高校生のための現代数学講座　　東京大学
「素数と暗号」　　玉原国際セミナーハウス
講義 (1) 寺杣　友秀　　2017 年 7 月 22 日

「因数分解と暗号」

1　共通鍵暗号

1.1　シーザー暗号

昔から秘密の情報をやり取りするのに暗号が使われてきた。ＡからＺまでの文字をアルファベットの並びに関してある一定の数だけずらす（例えば 3 文字ずらすなど）ことにより、伝えたい文章をそのままでは意味が分からない文章に変換する。伝えたい文章は「平文」と呼ばれ、変換された文章を「暗号文」と呼ばれる。「平文」から「暗号文」に変換することを「暗号化」という

例えば「3 文字あとの文字に変換する」という規則を使えば「TAMBARA」は「WDPEDUD」と変換される。受け取った文をもとの文章に戻すには「3 文字前の文字に変換」すればよい。このように「暗号文」から「平文」に変換することを「復号」という。

この暗号方式は古代シーザーによって用いられたもので「シーザー暗号」と呼ばれる。シーザー暗号において、「3 文字」という情報は暗号化及び復号するときに必要な情報で、これを暗号化、復号の「鍵」とよばれている。シーザー暗号では暗号化に必要な鍵と復号に必要な鍵が共通なので共通鍵暗号と呼ばれる。

これを少し一般化して一つの文字をほかの文字で置き換える暗号は単一換次式暗号と呼ばれる。英文などでは現れる文字の頻度を分析 (e が一番多くそのあと a,t,i,o と続く) することにより鍵を推測されてしまうことがあり、現在では安全ではないとされている

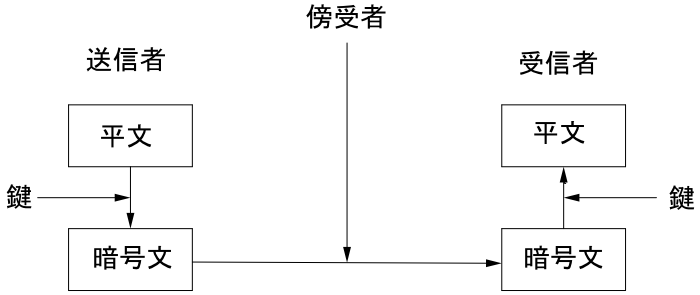
1.2　共通鍵暗号

単一換字式暗号の弱点を補うために考案されたものがいくつかの情報をブロックとして暗号化する方式でアメリカが国家を上げて設計に関与した「DES」などがそれである。ある一定のが長さをブロック化してそれを「鍵」と複雑なアルゴリズムにより暗号化する。復号に際して用いられる「鍵」は暗号化する時に用いられる「鍵」と同じものである。このような暗号は共通鍵暗号と呼ばれる。破ることが困難であ

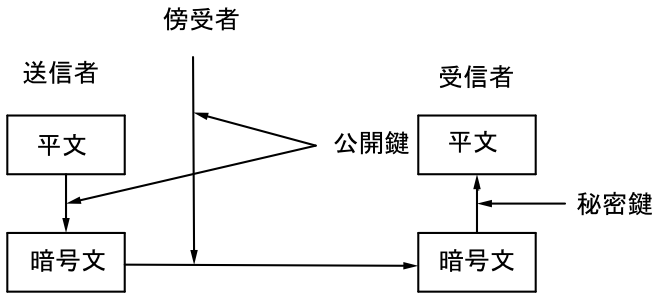
るものが、次々に発表されているが、暗号に用いられる鍵をどう通信したい相手と共有するかが一番の問題である。これは「鍵配送問題」と呼ばれる。ドイツの「エニグマ」は平文を自動暗号化、復号する機械で毎日鍵を取り換えることにより解読が難しいとされていたが、人口知能の父と称されるアラン・チューリングが計算機を用いて解読したとされている。計算機の初期段階から暗号と計算機とは切っても切れない関係にある。

1.3 共通鍵暗号と公開鍵暗号

ディフィーとヘルマンにより共通鍵暗号の考え方を超える、公開鍵暗号の考え方が提唱された。共通鍵暗号の暗号化、復号の手順は図式的にいうと下のようなものであった。



共通鍵暗号において、暗号化するのに必要な情報である「鍵」と復号するのに必要な情報である「鍵」は共通で送信側と受信側はこの情報を共有する必要がある。これに対して公開鍵暗号の基本的な考え方は暗号化に必要である「鍵」と復号に必要な「鍵」は別のものを用いることである。復号に必要な鍵は受信者だけが知っている情報でこれを「秘密鍵」という。これに対して暗号化するための「鍵」は公開してもよく、これを「公開鍵」という。これは図式的にいうと次のようになる。



公開鍵と秘密鍵はペアになるように受信者があるアルゴリズムにしたがって作成する。公開鍵を用いて平文を暗号化は容易にできるが、暗号化されたものを公開鍵

の情報のみで復号するのは困難であるが、秘密鍵があれば容易に復号できるような仕組みを作っておくのである。ポイントは受信者が公開鍵、秘密鍵の二つをつくることと、公開鍵は傍受者も含めだれでも参照できるようにするところである。

2 RSA暗号と因数分解

2.1 RSA暗号

上のような条件を満たす暗号の体系を実現するようなアルゴリズムがRivest-Shamir-Adelmanによって考案された。これは3人の頭文字をとってRSA暗号と呼ばれる。

平文を暗号文へと暗号化し、その暗号文をまた平文に戻すための数学的基礎付けは先週証明したフェルマーの定理である。まずはフェルマーの定理をどのように暗号化、復号に用いるかを説明しよう。

$$S = \{pq\text{以下の自然数で}pq\text{と互いに素}\}$$

なる集合を考えると、$x \in S$ に対して

$$x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

となるというのがフェルマーの定理である。そこで $m(p-1)(q-1)+1 = k$ とおくと、

$$x^k = x^{m(p-1)(q-1)+1} = (x^{(p-1)(q-1)})^m \cdot x \equiv x \pmod{pq}$$

となることがわかる。いま $ed = k$ となる自然数 d, e があれば、

$$(x^e)^d = x^{ed} = x^k = x$$

となる性質が暗号化、復号に利用できる。

以上のことを踏まえて、実際にどのように暗号に応用するかを見てみよう。まず受信者が二つの素数 p, q を選び、その積 $n = pq$ を計算する。さらに

$$m(p-1)(q-1) + 1 = ed$$

となる整数 d, e を見つける。そのためには

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

を満たす d, e を求めればよいことになる。そして公開鍵として (n, e) を公開し、(n, d) を秘密鍵として誰にも見られないようにする。送信者が伝えたい平文を x とする。このとき公開鍵 e と n を用いて $x^e \pmod{n}$ を暗号文とする。この暗号文を受信した受信者は秘密鍵である (n, d) を用いて暗号文 x^e を $\pmod{n}$ 計算で d 乗する。こうすると

$$(x^e)^d \equiv x^{ed} \equiv x^k \equiv x \pmod{n}$$

となり平文 x を回復できるのである。

2.2 例

$p = 3, q = 7$ として、RSA 暗号を考えてみよう。このとき $n = 21$ となる。さらに $(p-1)(q-1) = 12$ なので 12 と互いに素である数 e を選ぶ。例えば $e = 5$ としてみよう。このとき d は

$$5 \cdot d \equiv 1 \pmod{12}$$

となるように選べばよいが、これは $d = 5$ となるように選べば十分である。従って $e = 5, d = 5$ ととれば、

$$de = 25 = 1 + 24 = 1 + 2(p-1)(q-1)$$

となり公開鍵が $(n, e) = (21, 5)$ で秘密鍵が $(n, d) = (21, 5)$ となる。（このような小さい素数で考えると簡単に因数分解がされてしまうので、暗号を定めるのには不適切である。）さて平文 $x = 4$ を暗号化しよう。

$$x^e = x^5 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \equiv 16 \cdot 4 \cdot 4 \cdot 4 \equiv 1 \cdot 4 \cdot 4 \equiv 4 \cdot 4 \equiv 16 \pmod{21}$$

暗号化された暗号文は 16 となる。そこで 16 を $16^d = 16^5 \bmod 21$ を計算することにより復号できているかどうか確かめてみよう。

$$16^5 \equiv 16 \cdot 16 \cdot 16 \cdot 16 \cdot 16 \equiv 4 \cdot 16 \cdot 16 \cdot 16 \equiv 1 \cdot 16 \cdot 16 \equiv 16 \cdot 16 \equiv 4 \pmod{21}$$

となり $x = 4$ が回復された。

2.3 実用性と安全性

RSA 暗号が実用的であり、暗号として安全であることを考察してみたい。まず、公開鍵、秘密鍵をつくるときに必要な材料が容易に得られることをみてみよう。まず p, q を簡単に選べることを見るには素数は「たくさん」あることが必要であるが、それは素数定理により保証されている。そして大きな数 p, q が素数であるかどうかの判定法には「フェルマーふるい」とい効果的方法がある。さらに

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

を満たす d, e を作るにはユークリッドの互除法により容易に作ることができる。

最後に暗号として安全であることの保障であるが、(n, e) から (n, d) を求めるためには現在 n を因数分解する方法以外には知られていない。すなわち二つの素数の積であることがわかっている自然数 n を効率的に因数分解することができるか？という問題に RSA 暗号の安全性は帰着される。現在このような因数分解の効果的なアルゴリズムは知られておらず、RSA 暗号は安全な暗号であるとされている。