# 4　公開鍵暗号

公開鍵暗号の考え方は，1976 年に Whitfield Diffe と Martin Hellman によって考案され，1977 年に Rivest と Shamir，そして Adleman によって実現された．最初に実現された公開鍵暗号は三人の名前から RSA 暗号と呼ばれる．

公開鍵暗号は，それまでに存在していた暗号系とは大きく異なるものである．その特徴の一つとして，換字や転置ではなく数学的な理論に基づいているという点である．もう一つの特徴は，暗号化するための鍵と復号化するための鍵が異なっているという点である．

公開鍵暗号の原理は以下のようになっている．

**鍵生成，登録** 利用者 A は秘密鍵 $S_A$ と公開鍵 $P_A$ の対をある方法で生成する．A は $P_A$ を公開鍵簿に登録する．公開鍵簿は電話帳のようなもので，A の名前に対応して電話番号の代わりに $P_A$ が掲載されている．

**暗号化** 別の利用者 B が A に暗号化して送信する場合を考える．B は公開鍵簿を使い，A の公開鍵 $P_A$ を検索する．次に，通話内容 $m$ を $P_A$ を使って暗号化する．この暗号文を $c$ とする．

**復号化** 暗号文を $c$ を受け取った A は，A だけが知っている秘密鍵 $S_A$ を用いて $m$ を復号化する．

# 5　整数論の基礎

## 5.1　素数

自然数の集合を

$$\mathcal{N} = \{1, 2, 3, \cdots\} \tag{1}$$

整数の集合を

$$\mathcal{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\} \tag{2}$$

とする．

ある $a, b \in \mathcal{N}$ について，$a$ が b で割り切れるとき $b$ は $a$ の約数であるという．1 はすべての自然数の共通の約数である．

任意の $n \in \mathcal{N}$ について，1 と $n$ 自身は明らかに $n$ の約数である．これらを $n$ の自明な約数という．1 以外の自然数 $n$ が自明な約数以外の約数をもたないとき，$n$ は素数であるという．

ある $x, y, z \in \mathcal{Z}$ について，$z$ が $x$ の約数であり，$y$ の約数でもあるとき，$z$ を $x$ と $y$ の公約数といい，その最大のものを最大公約数という．これを $\gcd(a, b)$ で表す．特に，$\gcd(a, b) = 1$ であるとき，$a$ と $b$ は互いに素であるという．

## 5.2　剰余類

ある整数 $a, b$，と正の整数 $n$ に対して，$a - b$ が $n$ の倍数であるとき，$a$ と $b$ は法 $n$ に関して合同であるといい，

$$a \equiv b \pmod{n} \tag{3}$$

と表す．このような式を合同式という．

**例 5.1** $8 - 2 = 6$ は 3 の倍数なので，

$$8 \equiv 2 \pmod{3}$$

$5 - 12 = -7 = (-1) \times 7$ は 7 の倍数なので，

$$5 \equiv 12 \pmod{7}$$

である．[]

任意の整数 $x$ を正の整数 $n$ で割ると，その余り $r$ は $0 \leq r < n-1$ の範囲で現れる．

**例 5.2** ある整数 $x$ を正の整数 $n$ で割ることを考える．ここでは $n=3$ とし，各 $x$ に対する余りを $r$ とすると，表 1 のようになる．

表 *1:* 整数 $x$ を 3 で割ったときの余り $r$

| $x$ | $\cdots$ | $-4$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | $\cdots$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $r$ | $\cdots$ | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | $\cdots$ |

[]

ある整数 $a$ と $b$ を $n$ で割ることを考える．このとき，

$$a = q_1 n + r_1$$
$$b = q_2 n + r_2$$

を満たす $q_1, q_2$ と $r_1, r_2 (0 \leq r_1, r_2 < n-1)$ が存在する．ここで，$r_1 = r_2$ であるとき，$r_1 \equiv r_2 \pmod{n}$ である．そこで，次式

$$a \bmod n \tag{4}$$

を $a$ を $n$ で割ったときの余りを示す記述として使用する．このように $a$ を $a \bmod n$ で置き換えることを，$a$ は法 $n$ で還元されたと呼ぶ．

ある整数を $n$ で割ったときの余りの集合を

$$\mathcal{Z}_n = \{0, 1, \cdots, n-1\} \tag{5}$$

と表す．これを剰余類という．この集合 $\mathcal{Z}_n$ での加算と乗算を定義する．任意の $a, b \in \mathcal{Z}_n$ に対して加算は

$$(a+b) \bmod n \tag{6}$$

であり，乗算は

$$(a \times b) \bmod n \tag{7}$$

である．

**例 5.3** $\mathcal{Z}_{15}$ の加算表を表 2 に示す．

表 *2:* $\mathcal{Z}_{15}$ の加算表

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 9 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 10 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 11 | 11 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 12 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 13 | 13 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 14 | 14 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

[]

**例 5.4** $\mathcal{Z}_{15}$ の乗算表を表 3 に示す.

表 3: $\mathcal{Z}_{15}$ の乗算表

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 2 | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 1 | 3 | 5 | 7 | 9 | 11 | 13 |
| 3 | 0 | 3 | 6 | 9 | 12 | 0 | 3 | 6 | 9 | 12 | 0 | 3 | 6 | 9 | 12 |
| 4 | 0 | 4 | 8 | 12 | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 |
| 5 | 0 | 5 | 10 | 0 | 5 | 10 | 0 | 5 | 10 | 0 | 5 | 10 | 0 | 5 | 10 |
| 6 | 0 | 6 | 12 | 3 | 9 | 0 | 6 | 12 | 3 | 9 | 0 | 6 | 12 | 3 | 9 |
| 7 | 0 | 7 | 14 | 6 | 13 | 5 | 12 | 4 | 11 | 3 | 10 | 2 | 9 | 1 | 8 |
| 8 | 0 | 8 | 1 | 9 | 2 | 10 | 3 | 11 | 4 | 12 | 5 | 13 | 6 | 14 | 7 |
| 9 | 0 | 9 | 3 | 12 | 6 | 0 | 9 | 3 | 12 | 6 | 0 | 9 | 3 | 12 | 6 |
| 10 | 0 | 10 | 5 | 0 | 10 | 5 | 0 | 10 | 5 | 0 | 10 | 5 | 0 | 10 | 5 |
| 11 | 0 | 11 | 7 | 3 | 14 | 10 | 6 | 2 | 13 | 9 | 5 | 1 | 12 | 8 | 4 |
| 12 | 0 | 12 | 9 | 6 | 3 | 0 | 12 | 9 | 6 | 3 | 0 | 12 | 9 | 6 | 3 |
| 13 | 0 | 13 | 11 | 9 | 7 | 5 | 3 | 1 | 14 | 12 | 10 | 8 | 6 | 4 | 2 |
| 14 | 0 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

[]

$\mathcal{Z}_n$ の元を $x$ とし，$\gcd(x,n)=1$ を満たす元の集合を $\mathcal{Z}_n^*$ と表す．これを既約剰余類という.

**例 5.5**

$$\mathcal{Z}_1^*=\{1\} \qquad \mathcal{Z}_2^*=\{1\}$$
$$\mathcal{Z}_3^*=\{1,2\} \qquad \mathcal{Z}_4^*=\{1,3\}$$
$$\mathcal{Z}_5^*=\{1,2,3,4\} \qquad \mathcal{Z}_6^*=\{1,5\}$$

[]

## 5.3 有限体理論

有限体理論は暗号化技術にとって重要な理論的基盤を構築している．ここでは群 (group)，および体 (field) について述べる.

$G$ をある集合とし，$*$ は $G$ 上の二項演算とする．このとき，次の条件を満たすならば，$(G,*)$ は群と呼ばれる.

**G-1.** 任意の $x,y\in G$ に対して，$x*y\in G$ を満たす.

**G-2.** 任意の $x,y,z\in G$ に対して，$x*(y*z)=(x*y)*z$ を満たす.

**G-3.** 任意の $x\in G$ に対して，$x*e=e*x=x$ を満たす $e\in G$ が存在する．(単位元 $e$ が存在する)

**G-4.** 任意の $x\in G$ に対して，$x*x^{-1}=x^{-1}*x=e$ を満たす $x^{-1}\in G$ が存在する．($x$ の逆元 $x^{-1}$ が存在する)

また，任意の $x,y\in G$ に対して，$x*y=y*x$ を満たすような $(G,*)$ を可換群またはアーベル群という.

群の元の個数が無限であるような群を無限群と呼び，元の個数が有限となるような群を有限群と呼ぶ.

**例 5.6** $(\mathcal{Z},+)$ は可換群 ( 無限群 ) である.

$(\mathcal{Z},\times)$ は群ではない．なぜなら，条件 $G-4$ を満たさないからである.. 例えば，単位元 $e$ は 1 である．$x=4$ とすると，$xx^{-1}=x^{-1}x=e$ を満たす $x^{-1}$ は $1/4$ である．$1/4\notin\mathcal{Z}$ なので条件 $G-4$ は満たされない．[]

$F$ をある集合とし，加法 $+$ と乗法 $\cdot$ を $F$ 上の二項演算とする．このとき，次の条件を満たすならば，$(F,+,\cdot)$ は体と呼ばれる.

**F-1.** $(F,+)$ は可換群である．(加算単位元は $0 \in F$ である)

**F-2.** $(F \setminus \{0\},\cdot)$ は可換群である．(乗算単位元 $e \in F$ は $e \neq 0$ を満たす)

**F-3.** 任意の $x,y,z \in F$ に対して，$x\cdot(y+z) = x\cdot y + x\cdot z$，$(x+y)\cdot z = x\cdot z + y\cdot z$ を満たす．

体の元の個数が有限の体を有限体という．一般的に，$p$ 個の個数を持つ有限体を $F_p$ と表す．整数の集合 $\mathcal{Z}_p$ に対してもし $p$ が素数であるとき，それは体となる．

有限体 $\mathcal{Z}_p$ について，$\mathcal{Z}_p^* = \mathcal{Z}_p \setminus \{0\}$ は乗法群として巡回群である．つまり，$\mathcal{Z}_p$ の元の個数を $p$ とすると

$$\mathcal{Z}_p^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}$$

となる $\alpha \in \mathcal{Z}^*$ が存在する．この $\alpha$ は $\mathcal{Z}_p$ の原始元と呼ばれる．

剰余類 $\mathcal{Z}_n$ について考える．$(\mathcal{Z}_n,+)$ は可換群であり，$(\mathcal{Z}_n \setminus \{0\},\times)$ は $n$ の値によって体になったり，ならなかったりする．

$(\mathcal{Z}_n \setminus \{0\},\cdot)$ の単位元は 1 である．ある $x \in \mathcal{Z}_n \setminus \{0\}$ に逆元 $x^{-1} \in \mathcal{Z}_n \setminus \{0\}$ が存在するとき，

$$xx^{-1} \equiv x^{-1}x \equiv 1 \pmod{n} \tag{8}$$

が成り立つ．上式から，ある $k \in \mathcal{Z}$ が存在して，

$$xx^{-1} + kn = 1 \tag{9}$$

が成り立つことがわかる．この式は $\gcd(x,n) = 1$，$\gcd(x^{-1},n) = 1$ であることを表している．つまり，$\mathcal{Z}_n$ の元で，$\gcd(x,n) = 1$ を満たすものが逆元 $x^{-1}$ をもつ．つまり，$\mathcal{Z}_n^*$ と $\mathcal{Z}_p \setminus \{0\}$ の任意の元は乗法の逆元を持つ．

## 5.4 ユークリッドの互除法

ユークリッドの互除法とは，ユークリッドが発明した 2 つの整数の最大公約数を求めるアルゴリズムである．

**アルゴリズム 1 (ユークリッドの互除法)** $a,b \in \mathbb{Z}$ に対して，次の操作を行い，$\gcd(a,b)$ を得る．

**入力** $a$ と $b$ を入力する．

**初期設定** 初期設定として次の操作を行う．

$$r_{-1} = a$$
$$r_0 = b$$

**step** $i$ $r_i \neq 0 (i = 0,1,2,\cdots,n-1)$ である限り以下の操作を行う．ただし，$r_n = 0$ である．

$r_{i-1}$の $r_i$による除算の剰余を $r_{i+1}$とする．

**出力**

$$\gcd(a,b) = r_{n-1}$$

**例 5.7** 85 と 204 の最大公約数 $\gcd(85,204)$ を求める．

**入力** $a = 85$，$b = 204$ とする．

**初期設定**

$$r_{-1} = 85$$
$$r_0 = 204$$

**step** 1

85 の 204 による除算の剰余は 85 である．

**step** 2

204 の 85 による除算の剰余は 34 である．

**step** 3

85 の 34 による除算の剰余は 17 である．

**step** 4

34 の 17 による除算の剰余は 0 である．

**出力**

$$\gcd(a, b) = 17$$

[]

アルゴリズム 1 は各 step $n(n = 1, \cdots)$ の商を $q_n$ とすると次のように表せる．

$$\begin{cases} r_{-1} = q_1 r_0 + r_1 \quad (0 < r_1 < r_0) \\ r_0 = q_2 r_1 + r_2 \quad (0 < r_2 < r_1) \\ r_1 = q_3 r_2 + r_3 \quad (0 < r_3 < r_2) \\ \quad \vdots \\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad (0 < r_{n-1} < r_{n-2}) \\ r_{n-2} = q_n r_{n-1} + r_n \quad (r_n = 0) \\ \gcd(a, b) = r_{n-1} \end{cases} \tag{10}$$

これは次のように表せる．

$$\gcd(r_{-1}, r_0) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{i-3}, r_{i-2}) = \gcd(r_{i-2}, r_{i-1}) = r_{i-1}$$

ここで，式 (10) は次式のようにまとめられる．

$$r_{i-2} = q_i r_{i-1} + r_i \quad (i = 1, \cdots, n) \tag{11}$$

上式を変形すると次式が得られる．

$$r_i = r_{i-2} - q_i r_{i-1} \tag{12}$$

また，

$$r_{-1} = a = 1 \cdot a + 0 \cdot b \tag{13}$$
$$r_0 = b = 0 \cdot a + 1 \cdot b \tag{14}$$

であるから，次式を導入する．

$$r_i = u_i a + v_i b \quad (i = 0, 1, \cdots, n) \tag{15}$$

上式は $i - 1$，$i - 2$ の場合，次のようになる．

$$r_{i-1} = u_{i-1} a + v_{i-1} b \tag{16}$$

$$r_{i-2} = u_{i-2}a + v_{i-2}b \tag{17}$$

ここで，式 (12) に式 (16) と式 (17) を代入する．

$$r_i = u_{i-2}a + v_{i-2}b - q_i(u_{i-1}a + v_{i-1}b)$$

これを整理すると次式を得る．

$$r_i = (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b$$

ここで，

$$u_i = u_{i-2} - q_i u_{i-1} \tag{18}$$

$$v_i = v_{i-2} - q_i v_{i-1} \tag{19}$$

とおくと，次式を得る．

$$r_i = u_i a + v_i b \tag{20}$$

以上から，以下に示すアルゴリズム 2 を得る．

**アルゴリズム 2 (拡張されたユークリッドの互除法)** $a, b \in \mathbb{Z}$ に対して，次の操作を行う．

**入力** $a$ と $b$ を入力する．

**初期設定** 初期設定として次の操作を行う．

$r_{-1} = a$, $u_{-1} = 1$, $v_{-1} = 0$ とする．
$r_0 = b$, $u_0 = 0$, $v_0 = 1$ とする．

**step** $i$ $r_i \neq 0 (i = 1, 2, \cdots, n-1)$ である限り以下の操作を行う．ただし，$r_n = 1$ である．

$r_{i-2}$の $r_{i-1}$による除算の剰余を $r_i$とする．
$r_{i-2}$の $r_{i-1}$による割算の商を $q_i$とする．
$u_i = u_{i-2} - q_i u_{i-1}$
$v_i = v_{i-2} - q_i v_{i-1}$

**出力**

$$\gcd(x, y) = r_{n-1}$$

**例 5.8** $\gcd(408, 595)$ を求める．

**入力** $a = 408$，$b = 595$ とする．

**初期設定**

$r_{-1} = 408$, $u_{-1} = 1$, $v_{-1} = 0$ とする．
$r_0 = 595$, $u_0 = 0$, $v_0 = 1$ とする．

**(step** 1**)**

408 の 595 による除算の剰余は 408 である．
408 の 595 による除算の商は 0 である．

$$\begin{aligned} u_1 &= 1 - 0 \times 0 \\ &= 1 \\ v_1 &= 0 - 0 \times 1 \\ &= 0 \end{aligned}$$

**(step 2)**

595 の 408 による除算の剰余は 187 である．
595 の 408 による除算の商は 1 である．

$$\begin{aligned} u_2 &= 1 - 1 \times 1 \\ &= 1 \\ v_2 &= 0 - 1 \times 1 \\ &= 0 \end{aligned}$$

**(step 3)**

408 の 187 による除算の剰余は 34 である．
408 の 187 による除算の商は 2 である．

$$\begin{aligned} u_3 &= 0 - 2 \times 1 \\ &= -2 \\ v_3 &= 1 - 2 \times (-1) \\ &= 3 \end{aligned}$$

**(step 4)**

187 の 34 による除算の剰余は 17 である．
187 の 34 による除算の商は 5 である．

$$\begin{aligned} u_4 &= 1 - 5 \times (-2) \\ &= 11 \\ v_4 &= -1 - 5 \times (3) \\ &= -16 \end{aligned}$$

**(step 5)**

34 の 17 による除算の剰余は 0 なので終了．

**出力**

$$\begin{aligned} \gcd(x, y) &= 17 \\ &= 11 \times 408 + (-16) \times 595 \end{aligned}$$

[]

## 5.5 平方剰余問題

**定義 5.1** $p$ を奇数の素数，$x$ を整数で，$1 \leq x \leq p-1$ とする．合同式 $y^2 \equiv x \pmod{p}$ が解 $y \in \mathcal{Z}_p$ をもつならば，$x$ は $p$ を法とする**平方剰余 (quadratic residue)** と定義される．$x \neq 0 \pmod{p}$ かつ $x$ が $p$ を法とする平方剰余でないならば，$x$ は $p$ を法とする**非平方乗余 (quadratic non-residue)** と定義する．

**例 5.9** 11 を法とする平方剰余は $1,3,4,5,9$ である．ここで，$(\pm 1)^2 = 1$，$(\pm 5)^2 = 3$，$(\pm 2)^2 = 4$，$(\pm 4)^2 = 5$，$(\pm 3)^2 = 9$,（それぞれ $\mathcal{Z}_{11}$ についての演算.）　[]

平方剰余の判定問題は Euler の判定法としてよく知られている．

**定理 5.2** *Euler* の判定法 *(Euler's criterion)*
$p$ を素数をすると，$x$ が $p$ を法とする平方剰余であるための必要十分条件は

$$x^{(p-1)/2} \equiv 1 \pmod{p}$$

## 5.6　オイラーの関数

$\phi(n)$ はオイラーの関数と呼ばれ，$\mathcal{Z}_n^*$ の元の個数を表している．言い換えると，$\phi(n)$ は $1 \leq \alpha < n$ である整数 $\alpha$ のうち $\gcd(\alpha, n) = 1$ となる個数をあらわしている．

もし $p$ が素数であれば，$1 \leq \alpha < p$ の $\alpha$ はすべて $p$ と互いに素であるので，次式が成り立つ．

$$\phi(p) = p - 1 \tag{21}$$

もし $n$ が相異なる素数 $p, q$ の積，つまり $n = pq$ であるとき，

$$\begin{aligned} \phi(n) &= \phi(pq) \\ &= \phi(p)\phi(q) \\ &= (p-1)(q-1) \end{aligned} \tag{22}$$

が成り立つ．

**例 5.10** $n = 7$ の場合，$1 \leq \alpha < 7$ の整数で $\gcd(\alpha, 7) = 1$ となるものは $\{1,2,3,4,5,6\}$ なので $\phi(n) = 6$ である．

$n$ は素数なので式 (21) を用いると，

$$\begin{aligned} \phi(7) &= 7 - 1 \\ &= 6 \end{aligned}$$

となる．[]

**例 5.11** $n = 14$ の場合，$1 \leq \alpha < 14$ の整数で $\gcd(\alpha, 14) = 1$ をみたす $\alpha$ は $\{1,3,5,9,11,13\}$ なので $\phi(n) = 6$ である．

$14 = 2 \times 7$ であり，2 と 4 は素数なので式 (22) を適用できる．

$$\begin{aligned} \phi(14) &= (2-1)(7-1) \\ &= 6 \end{aligned}$$

[]

## 5.7　オイラーの定理

オイラーの定理は，任意の $x \in \mathcal{Z}_n^*$ に対して

$$x^{\phi(n)} \equiv 1 \pmod{n} \tag{23}$$

が成立すると述べている．

ここで，式 (23) の両辺を $k \in \mathcal{Z}$ 乗する．

$$\begin{aligned} x^{k\phi(n)} &\equiv 1^k \pmod{n} \\ &\equiv 1 \pmod{n} \end{aligned} \tag{24}$$

さらに，上式の両辺に $x$ をかけると次のようになる．

$$x^{k\phi(n)+1} \equiv x \pmod{n} \tag{25}$$

これは $x$ が $\mathcal{Z}_n^*$ の元なら，$k\phi(n)+1$ 乗すれば $x$ に戻るということを表している．しかし，これは $n$ が相異なる素数 $p, q$ の積なら，任意の $x \in \mathcal{Z}_n$ に対しても成り立つ．

ここで，$k\phi(n)+1$ について考える．まず，

$$y = k\phi(n) + 1 \tag{26}$$

とおく．この式は，$\phi(n)$ を $k$ 倍したものに 1 を加えたものだから，

$$y \equiv 1 \pmod{\phi(n)} \tag{27}$$

が成り立つ．上式において，$y = ab$ とすると次式が成り立つ．

$$ab \equiv 1 \pmod{\phi(n)} \tag{28}$$

この式は $a$ と $b$ が，

$$\begin{aligned} \gcd(a, \phi(n)) &= 1 \\ \gcd(b, \phi(n)) &= 1 \end{aligned}$$

を満たし，さらに $b$ が $\phi(n)$ における $a$ の乗法の逆数 ($a$ が $\phi(n)$ における $b$ の乗法の逆数) であることを表している．

以上から次のことが言える．

$p, q$ を互いに異なる素数とし，$n = pq$ とする．ある整数 $a$ が $\gcd(a, \phi(n))$ を満たすなら，

$$ab \equiv 1 \pmod{\phi(n)}$$

を満たす $b$ が存在し，任意の $x \in \mathcal{Z}_n$ に対して，

$$x^{ab} \equiv x \pmod{\phi(n)} \tag{29}$$

が成り立つ．

**例 5.12** 相異なる素数 $p, q$ を $p = 3, q = 5$ とすると $n = 15$ である．式 (22) から，

$$\begin{aligned} \phi(n) &= \phi(pq) \\ &= (3-1)(5-1) \\ &= 8 \end{aligned}$$

である．8 と互いに素である数として 3 を選ぶ． mod 8 の 3 の乗法の逆数は 3 である．$x = 3$ とすると，

$$3^{3\times 3} \equiv 3 \pmod{8}$$

が成り立つ．[]

# 6 RSA 暗号

**鍵生成** 次のように，暗号化鍵と復号化鍵を求める．

1. 相異なる素数 $p, q$ を選び，$n = pq$ を求める．
2. $\phi(n)$ と互いに素である数 $e$ を選ぶ．
3. $\mathrm{mod}\phi(n)$ での $e$ の乗法の逆数 $d$ を求める．

以上から，暗号化鍵 $n, e$ と復号化鍵 $d, n$ が得られる．ただし，$n, e$ を公開し，$p, q, \phi(n), d$ は公開してはならない．

**暗号化** 平文 $x(x \leq n)$ に対して

$$y = x^e \bmod n \tag{30}$$

となる暗号文 $y$ を求める．

**復号化** 暗号文 $y$ に対して

$$x = y^d \bmod n \tag{31}$$

となる平文 $x$ を求める．

**例 6.1** 文字 *RSA* を暗号化，復号化する．これらの文字は *10* 進数で表すと *ASCII* コードでは，$R = 82, S = 83, A = 65$ である．これを一文字毎に暗号化，復号化する．

**鍵生成** 次のように，暗号化鍵と復号化鍵を求める．

1. $p = 17, q = 7$ とする．$n = 17 \times 7 = 119$ である．
2. $\phi(n) = 96$ であり，$e = 13$ とする．
3. $\mathrm{mod}\phi(n)$ での $e$ の乗法の逆数 $d$ は 37 である．

以上から，暗号化鍵 $n = 119, e = 13$ と復号化鍵 $d = 37, n = 119$ が得られる．

**暗号化** $x_1 = R = 82, x_2 = S = 83, x_3 = A = 65$ に対して，暗号文 $y_1, y_2, y_3$ を求める．

$$\begin{aligned}
y_1 &= x_1^e \bmod n \\
&= 82^{13} \bmod 119 \\
&= 5 \\
y_2 &= x_2^e \bmod n \\
&= 83^{13} \bmod 119 \\
&= 104 \\
y_3 &= x_3^e \bmod n \\
&= 65^{13} \bmod 119 \\
&= 107
\end{aligned}$$

**復号化** 暗号文 $y_1, y_2, y_3$ に対して，平文 $x_1, x_2, x_3$ を求める．

$$\begin{aligned} x_1 &= y_1^d \bmod n \\ &= 5^{37} \bmod 119 \\ &= 82 \\ &= R \\ x_1 &= y_2^d \bmod n \\ &= 104^{37} \bmod 119 \\ &= 83 \\ &= S \\ x_1 &= y_3^d \bmod n \\ &= 107^{37} \bmod 119 \\ &= 65 \\ &= A \end{aligned}$$

[]

素因数 $p$ と $q$ から $n$ を簡単に計算できる．また，$e$ と $d$ を求めることも易しい．しかし，暗号文 $y$ と暗号化鍵 $n, e$ 知ったとしても，暗号文 $y$ から平文 $x$ を求めることは非常に難しい．現在のところ，復号化鍵 $d$ を求めずに $y$ から $x$ を得る一般的な方法，そして，素因数分解 $n = pq$ を知らずに $d$ を求める一般的な方法が知られていない．従って，$y$ から $x$ を得るには $d$ を求めることが必要で，そのためには $\phi(n)$ を求める必要があり，そのためには素因数分解が必要となる．結局，暗号文 $y$ から平文 $x$ を求めるためには，素数因数分解 $n = pq$ が必要になるが，この素数因数分解は $p, q$ が大きくなるほど難しくなる．RSA 暗号のポイントは素数 $p, q$ から $n$ を得るのは簡単であるが，$n$ から $p, q$ を求めることは非常に困難であるという一方向性にある．

ただし，厳密には RSA 暗号を解読することは $n$ を素因数分解することと同程度難しいらしい，としかいえない．なぜなら，現在のところ，復号化鍵 $d$ を求めずに $y$ から $x$ を得る簡単な方法が存在しないことも，素因数分解 $n = pq$ を知らずに $d$ を求める方法が存在しないことも証明されていないからである．

# 参考文献


[1] Charlie Kaufman，Radia Perlman，Mike Speciner (訳：石橋啓一郎，菊地浩明，松井彩，土井祐介)，ネットワークセキュリティー，プレスティンホール出版 (1997)

[2] 楫元，情報数学シリーズ A-5 工学系のための初等整数論入門-公開鍵暗号を目指して-，培風館 (2000)

[3] Douglas R. Stinson (監訳：櫻井幸一) 暗号理論の基礎，共立出版 (1996)

[4] 岡本龍明，山本博資，シリーズ／情報科学の数学 現代暗号，産業図書 (1998)

[5] Neal Loblits，(訳：林彬)，暗号の代数理論，シュプリンガーフェアラーク東京 (1999)

[6] 岡本龍明，太田知夫，暗号 · ゼロ知識証明 · 数論，共立出版 (1995)

[7] 和田秀男，[改訂版] コンピュータと素因子分解，遊星社 (1999)

[8] 山本芳彦，岩波講座 現代数学への入門 4 数論入門，岩波書店 (1996)

# 7 ElGamal暗号系

ElGamal 暗号系は離散対数問題に基づいている．離散対数とは、素数 $p$ を定めたとき，$\mathcal{Z}_p^*$ における原始元 $\alpha$ に対して，$\alpha^a \equiv \beta \pmod p$ であるような唯一の整数 $a$ $(0 \le a \le p-2)$ を求める．この整数 $a$ を $a = \log_\alpha \beta$ と記する．$p$ をうまく選べば，この問題は一般に難しいと考えられている．

## 7.1 $\mathcal{Z}_p^*$ における ElGamal 暗号方式

A を送信者，B を受信者とすると，B は予め暗号化鍵を生成して公開しておかなければならない．A はその公開鍵を用いて平文 M を暗号化し，その暗号文を受け取った B は自分の秘密鍵で復号化する．A と B は $\mathcal{Z}_p^*$ と $\alpha$ を決めておく．
$p$ を $\mathcal{Z}_p$ において離散対数問題が手に負えなくなる素数とする．また，$\alpha \in \mathcal{Z}_p^*$ を原始元とする．ここで，$\mathcal{P} = \mathcal{Z}_p^*$，$\mathcal{C} = \mathcal{Z}_p^* \times \mathcal{Z}_p^*$ として，以下のように定義する．

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$$

値 $p, \alpha, \beta$ は公開されていて，$a$ は秘密であるとする．
K= $(p, \alpha, a, \beta)$ と（秘密）の乱数 $k \in \mathcal{Z}_{p-1}$ について

$$e_K(x, k) = (y_1, y_2)$$

と定義する．ここで

$$y_1 = \alpha^a \pmod p$$
$$y_2 = x\beta^k \pmod p$$

である．
$y_1$,$y_2 \in \mathcal{Z}_p^*$ に対して

$$d_k(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p$$

と定義する．

**例 7.1** $p = 2579$, $\alpha = 2$, $a = 765$ とする．このとき

$$\beta = 2^{765} \bmod 2579 = 949$$

である．ここでアリスはメッセージ $x = 1299$ をボブに送りたいとする．また，アリスは乱数として $k = 853$ を選んだとする．このときアリスは以下の計算を行う．

$$y_1 = 2^{853} \bmod 2579 = 435$$

さらに

$$y_2 = 1299 \times 949^{853} \bmod 2579 = 2396$$

ボブは暗号文 $y = (435, 2396)$ を受け取って以下の計算をする．

$$x = 2396 \times (435^{765})^{-1} \bmod 2579 = 1299$$

これは，アリスが暗号化した平文となっている． □

# 8　楕円曲線暗号系

楕円曲線暗号は 1985 年に Koblitz 氏と Miller 氏がほぼ同時に独立に考案した公開鍵型の暗号方式．楕円曲線と呼ばれる数式によって定義される特殊な加算法に基づいて暗号化，復号化を行う暗号方式．解読の困難さは，楕円曲線上の離散対数問題を解くのと同程度と言われ，効率のよい解読法はまだ発見されていない．短い鍵で高い安全性が確保でき，また計算も高速に行うことができる．1024 ビットの鍵を使う RSA 暗号と同程度の安全性を，楕円曲線暗号では 160 ビットで実現することができる．また，暗号化，復号化は RSA 暗号に比べて約 10 倍高速であると言われている．こうして，楕円曲線暗号は，スーパーコンピュータを利用しなくても，われわれが普段利用しているパーソナルコンピュータで十分高速に動作する，これが，楕円曲線暗号の魅力である．

## 8.1　$\mathcal{Z}_p$ 上の楕円曲線

**定義 8.1**　$p > 3$ を素数とする．$Z_p$ 上の楕円曲線 $y^2 = x^3 + ax + b$ は合同式

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

の解 $(x, y) \in Z_p \times Z_p$ 全体の集合である．ここで，$a, b \in Z_p$ は $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ を満たす整数で，無限遠点 $\mathcal{O}$ を一緒にもつ．

楕円曲線 $E$ 上の点に対する適当な加算演算 $+$ が以下のように定義される．ここで，すべての算術演算は $Z_p$ の上で行われる．

$$P = (x_1, y_1), \qquad Q = (x_2, y_2)$$

を $E$ 上の点とする．もし $x_2 = x_1$ かつ $y_2 = -y_1$ ならば，$P + Q = \mathcal{O}$ とするが，そうでないなら $P + Q = (x_3, y_3)$ とする．ただし，

$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$

かつ

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & \text{if } P \neq Q, \\ (3x_1^2 + a)(2y_1)^{-1}, & \text{if } P = Q. \end{cases}$$

最後に，すべての $P \in E$ について以下のように定義する．

$$P + \mathcal{O} = \mathcal{O} + P = P.$$

ここで加算の定義を与えることで，$(E, +)$ が単位元 $\mathcal{O}$ を持つ可換群であることも証明できる．

**例 8.1**　$E$ を $Z_{11}$ 上の楕円曲線 $y^2 = x^3 + x + 6$ とする．まず $E$ 上の点を決める．これには，可能性のある $x \in \quad Z_{11}$ を取って $x^3 + x + 6 \bmod 11$ を計算し，$y$ についての方程式 $y^2 \equiv x^3 + x + 6 \pmod{11}$ を解いて見ることで実行できる．与えられた $x$ について，Euler の判定条件を利用し，$z = x^3 + x + 6 \bmod 11$ が平方剰余であるかどうかを判定できる．ここで素数 $p \equiv 3 \pmod{4}$ の場合，$p$ を法とする平方剰余の平方根の計算には具体的な公式がある．$\beta$ が $p$ を法とする平方剰余であれば，$\pm\beta^{(p+1)/4} \bmod p$ が法 $p$ とする $\beta$ の二つの平方根である．この公式を用いると，平方剰余 $z$ の平方根は

$$\pm z^{(11+1)/4} \bmod 11 = \pm z^3 \bmod 11$$

となる．この計算結果は次の表 4 に示す通りである．こうして，$E$ 上には 13 個の点が存在することが分かる．素数位数の群は常に巡回群であるから，$E$ は $Z_{13}$ と同型であり，無限遠点以外のどの点も $E$ の

表 4: $Z_{11}$ 上の楕円曲線 $y^2 = x^3 + x + 6$ の点

| x | $x^3 + x + 6 \bmod 11$ | in $QR(11)$? | y |
|---|---|---|---|
| 0 | 6 | no | |
| 1 | 8 | no | |
| 2 | 5 | yes | $4, 7$ |
| 3 | 3 | yes | $5, 6$ |
| 4 | 8 | no | |
| 5 | 4 | yes | $2, 9$ |
| 6 | 8 | no | |
| 7 | 4 | yes | $2, 9$ |
| 8 | 9 | yes | $3, 8$ |
| 9 | 7 | no | |
| 10 | 4 | yes | $2, 9$ |

生成元である．ここで生成元 $\alpha = (2, 7)$ を選んだ時，$\alpha$ の“ べき乗 ”( ここでの群の演算は加算演算であるので，これは $\alpha$ の倍数のように書かれる ) を計算することができる．$2\alpha = (2, 7) + (2, 7)$ を計算するにはまず，以下を計算する．

$$\begin{aligned}\lambda &= (3 \times 2^2 + 1)(2 \times 7)^{-1} \bmod 11 \\ &= 2 \times 3^{-1} \bmod 11 \\ &= 2 \times 4 \bmod 11 \\ &= 8\end{aligned}$$

従って

$$x_3 = 8^2 - 2 - 2 \bmod 11 = 5,$$

かつ

$$y_3 = 8(2 - 5) - 7 \bmod 11 = 2$$

であるから $2\alpha = (5, 2)$ を得る．次の倍数は $3\alpha = 2\alpha + \alpha = (5, 2) + (2, 7)$ であるので，さらに $\lambda$ をここでは以下のように計算する．

$$\begin{aligned}\lambda &= (7 - 2)(2 - 5)^{-1} \bmod 11 \\ &= 5 \times 8^{-1} \bmod 11 \\ &= 5 \times 7 \bmod 11 \\ &= 2.\end{aligned}$$

よって以下を得る：

$$x_3 = 2^2 - 5 - 2 \bmod 11 = 8,$$

かつ

$$y_3 = 2(5 - 8) - 2 \bmod 11 = 3.$$

ゆえに，$3\alpha = (8, 3)$ となる．この方法を続けて残りの倍数を計算すると，次のようになる．

$$\begin{array}{lll} \alpha = (2, 7), & 2\alpha = (5, 2), & 3\alpha = (8, 3), \\ 4\alpha = (10, 2), & 5\alpha = (3, 6), & 6\alpha = (7, 9), \\ 7\alpha = (7, 2), & 8\alpha = (3, 5), & 9\alpha = (10, 9), \\ 10\alpha = (8, 8), & 11\alpha = (5, 9), & 12\alpha = (2, 4). \end{array}$$

したがって，$\alpha = (2,7)$ は確かに原始元であることが分かる．

楕円曲線 $E$ 上の点数 $\#E$ について次の Hasse 定理があるが，$\#E$ の正確な値を計算することは難しい．

**定理 8.2** $p > 3$ を素数とする．$Z_p$ 上の楕円曲線 $E$ 上の点数 $\#E$ は次の不等式を満たす．

$$|\#E - (p+1)| \leq 2\sqrt{p}.$$

# 9 楕円曲線上の ElGamal 暗号系

ElGamal 暗号系は離散対数問題が困難であるようなあらゆる群の上で実現できる．楕円曲線 $E$ 上にも可換群を定義することができる．ElGamal 暗号系を楕円曲線 $E$ 上に定義したいならば，離散対数問題が困難であるような $E$ の巡回部分群を調べる必要がある．

**定理 9.1** $p > 3$ を素数とし，$E$ を $Z_p$ 上で定義された楕円曲線とする．この時，$E$ が $Z_{n_1} \times Z_{n_2}$ と同型であるような整数 $n_1$ と $n_2$ が存在する．さらに，$n_2 | n_1$ かつ $n_2 | (p-1)$ である．

従って，もし二つの整数 $n_1$ と $n_2$ が計算できるならば，$E$ は $Z_{n_1}$ と同型な巡回部分群を持ち，これは ElGamal 暗号系を構成することに利用できる可能性がある．

ここで，$n_2 = 1$ の時 $E$ が巡回群であることに注意してほしい．また，もし $\#E$ が素数または異なる素数の積である時，$E$ は巡回群でなければならない．

次は例 8.1 の楕円曲線を用いて ElGamal 暗号系の例を着作って見る．

**例 9.1** $\alpha = (2,7)$ かつ Bob の秘密 “ べき指数 ” を $a = 7$ とすると

$$\beta = 7\alpha = (7,2).$$

よって，暗号化演算は $x \in E$，$0 \leq k \leq 12$，において

$$e_K(x,k) = (k(2,7), x + k(7,2))$$

であり，復号化は

$$d_K(y_1, y_2) = y_2 - 7y_1.$$

また，Alice はメッセージ $x = (10,9)$（これは $E$ 上の点）を暗号化したいとする．もし，Alice が乱数 $k = 3$ を選んだとすると，Alice は以下のような計算を行う．

$$y_1 = 3(2,7) = (8,3),$$

さらに

$$y_2 = (10,9) + 3(7,2) = (10,9) + (3,5) = (10,2).$$

ゆえに $y = ((8,3),(10,2))$．ここで，Bob が暗号文 $y$ を受け取った時，以下のようにして復号化を行う．

$$x = (10,2) - 7(8,3) = (10,2) - (3,5) = (10,2) + (3,6) = (10,9).$$

従って，この復号化から正しい平文を得ることができる．

# 参考文献


[1] A. K. Lenstra and E. R. Verhen, *Selecting cryptograpic key sizes*, in: H. Imai and Y. Zheng, eds., *Public Key Cryptography*, Springer-Verlag., Berlin, Heideberg, New York, 2000.

[2] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, 1995.

[3] 岡本龍明，山本博資，現代暗号，産業図書株式会社，1997.

# 10　結論

- 共通鍵暗号系のスピードが速いが、鍵を安全に相手に送る手段がない。
- 公開鍵暗号系の安全性が高いが、スピードが遅い。
- 公開鍵暗号系は共通鍵の配送に使う、平文の暗号化と復号は共通鍵暗号系で。
- 安全性の要求が高い、記憶容量が少ないのは　楕円曲線暗号系で (Master card など)。