥書式に「濃い赤の文字、明るい背景」を選択する。ＯＫをクリックする。

（３）かぎＢのパターンの作成

①Ｒ１：ＡＧ１６のセルを選択して、実線（細線）で格子を描く。

②図１のかぎＢのパターンのようにＲ１：ＡＧ１６のセルに０と１を入力する。

③Ｒ１：ＡＧ１６のセルを選択して、「ホーム」、「スタイル」グループの「条件付き書式」をクリックする。

④「セルの強調表示ルール」を選択し、「指定の値に等しい」をクリックする。

⑤「次の値に等しいセルを書式設定」のボックスに１を入力する。

⑥書式に「濃い赤の文字、明るい背景」を選択する。ＯＫをクリックする。

（４）ＸＯＲ演算の実施（暗号文の作成）

①ＡＩ１：ＡＸ１６のセルを選択して、実線（細線）で格子を描く。

②ＡＩ１のセルに、次のＩＦ文を使ってＸＯＲ演算を実施する。

=IF(AND(A1=1,R1=1),0,IF(AND(A1=1,R1=0),1,IF(AND(A1=0,R1=1),1,0)))

③ＡＩ１のセルに入力された関数をＡＩ１：ＡＸ１６のセルに、オートフィルでコピーしてはりつける。

④ＡＩ１：ＡＸ１６のセルを選択して、「ホーム」、「スタイル」グループの「条件付き書式」をクリックする。

⑤「セルの強調表示ルール」を選択し、「指定の値に等しい」をクリックする。

⑥「次の値に等しいセルを書式設定」のボックスに１を入力する。

⑦書式に「濃い赤の文字、明るい背景」を選択する。ＯＫをクリックする。

以上の操作をすると、ビット列Ａのパターンでは１の並びでＥの型ができているが、かぎＢのパターンとの排他的論理和をとると、暗号文のパターンのように０と１の並びがランダムな状態になっている。

２．２　ＸＯＲ演算による復号

（１）列幅の設定

①開いたブックのＳｈｅｅｔ２において、全セル選択ボタンをクリックする。

②Ａ列とＢ列の境界をドラッグして、１８ピクセルの幅に設定する。

③Ｑ列，ＡＨ列、ＡＹ列を選択し直して、７２ピクセルの幅に設定する。

（２）暗号文パターンのコピー＆貼り付け

①Ｓｈｅｅｔ１のＡＩ１：ＡＸ１６のセルを選択して、コピーする。

②Ｓｈｅｅｔ２のＡ１セルを選択する。

③「ホーム」タブ「クリップボード」グループから、貼り付けのオプションの「テキストのみ保持」をクリックする。

（３）かぎＢのパターンのコピー

①Ｓｈｅｅｔ１のＲ１：ＡＧ１６のセルを選択して、コピーする。

②Ｓｈｅｅｔ２のＲ１セルを選択する。

③「ホーム」タブ「クリップボード」グループから、「貼り付け」をクリックする。

（４）ＸＯＲ演算の実施（平文への復号）

①Ｓｈｅｅｔ２のＡＩ１：ＡＸ１６のセルを選択して、実線（細線）で格子を描く。

②ＡＩ１のセルに、次のＩＦ文を使ってＸＯＲ演算を実施する。

=IF(AND(A1=1,R1=1),0,IF(AND(A1=1,R1=0),1,IF(AND(A1=0,R1=1),1,0)))

③ＡＩ１のセルに入力された関数をＡＩ１：ＡＸ１６のセルに、オートフィルでコピーしてはりつける。

④ＡＩ１：ＡＸ１６のセルを選択して、「ホーム」、「スタイル」グループの「条件付き書式」をクリックする。

⑤「セルの強調表示ルール」を選択し、「指定の値に等しい」をクリックする。

⑥「次の値に等しいセルを書式設定」のボックスに１を入力する。

⑦書式に「濃い赤の文字、明るい背景」を選択する。ＯＫをクリックする。

以上の操作をすると、暗号文のパターンのように０と１の並びがランダムな状態になっているものが、かぎＢのパターンとの排他的論理和をとると、ビット列Ａのパターンに戻り、１の並びでＥの型ができている。

３．まとめ

（１）学習の目的のとおり、ＸＯＲ演算によって暗号化と復号ができることを確認する。

（２）どのようにかぎＢのパターンを作るかによって強い暗号ができることを理解する。かぎＢのパターンをどのように作るかのことを「暗号アルゴリズム」という。すなわち、暗号アルゴリズム次第で解読が難しい暗号となるのである。

付録４

暗号学習プログラム　別紙４

アイスクリームワゴン問題

次の図１は黒丸が交差点を、線が道を表している。黒丸のどこかにアイスクリームワゴン車を１台止めたい。お客様は止めた黒丸の一つ隣りからはアイスクリームワゴン車までアイスクリームを買いに来られるものとする。２つとなりは遠いので、一つ隣りまでとする。どの黒丸にアイスクリームワゴン車を止めると、一番少ない台数ですべての交差点からお客様はアイスクリームを買いに来ることができるか？

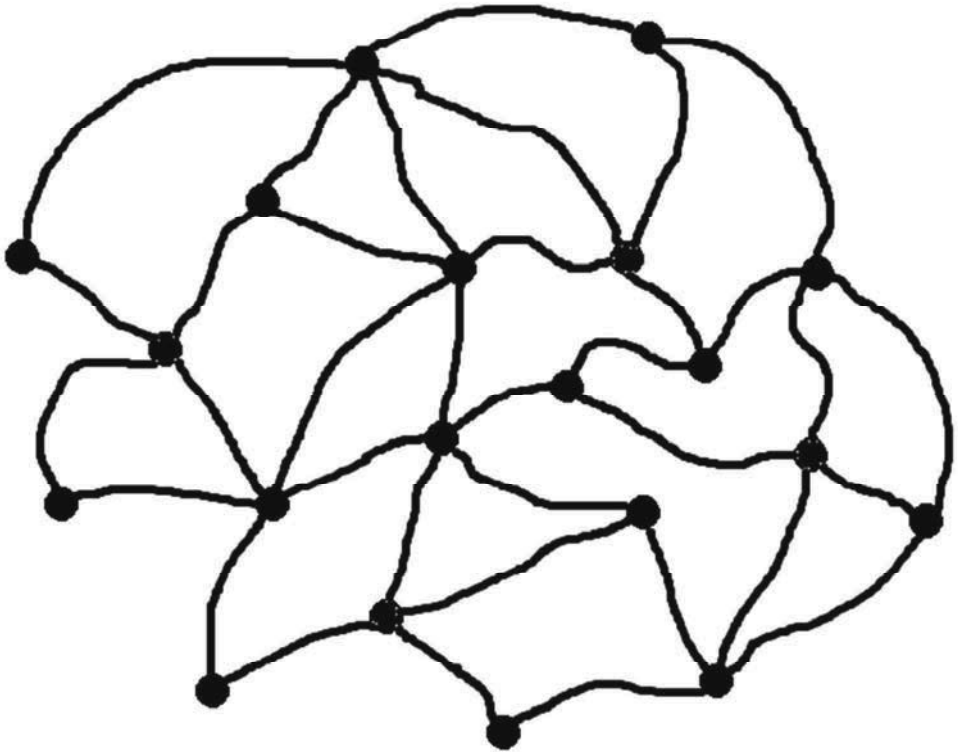


図 12　アイスクリームワゴン問題

付録５

暗号学習プログラム　別紙５

アイスクリームワゴン問題の作り方

１．交差点の親子を作る（図 1）

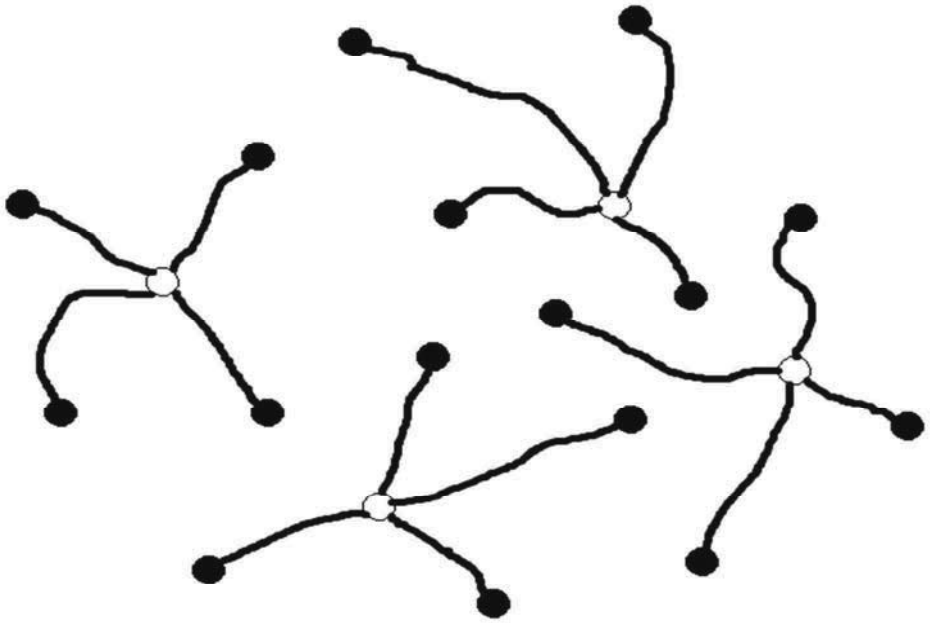


図１　交差点の親子を作る

２．子同士をつなぐ（図 2）

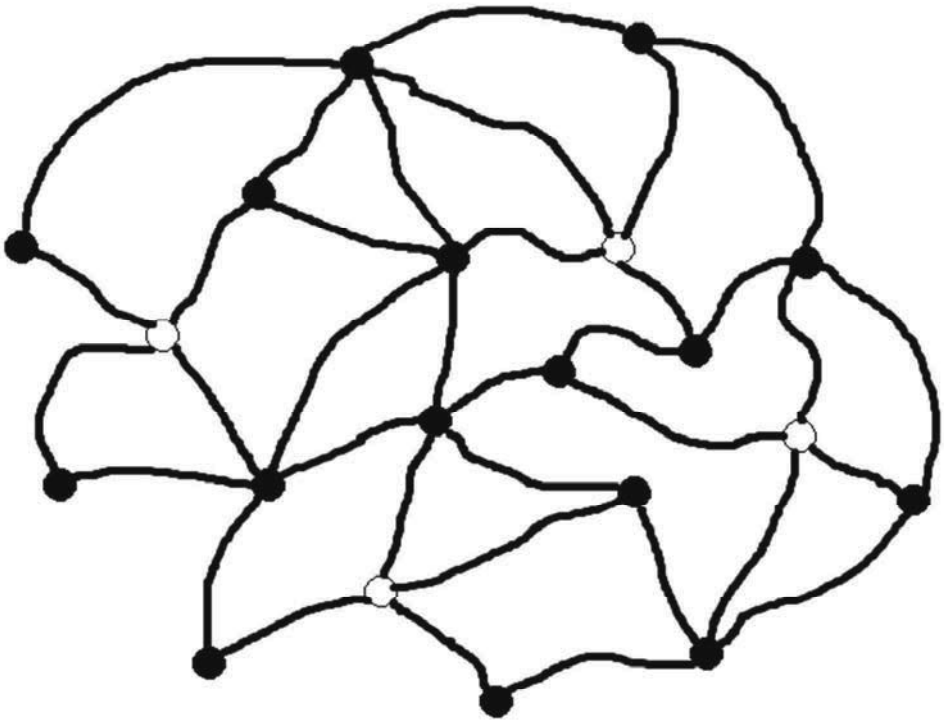


図２　子同士をつなぐ

４．親と子の区別をなくす（図 3）

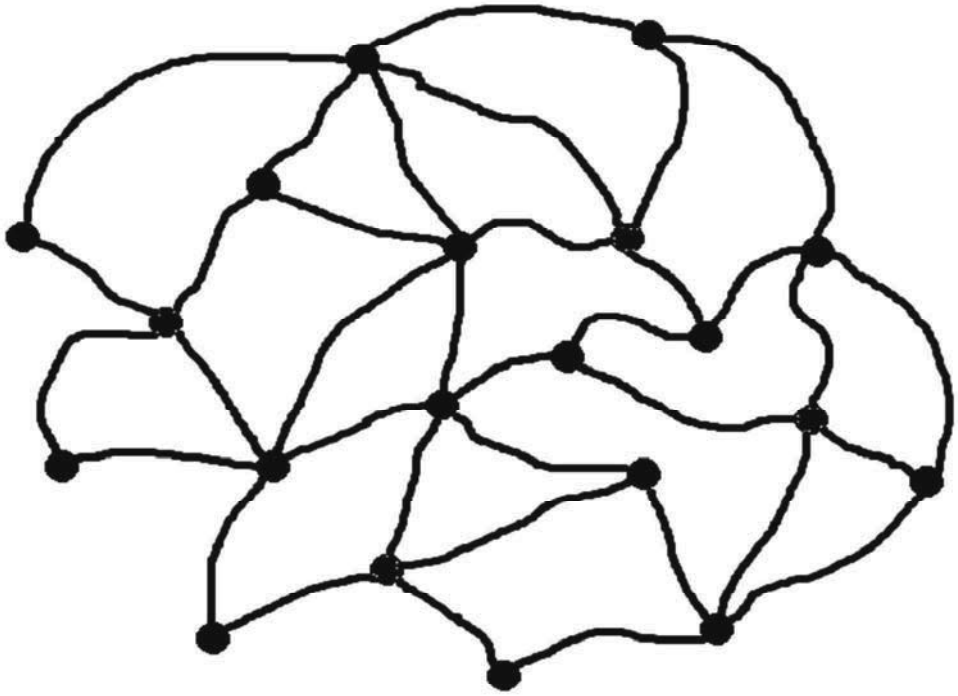


図 3　親と子の区別をなくす

５．まとめ

アイスクリームワゴン問題を作ることは簡単だが、解くことは難しい。このような性質を「一方向性」と呼ぶ。一方の向きに計算ができて答えを出すことができても、反対の向きに計算するのが極めて困難な性質のことであり、そのような働きを持つ関数を「一方向性関数」という。公開鍵暗号方式は、この「一方向性」という性質を利用して、一つの鍵を公開しても暗号を解読できないような仕組みを作っている。一方向性関数には、素因数分解問題がある。

たとえば、素因数分解は、桁数の少ない小さな数の時は比較的容易に素因数分解することができるが、桁数の大きな数になると素因数分解することが難しくなる。この性質を利用して、公開鍵暗号方式（RSA）では鍵を公開しても２つの素数のがわからなければ、解読できないようにしている。

今、３５を素因数分解すると、５×７とすぐにわかる。桁の小さな素数をすでに暗記しているため素因数分解が暗算でできるのである。ところが、１００００１の素因数分解はいくつになるかと聞かれてもすぐには答えられない。素因数分解で公式があてはまって解けるものはほんの一部で、公式があてはまらないものがほとんどだからである。これを解くには、１００００１の約数の候補である$\sqrt{100001}$以下の素数２，３，５，７，･･･の中から一つずつ約数の候補を探すのである。それらを試していくうちに１００００１＝７３×１３７であることがわかる。このように桁数が増えると素因数分解はさらに困難になるのである。

付録６

暗号学習プログラム　別紙６

公開鍵暗号方式の仕組み

１．公開鍵暗号方式の仕組み

公開鍵暗号方式の一つであるＲＳＡは、平文を数値（文字コード）としてとらえ、それに数学的な処理をすることにより暗号化する。その数学的な処理（暗号化）とは次の式で表現することができる。

暗号文＝平文^{E} mod N　　(1-1 式)

ここで、暗号文と平文は数値である。

この暗号化は、「平文(数値)をＥ乗して mod N をとる」ことである。「mod N をとる」とは、「N で割った余りを求めること」（モジュロ演算）である。「mod N をとる」ことを、「Ｎを法とする世界」ともいう。言い換えると平文(数値)をＥ回掛けて、その結果をＮで割った余りを求めると暗号文が求まる。

また、暗号文の復号も次式のとおり数学的な処理が行われる。

平文＝暗号文^{D}mod N　　(1-2 式)

２．Ｎを法とする世界

それでは「Ｎを法とする世界」を求め、公開鍵暗号方式の仕組みを見てみよう。

表計算ソフト(Ｅｘｃｅｌ)を使って「Ｎを法とする世界」を求める

ここで、Ｎは素数Ｐと素数Ｑをかけた数である。わかりやすくするためＰとＱは小さい値を考え、「Ｎを法とする世界」の基本原理を考える。たとえば、Ｐ＝３，Ｑ＝５とすると、Ｎ＝Ｐ×Ｑ＝１５となる。そこで、１５を法とする世界を求めてみる。平文は１から１４までとし、その平文を１乗から１０乗までべき乗計算してｍｏｄ１５をとった表を作成する。

（１）Ｅｘｃｅｌを起動し、次の操作をする。

(i) 列幅の設定

①Ａ列からＬ列まで選択し、列幅を４０ピクセルに設定する。

(ii) １５を法とする世界

①図１の表を作成する。Ｂ４：Ｂ１７は平文の数値で、Ｃ３：Ｌ３はべき乗数である。

②Ｃ４：Ｌ１７に暗号文(数値)を求める。（図２参照）数式はつぎのとおり。

暗号文＝平文^{E} mod N　　(2-1 式)

ここで、平文はＢ４：Ｂ１７の数値であり、ＥはＣ３：Ｌ３の数値である。ｍｏｄＮはＭＯＤ関数を使って求めなさい。ＭＯＤ関数の書式はつぎのとおり。

=ＭＯＤ（数値，剰余）　　(2-2 式)

	A	B	C	D	E	F	G	H	I	J	K	L
1	15を法とする世界　P=3、Q=5											
2			べき乗									
3			1	2	3	4	5	6	7	8	9	10
4		1										
5		2										
6		3										
7		4										
8	平	5										
9	文	6										
10	の	7										
11	数	8										
12	値	9										
13		10										
14		11										
15		12										
16		13										
17		14										
18												

図 1　１５を法とする世界

	A	B	C	D	E	F	G	H	I	J	K	L
1	15を法とする世界　P=3、Q=5											
2			べき乗									
3			1	2	3	4	5	6	7	8	9	10
4		1	1	1	1	1	1	1	1	1	1	1
5		2	2	4	8	1	2	4	8	1	2	4
6		3	3	9	12	6	3	9	12	6	3	9
7		4	4	1	4	1	4	1	4	1	4	1
8	平	5	5	10	5	10	5	10	5	10	5	10
9	文	6	6	6	6	6	6	6	6	6	6	6
10	の	7	7	4	13	1	7	4	13	1	7	4
11	数	8	8	4	2	1	8	4	2	1	8	4
12	値	9	9	6	9	6	9	6	9	6	9	6
13		10	10	10	10	10	10	10	10	10	10	10
14		11	11	1	11	1	11	1	11	1	11	1
15		12	12	9	3	6	12	9	3	6	12	9
16		13	13	4	7	1	13	4	7	1	13	4
17		14	14	1	14	1	14	1	14	1	14	1
18												

図 2　１５を法とする世界完成

（2）１５を法とする世界の考察

図２からわかることは次の通り。

①１乗、５乗、９乗は元の数値(平文の数値)に戻っている。

②それ以外のべき乗数では、平文の数値からは予想のつかない数値になっている

このように２つの素数（ＰとＱ）をかけた数（Ｎ）を法とする世界では、全ての数が自分自身の数に戻るべき乗数が必ず存在する。（この例では１乗、５乗と９乗である。）そしてそれが何乗になるかは次

の式で求められる。

$m \times \{(P-1)と(Q-1)の最小公倍数\} + 1$　　(2-3 式)

mは任意の整数である。

ここで、Ｐ－１＝２、Ｑ－１＝４なので、最小公倍数は４となる。m=０，１，２のとき、(2-3 式）は１乗、５乗、９乗となる。

（３）公開鍵暗号方式の仕組み

（ａ）平文の暗号化

2-1 式において、平文を２、８、１３とし、公開鍵Ｅ＝３とする。すると、図 2 より、暗号文の数値は、８，２，７となる。暗号文の復号は、暗号文(数値)を次の式で数学的に変換して平文を求める。

平文＝暗号文^{D}mod N　　(2-4 式)

ここで、暗号文と平文は数値である。また、2-1 式と 2-4 式は同じ演算処理である。

したがって、秘密鍵Ｄがわかれば図２を使って平文を求めることができる。

（ｂ）秘密鍵Ｄと暗号文の復号

Ｄは次のように求めることができる。

Ａという数値を暗号化するときにＥ乗(公開鍵)し、復号するときさらにＤ乗(秘密鍵)したとすると、元の数値Ａに戻らなくてはならないので、秘密鍵Ｄは次の式から求まる。

$$(A^{E})^{D} = A^{[m\{(P-1)と(Q-1)の最小公倍数\}+1]}$$

$$ED = m\{(P-1)と(Q-1)の最小公倍数\}+1$$

$$D = m[\{(P-1)と(Q-1)の最小公倍数\}+1] / E \qquad (2-5 式)$$

公開鍵はＥ＝３、Ｐ－１＝２、Ｑ－１＝４なので、最小公倍数は４となるから、Ｄ＝（ｍ×４＋１）／３となり、ｍ＝２のとき秘密鍵Ｄは整数となり、Ｄ＝３と求まる。つまり、今回の例では公開鍵をＥ＝３とすると、秘密鍵はＤ＝３と計算で求めることができる。

暗号文８，２，７を秘密鍵Ｄ＝３で復号してみよう。

図２から、８，２，７を３乗してｍｏｄ１５をとると、２，８，１３になる。元の平文に戻った。

（ｃ）暗号の安全性

素数ＰとＱを与えられたときＮ＝Ｐ×Ｑを求めることは簡単であるが、Ｎ（Ｐ×Ｑ）の値を与えられたとき、Ｎの桁数が大きければ素数ＰとＱを求めることは困難である。また、平文の文字の数値を何乗かしてＮを法とする世界の数を求めること（暗号化）は容易であるが、Ｅの値がわかっていてもＰとＱの値がわからなければ、秘密鍵Ｄを求めることができず、あと何乗すれば元の平文の数値に戻すこと（復号）ができるかわからない。

このように法とする数Ｎと公開鍵Ｅを公開しても、ＰとＱを使って秘密鍵Ｄを求めた本人以外は秘密鍵を知ることはできない。この素因数分解の難しさが、公開鍵暗号方式の解読に対する安全性になっている。