

第11章 暗号システム

11.1 暗号

本章では、整数論が暗号理論にどのように応用されるか、その概略を解説する。

暗号あるいは暗号化とは、第三者に通信内容を知られないように行う特殊な通信方法のうち、通信文を見ても特別な知識なしでは読めないように変換する表記法のことである。暗号化される前の文を平文、暗号化によって第三者に通信内容が知られないようにした文を暗号文という。平文は暗号化によって暗号文に変換されるが、逆に暗号文をから平文を復活させることを復号化という。暗号化、復号化のための手順あるいはそのパラメータを鍵という。暗号化は復号化と対をなしており、暗号化のための手順の逆を行うことで復号化がなされる（以上、ほぼ Wikipedia からの引用）。

さて、整数論の応用という観点から、平文や暗号文は、日本語や英語など普通の言語で書かれた文ではなく、自然数によって表されるものとする。また、もともとコンピュータ内部では、文字でも何でもすべてが数として表現されていると考えてよいので、平文や暗号文、パラメータとしての鍵も自然数として表され、それらに対して整数論的な操作をほどこすことで暗号システムが構築される。

暗号化の鍵と復号化の鍵が同一である（あるいは片方からもう一方が容易に得られる）暗号を共通鍵暗号という。古典的な暗号はすべて共通鍵暗号であり、あとで紹介する公開鍵暗号が現れる以前は「暗号 = 共通鍵暗号」であった。

11.2 Diffie-Hellman 鍵共有

一般に共通鍵暗号は、公開鍵暗号に比べ単純な組み立てになっており、暗号化・復号化も速やかに実行でき大量データの処理が可能である。しかし、通信をしたい両者があらかじめ鍵を共有する必要がある、そこで安全性が損なわれる可能性がある。つまり、普通に考えれば、一方が作成した鍵をもう一方に伝えなくてはならず、その際、鍵を盗聴されるおそれがある。このような危険を回避するひとつの方法として、1976年、W. Diffie と M. E. Hellman は、鍵自体を伝えることなしに両者が同一の鍵を共有する手法を提唱した。これを Diffie-Hellman 鍵共有という。

一般に、大きな数 b, m を固定し、 a, x が関係式 $a \equiv b^x \pmod{m}$ をみたすとする。このとき、 x から a は簡単に計算できるが、 a から x を求めることは一般には困難である。こ

の困難な問題を離散対数問題とよぶ。実数における対数の類似を既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^\times$ で考えたものである。Diffie-Hellman 鍵共有の安全性は離散対数問題に依拠しており、実際の手順は以下のように説明される。

- (1) 太郎と花子が鍵として「大きな数」を共有したいとする。
- (2) 太郎と花子は、大きな素数 p と、法 p に関する位数が小さくない自然数 $g < p$ を用意して共有する（可能ならば、 g を法 p に関する原始根とする）。 p, g は第三者に知られてもかまわない。

- (3) 太郎は $p-1$ と互いに素な大きな数 $x < p$ を任意にとり、

$$i \equiv g^x \pmod{p}, \quad 0 < i < p$$

によって定まる i を花子に伝える。太郎は x を秘密にする。

- (4) 花子は $p-1$ と互いに素な大きな数 $y < p$ を任意にとり、

$$j \equiv g^y \pmod{p}, \quad 0 < j < p$$

によって定まる j を太郎に伝える。花子は y を秘密にする。

- (5) 太郎は、花子から届いた j と、秘密の数 x を用いて

$$k_1 \equiv j^x \pmod{p}, \quad 0 < k_1 < p$$

なる k_1 を計算する。

- (6) 花子は、太郎から届いた i と、秘密の数 y を用いて

$$k_2 \equiv i^y \pmod{p}, \quad 0 < k_2 < p$$

なる k_2 を計算する。

- (7) 以上の方法で得られた k_1 と k_2 は等しいことが、

$$k_1 \equiv j^x \equiv g^{xy} \equiv i^y \equiv k_2 \pmod{p}, \quad 0 < k_1, k_2 < p$$

よりわかる。これを $k = k_1 = k_2$ とする。

- (8) k が「大きな数」ならば、これを共通の鍵として採用する。もし k が「小さな数」になってしまったら、もう一度はじめからやり直す。

以上の手順において重要なことは、 p, g, i, j は通信路に乗るが、 x, y と鍵 k は通信路に乗らないことである。ここで、 x, y が第三者に知られてしまえば鍵 k も簡単な計算ですぐに知られてしまうが、 p, g, i, j から x や y を求めることは離散対数問題となっており、現実には不可能であると考えられる。すなわち、Diffie-Hellman 鍵共有の安全性は離散対数問題の困難さによるといえる。

11.3 RSA 公開鍵暗号

前節で述べたように、共通鍵暗号は、暗号化の鍵と復号化の鍵が同一、または、一方からもう一方が容易に導出できるものであった。これとは違い、暗号化の鍵がわかって復号化の鍵を得ることが現実的に困難であるような場合、暗号化の鍵を公開しても暗号の安全性は保たれると考えられる。たとえば、インターネット上で多くのユーザからの情報を暗号で受け取りたい人は、まず、暗号化、復号化の鍵を1組だけ生成し、暗号化の鍵のみを公開する。どのユーザもその鍵を使って暗号文を作成し鍵を公開している人に送ることができる。受け手は復号化の鍵を用いて、平文、すなわちユーザの情報を得るわけである。

このように、暗号化の鍵を公開しても安全性が保たれるような暗号を一般に公開鍵暗号という。暗号化の鍵を公開鍵とよび、復号化の鍵を秘密鍵とよぶ。公開鍵暗号は、通信相手の各々に対して別々の鍵を用意する必要がなく鍵管理が容易であるなど、共通鍵暗号に対する利点が多い反面、安全性を保つために鍵を大きくする必要があり処理時間を要するなどの欠点がある。詳しくは、情報工学の文献を参照のこと。

以下で解説する RSA 暗号は、1978年に R. L. Rivest, A. Shamir, L. Adleman により開発された代表的な公開鍵暗号であり、現在広く普及している。花子が太郎からのメッセージを暗号化して送ってほしいとき、RSA 暗号では次のような手順をふむ。

- (1) 【準備】花子は、2つの異なる大きな素数 p, q を用意し、積 $N = pq$ をとる。また、 $\varphi(N) = (p-1)(q-1)$ と互いに素な大きな自然数 $d < \varphi(N)$ を任意にとり、

$$ed \equiv 1 \pmod{\varphi(N)}, \quad 0 < e < \varphi(N)$$

をみたく e を計算する。 (e, N) を公開鍵として太郎に知らせ、 (d, N) を秘密鍵として秘密にする。 p, q および $\varphi(N)$ の値も秘密にする。

- (2) 【暗号化】太郎は、平文 T を自然数として用意する。必要ならば簡単な修正をほどこして、 $T < N$ および $\gcd(T, N) = 1$ が成り立つようにしておく。この T から、公開鍵 (e, N) を用いて

$$C \equiv T^e \pmod{N}, \quad 0 < C < N$$

によって暗号文 C を作成し、花子に送る。

- (3) 【復号化】花子は、届いた暗号文 C から、秘密鍵 (d, N) を用いて

$$T' \equiv C^d \pmod{N}, \quad 0 < T' < N$$

を計算すると、 $T' = T$ となっており太郎からのメッセージを受け取ることができる。

実際、 d, e のとり方から $ed = 1 + m\varphi(N)$ と書けるので、オイラーの定理より

$$T' \equiv C^d \equiv T^{ed} = T^{1+m\varphi(N)} = T(T^{\varphi(N)})^m \equiv T \pmod{N}$$

であるが、一方 $0 < T, T' < N$ であったから $T' = T$ を得る。

さて、RSA 暗号の安全性は、公開鍵 (e, N) から秘密鍵 (d, N) を導出することが困難であることによる。以下に、暗号の安全性に係わる秘密鍵の管理についてまとめておく。

- d は、法 $\varphi(N)$ に関する e の逆元として、ユークリッドの互除法により簡単に計算できてしまうので、受信者花子にとって $\varphi(N)$ の管理は重要である。
- N の素因数 p, q が知られると、 $\varphi(N) = (p-1)(q-1)$ と計算され、上述のとおり秘密鍵が知られてしまうので、 p, q の管理も重要である。
- p, q から $\varphi(N)$ は簡単に計算できるが、逆に $\varphi(N)$ が知られると、

$$\varphi(N) = (p-1)(q-1) = N - (p+q) + 1$$

から $p+q$ がわかり、2 次方程式

$$x^2 - (p+q)x + N = 0$$

を解くことで p, q が求まってしまう。したがって、 N の素因数 p, q が知られることと、 $\varphi(N)$ が知られることは同等であり、これらの管理は同程度に重要である。

大きな整数の素因数分解は一般には難しく、 N から p, q を求めることは現実には不可能であると考えられる。すなわち、素因数分解が困難であることが RSA 暗号の安全性の根拠となっているわけである。

11.4 ハイブリッド暗号システム

実際の RSA 暗号では、素数 p, q を選ぶとき、実際に素数であるかどうかの判定をする必要がある。素因数分解に比べて素数判定は短時間でできること等を考慮して、現状では十進表示で数百桁の素数 p, q を選ぶことになる。したがって N, d, e も数百桁になり、数百桁の数百桁乗の計算を実行することになるが、これには相当な時間がかかる。このようなことも含め様々な理由から、一般に公開鍵暗号は大量のデータを即時に暗号化・複合化するのには適さない。そこで、暗号化したい大量のデータは共通鍵暗号によって通信することとし、そこで使う共通鍵のみを公開鍵暗号によって配送する、という方法が考えられる。すなわち、共通鍵暗号の効率性と公開鍵暗号の安全性を組み合わせるわけである。このような暗号方式はハイブリッド暗号システムとよばれ、広く実用化されている。

このように、公開鍵暗号のような新しい暗号方式が提唱された後でも、以前に使われていた方式が捨てられるわけではなく、それらを共存させて「効率性と安全性」のバランスをとりながら新たな暗号システムが構築されている。ここに紹介したもの以外にも様々な暗号方式があり、それらの多くが整数論に依拠している。さらに「効率性や安全性」の評価にも整数論的な深い考察が必要とされ、暗号理論は整数論の知識なしでは展開できないと言える。