第10章　暗号

10.1　Diffie-Hellman 鍵共有

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（以上はほとんど Wikipedia からの引用）．

さて，整数論の応用という観点から，平文や暗号文は普通の言語で書かれた文としてではなく，自然数として表されたものとして扱うことになる． 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． したがって，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．

いま，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）場合を考えよう． このような暗号を**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，次節で紹介する**公開鍵暗号**が現れる以前は「暗号＝共通鍵暗号」であった． 一般に共通鍵暗号は，公開鍵暗号に比べシンプル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しなくてはならず，その際に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，一方が生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 $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ 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． 太郎と花子が鍵として「大きな数」を共有したいとする．

(1) 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．

(2) 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．

(3) 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．

(4) 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．

(5) 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．

(6) 以上の方法で得られた k_1, k_2 は等しいので，これを共通鍵として用いる．

最後の部分は

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

よりわかる． 重要なことは，p, g, i, j は通信路に乗るが，鍵 $k = k_1 = k_2$ 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．

10.2　RSA 公開鍵暗号

前節で述べたように，共通鍵暗号は，暗号化の鍵から復号化の鍵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も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，すなわち送り手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，あらかじめ共通鍵を用意する必要がなく鍵管理が容易で安全性も高く，また電子署名が容易に実現できるなど，共通鍵暗号に対する利点が多い反面，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，情報工学系の文献を参照のこと．

RSA 暗号は，代表的な公開鍵暗号のひとつであり，R. L. Rivest，A. Shamir，L. Adleman により 1978 年に開発され，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 $e < \varphi(N)$ を任意にとり，

$$de \equiv 1 \pmod{\varphi(N)}, \quad 0 < d < \varphi(N)$$

をみたす d を計算する． (d, N) を公開鍵として太郎に知らせ，(e, 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 (d, N) を用いて

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

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 (e, N) を用いて

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

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

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

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 (d, N) から秘密鍵 (e, N) を導出することが困難であることよる． いま，N の素因数 p, q が知られると，$\varphi(N) = (p-1)(q-1)$ がわかり，したがって，法 $\varphi(N)$ に関する d の逆元としての e が簡単な計算（たとえばユークリッドの互除法）によりわかってしまう． 逆に，e がわかったとき，$de - 1$ の値から $\varphi(N)$ が比較的簡単に求まる． よって，

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

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 が求まる．以上のことをまとめれば，公開鍵 (d,N) が既知のとき

$$N \text{ の素因数 } p \text{ と } q, \qquad \varphi(N), \qquad \text{秘密鍵 } (e,N)$$

のどれか１つが盗まれれば，それから他の２つが計算できることになる．とくに，秘密鍵 (e,N) が知られることと N の素因数が見つかることは同値である．言い換えれば，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．

10.3　ハイブリッド暗号系

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**ハイブリッド暗号系**とよばれ，現在多くのシステムで実用化されている．

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．