安全で高速な Chebyshev 多項式型公開鍵暗号

Chebyshev 多項式による ElGamal 暗号型の公開鍵暗号を，方程式による拡大体の観点から見直し，合成数を法とすると，Rabin 暗号と同じく，安全性の根拠を大きな合成数の素因数分解の困難さとすることができることを示した。

条件を満たす公開鍵において，「離散対数問題の解が求まれば，N＝pq を素因数分解できる」ことが証明する。したがって，その対偶

「N＝pq の素因数分解できない⇒離散対数問題の解は求まらない」

が示されたことになる。ただし，離散対数問題を解かずに，直接に DH 問題が解かれる可能性は否定できない。

また，素数を法とする場合は，有限体上の ElGamal 暗号と同じ安全性しかないことも示す。したがって，N=pq の素因数分解が求まり，かつ，素数を法とする有限体上の離散対数問題が解ければ，この暗号が解けることになる。

暗号化・復号時間は，共に通常の ElGamal 暗号の$\frac{4}{3}$倍かかる。また，中国人剰余定理を用いた場合，RSA 暗号の復号時間と比べても$\frac{4}{3}$倍かかる。しかし，指数法則 $a^r a^s = a^{r+s}$ に対応する法則が使えないため，有限体上の ElGamal 暗号および楕円曲線暗号に対する高速解読法がすべて無効となる。したがって，冪乗の指数のビット数を共通鍵暗号程度（楕円曲線暗号の$\frac{1}{2}$程度）にしても，安全性が損なわれることはなく，2048bit の暗号では暗号化の冪乗の指数を 112bit 程度に小さくとってもよいと思われる。さらに，新規に開発した「ElGamal 暗号の復号の高速化法」を用いて復号の冪乗の指数を極端に小さくすれば，復号が桁違いに高速になる。

また，このとき，デジタル署名では，RSA 署名と比べて署名生成が 3.4 倍ほど高速となり，署名長は，RSA 署名と同じである。

2 次方程式の解からのアプローチ

Chebyshev 多項式とは，n を整数として $\cos n\theta$ を $\cos\theta$ だけで表したときの，$\cos\theta$ の多項式で

$\cos 1\theta = \cos\theta$　より　$T_1(x) = x$

$\cos 2\theta = 2\cos^2\theta - 1$　より　$T_2(x) = 2x^2 - 1$

$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$　より　$T_3(x) = 4x^3 - 3x$

……

などの多項式である。このとき，$\cos(mn\theta)$ を $\cos\theta$ で表すことを考えれば

$$\cos((mn)\theta) = \cos(m(n\theta)) = \cos(n(m\theta))$$

より恒等式

$$T_{mn}(x) = T_m(T_n(x)) = T_n(T_m(x))$$

が成り立つ。特に，x に定数 c を代入すると

$$T_{mn}(c) = T_m(T_n(c)) = T_n(T_m(c))$$

この等式により，ElGamal 暗号型の公開鍵暗号が構成できる。

この公開鍵暗号を，２次方程式の解の観点から構築する。

$\cos\theta=\dfrac{e^{i\theta}+e^{-i\theta}}{2}$　であるから，2 次方程式 $x^2-(2\cos\theta)x+1=0$ の 2 解を α,β とすると，2 解は $e^{i\theta}$ と $e^{-i\theta}$ である。よって，n を整数として

$$\alpha^n+\beta^n=2\cos n\theta$$

が成り立つ。

ここで，$2\cos\theta=k$ と置き，次のように考える。

k を巨大な整数として，2 次式 x^2-kx+1 を考え，2 次方程式 $x^2-kx+1=0$ の複素数体上の 2 解を α,β とする。ただし，α,β は有理数でないものとする。

このとき，解と係数の関係により

$$\alpha+\beta=k,\quad \alpha\beta=1$$

α^n,β^n を 2 解に持つ 2 次方程式を求める。

x^n を x^2-kx+1 で割った商を $Q(x)$，余りを $sx+t$ とすると

$$x^n=(x^2-kx+1)Q(x)+sx+t\quad\cdots①$$

ここで，s，t は整数である。

s，t の値を求めるには $x^2=kx-1$ による次数下げを繰り返し行えばよい。

すなわち x^2-kx+1 を法として $x^i\equiv ax+b$ とすれば

$$\begin{aligned}x^{2i}&\equiv(ax+b)^2\\&=a^2x^2+2abx+b^2\\&\equiv a^2(kx-1)+2abx+b^2\\&=(ka^2+2ab)x+b^2-a^2\\&=a(ka+2b)x+(b+a)(b-a)\end{aligned}$$

$$\begin{aligned}x^{i+1}&\equiv x(ax+b)\\&=ax^2+bx\\&\equiv a(kx-1)+bx\\&=(ka+b)x-a\end{aligned}$$

すなわち

$$x^{2i}\equiv a(ka+2b)x+(b+a)(b-a)\quad\cdots①$$

$$x^{i+1}\equiv(ka+b)x-a\quad\cdots②$$

①，②において積の計算は和や差の計算に比べて遅いが，積は①では 3 回，②では 1 回使われている。後に，積の回数を減らした高速な方法を示す。

ここで，n を任意の自然数とするとき，n を 2 進法で表す。

$$n=(\cdots(((b_0\cdot2+b_1)\cdot2+b_2)\cdot2+b_3)\cdot2+\cdots)\cdot2+b_\ell\quad\cdots③$$

ただし，b_i は 0 か 1 の値をとり，$b_0=1$ である。

x^n を求めるには，n を③のように表し，①，②を繰り返し用いればよい。(バイナリー法)

このとき，係数は常に整数である。

ここで，①式の x に α,β を代入すると

$$\alpha^n=s\alpha+t,\quad \beta^n=s\beta+t$$

よって

$$\alpha^n+\beta^n=s(\alpha+\beta)+2t=ks+2t$$

$$\alpha^n\beta^n=(\alpha\beta)^n=1$$

したがって，α^n,β^n を 2 解に持つ 2 次方程式は

$$x^2-(ks+2t)x+1=0$$

である。

$$k_n=ks+2t$$

とおくと

$$x^2-k_nx+1=0$$

このとき，k_n は整数である。

ここで

$$\alpha^m\beta^m=(\alpha\beta)^m=1,\quad \alpha^n\beta^n=(\alpha\beta)^n=1$$
$$\alpha^{mn}+\beta^{mn}=(\alpha^m)^n+(\beta^m)^n=(\alpha^n)^m+(\beta^n)^m$$

であるから，$k_{mn}=\alpha^{mn}+\beta^{mn}$ は，$k_m=\alpha^m+\beta^m$ からでも $k_n=\alpha^n+\beta^n$ からでも上記の方法で求まることが分かる。

次に，p，q を相異なる素数とし，N＝pq とする。ただし，N の因数分解が現実的な時間ではできないくらいに p，q は巨大な素数であるとする。s，t を求める計算の途中には整数しか現れないので，N を法とする剰余類で考えても結論は成り立つ。

ただし，2 次方程式 $x^2-kx+1=0$ の判別式 D について，$D=k^2-4\neq 0$ とする。

安全性の根拠

$\alpha^n=s\alpha+t$，$\beta^n=s\beta+t$ より

$$(\alpha\beta)^n=\alpha^n\beta^n$$
$$=(s\alpha+t)(s\beta+t)$$
$$=s^2\alpha\beta+st(\alpha+\beta)+t^2$$

$\alpha+\beta=k,\alpha\beta=1$ であるから

$$1=s^2+kst+t^2$$

両辺を 4 倍して

$$4=4s^2+2ks(2t)+(2t)^2\quad \cdots①$$

また　$k_n=ks+2t$ より

$$2t=k_n-ks\quad \cdots②$$

②を①に代入して

$$4=4s^2+2ks(k_n-ks)+(k_n-ks)^2$$

整理して

$$4=(4-k^2)s^2+{k_n}^2$$

よって

$$(k^2-4)s^2={k_n}^2-4\quad \cdots③$$

k, k_n から s を求めるには，s についての 2 次方程式③を解かなければならない。
ここで，N を法とする剰余類で考えると，この方程式は N の因数分解を知らなければ解くことができない。s, t の値が求まらなければ，有限体上の離散対数問題の解法が使えないので，総当たり攻撃に近い方法でしか n の値は求まらない。よって，この暗号は安全である。

また，素数を法とする剰余類では，③は解けて s が求まり，s と②から t が求まるから，Chebyshev 多項式による ElGamal 暗号型の公開鍵暗号を解読するには，2 次方程式 $x^2 - kx + 1 = 0$ による拡大体上の ElGamal 暗号を解読すればよい。この暗号は，有限体上の ElGamal 暗号に比べて速度的に不利であるから，素数を法とする剰余類上には，この暗号を構築してはならない。

なお，N が素数とすると③から，$k^2 - 4 \neq 0$ かつ $k_n{}^2 - 4 \neq 0$ のとき，$k^2 - 4$ と $k_n{}^2 - 4$ の平方剰余，平方非剰余は一致することが分かる。これは，後に用いる重要な定理である。

指数法則に対応する恒等式

指数法則 $a^m a^n = a^{m+n}$ に対応する，次の恒等式を証明する。
任意の整数 m，n について

$$k_m k_n k_{m+n} - k_m{}^2 - k_n{}^2 - k_{m+n}{}^2 + 4 = 0$$

証明

$k_n = \alpha^n + \alpha^{-n}$　であるから

$k_{-n} = k_n$　…①

また

$$k_n{}^2 = (\alpha^n + \alpha^{-n})^2 = \alpha^{2n} + \alpha^{-2n} + 2 = k_{2n} + 2$$

より　$k_{2n} = k_n{}^2 - 2$　…②

また

$$k_m k_n = (\alpha^m + \alpha^{-m})(\alpha^n + \alpha^{-n}) = \alpha^{m+n} + \alpha^{-(m+n)} + \alpha^{m-n} + \alpha^{-(m-n)} = k_{m+n} + k_{m-n}$$

より　$k_m k_n = k_{m+n} + k_{m-n}$　…③
③の両辺に k_{m+n} を掛けて，①，②，③を用いると

$$k_m k_n k_{m+n} = k_{m+n}{}^2 + k_{m-n} k_{m+n}$$

$$= k_{m+n}{}^2 + k_{(m-n)+(m+n)} + k_{(m-n)-(m+n)}$$

$$= k_{m+n}{}^2 + k_{2m} + k_{2n}$$

$$= k_{m+n}{}^2 + k_m{}^2 + k_n{}^2 - 4$$

より成り立つ。

証明終り

この恒等式は，k_m, k_n が与えられたとき k_{m+n} に関する 2 次方程式となる。しかし，N の因数分解を知らない攻撃者は，その 2 次方程式を解くことはできないから，k_{m+n} を求めることはできない。

なお，この恒等式は，三角関数では次の公式に対応する。

$$2\cos\alpha\cos\beta\cos(\alpha+\beta)-\cos^2\alpha-\cos^2\beta-\cos^2(\alpha+\beta)+1=0$$

この三角関数の公式をデジタル署名に使う方法は，石井雅治氏の論文[1]より得た。

周期に関する考察

N＝pq を法とする剰余類で考える。

$x^2-kx+1=0$ より

$$\alpha^2-k\alpha+1=0 \quad \cdots①, \quad \beta^2-k\beta+1=0 \quad \cdots②$$

①×α^n ＋②×β^n より

$$(\alpha^{n+2}+\beta^{n+2})-k(\alpha^{n+1}+\beta^{n+1})+(\alpha^n+\beta^n)=0$$

よって

$$k_{n+2}-k\cdot k_{n+1}+k_n=0$$

また

$$k_0=\alpha^0+\beta^0=2, \quad k_1=\alpha+\beta=k$$

したがって，数列$\{k_n\}$は

$$k_0=2, \quad k_1=k$$

$$k_{n+2}=k\cdot k_{n+1}-k_n \quad (\text{n=0, 1, 2, 3, ……}) \quad \cdots③$$

によって定義されると考えてよい。（n は負の値を考えてもよい。）

③より，(k_i, k_{i+1}) の組が決まると (k_{i+1}, k_{i+2}) の組がただ 1 通りに決まるし，逆に，(k_{i+1}, k_{i+2}) の組が決まると (k_i, k_{i+1}) の組がただ 1 通りに決まる。

これと，(k_i, k_{i+1}) の組が有限個しかないことから，(k_i, k_{i+1}) (i=0, 1, 2, 3, ……)は周期性を持つ。

これより，k_i (i=0, 1, 2, 3, ……)も周期性を持つ。ただし，k_i から k_{i+1} は 1 通りには決まらない。

なぜなら，任意の自然数 i について

$$k_1k_ik_{i+1}-k_1^{\,2}-k_i^{\,2}-k_{i+1}^{\,2}+4=0$$

が成り立つ。これを k_{i+1} についての 2 次方程式とみなすと，p，q を法とする剰余類についてそれぞれ解は最大で 2 個あるから，N＝pq を法とする剰余類では，最大で $2\times2=4$ 個あるからである。

なお，N の因数分解を知らない攻撃者に k_i だけが与えられたとき，攻撃者はこの 2 次方程式が解けず，k_{i+1} を求められないから，漸化式③を用いることはできない。

次に，(k_i, k_{i+1}) の組の周期について調べる。

x^n を x^2-kx+1 で割った商を $Q(x)$，余りを $sx+t$ とすると

$$x^n=(x^2-kx+1)Q(x)+sx+t$$

ここで，s，t は整数である。

k を p で割った余りを a とする。

(ｉ)　2次式 x^2-ax+1 が p を法とする剰余類上で既約多項式であるとき

2 次方程式 $x^2-ax+1=0$ に解の公式を用いると，　$x=\dfrac{a\pm\sqrt{a^2-4}}{2}$　となるから，a^2-4が平方非剰余のとき，したがって，オイラーの基準により

$$\left(\frac{a^2-4}{p}\right)\equiv(a^2-4)^{\frac{p-1}{2}}\equiv-1 \pmod{p}$$

であるとき，x^2-ax+1は既約多項式となる。x^2-ax+1による拡大体上における，2 次方程式 $x^2-ax+1=0$ の解の 1 つをα とすると，もう一つの解は$\dfrac{1}{\alpha}$ である。

このとき，$x^2-ax+1=0$ の解の 1 つは，$\alpha=\dfrac{a+\sqrt{a^2-4}}{2}$ であるから，$D=a^2-4$とおくと

$$\alpha=\frac{a+\sqrt{D}}{2},\quad \frac{1}{\alpha}=\frac{a-\sqrt{D}}{2}$$

これより

$$\alpha^p=\frac{\left(a+\sqrt{D}\right)^p}{2^p}$$

右辺において，フェルマーの小定理により，$2^p\equiv2$ である。また，二項定理により

$$\left(a+\sqrt{D}\right)^p=\sum_{i=0}^{p}{}_pC_i\,a^{p-i}\left(\sqrt{D}\right)^i=a^p+\left(\sqrt{D}\right)^p+\sum_{i=1}^{p-1}{}_pC_i a^{p-i}\left(\sqrt{D}\right)^i$$

であるが，$1\leqq i\leqq p-1$のとき，$_pC_i=\dfrac{p!}{i!\,(p-i)!}$　は p の倍数であるから$_pC_i\equiv0$ である。よって

$$\left(a+\sqrt{D}\right)^p\equiv a^p+\left(\sqrt{D}\right)^p$$

右辺において，フェルマーの小定理により，$a^p\equiv a$

また，Dは$GF(p)$上で平方非剰余であるから，オイラーの基準により$D^{\frac{p-1}{2}}\equiv-1$である。よって

$$\left(\sqrt{D}\right)^p=D^{\frac{p}{2}}=D^{\frac{p-1}{2}}\sqrt{D}\equiv-\sqrt{D}$$

したがって

$$\left(a+\sqrt{D}\right)^p\equiv a-\sqrt{D}$$

ゆえに

$$\alpha^p\equiv\frac{a-\sqrt{D}}{2}=\frac{1}{\alpha}$$

これより$\alpha^{p+1}\equiv1$が成り立つ。

x^{p+1}をx^2-ax+1で割った商を$Q(x)$，余りを$sx+t$とすると

$$\alpha^{p+1}=(\alpha^2-a\alpha+1)Q(\alpha)+s\alpha+t\quad より\quad s\alpha+t\equiv1\quad \cdots①$$

さらに，$\alpha^{p+1}\equiv 1$より$\alpha^{-(p+1)}\equiv 1$も成り立つから，$\beta=\frac{1}{\alpha}$と置くと$\beta^{p+1}\equiv 1$である。よって

$$s\beta+t\equiv 1 \quad \cdots②$$

$\alpha\neq\beta$の場合だけを考えるから，①，②より

$$s\equiv 0, t\equiv 1$$

したがって

$$x^{p+1}\equiv 1 \mod x^2-ax+1$$

ゆえに，$p+1$は周期である。

周期が$p+1$である証明の考え方は，石井雅治氏の論文[2]より得た。

(ⅱ) 2次式 x^2-ax+1 がpを法とする剰余類上で既約多項式でないとき

オイラーの基準により，$(a^2-4)^{\frac{p-1}{2}}\equiv 1$ のときである。

このとき，2次方程式$x^2-ax+1=0$は$GF(p)$上に2解α,α^{-1}を持つ。

フェルマーの小定理により，$\alpha^{p-1}\equiv 1$，$\alpha^{-(p-1)}\equiv 1$が成り立つから，$p-1$は周期である。

qを法とする剰余類上で，kをqで割った余りをbとし，x^2-bx+1を考えても同様である。

安全な公開鍵の作成

x^2-ax+1，x^2-bx+1がそれぞれp，qを法とする剰余類上で既約多項式になるか，ならないかの組み合わせは4つある。よって，a,bから中国人剰余定理によりkを求め，x^2-kx+1を得る。

$p\pm 1$，$q\pm 1$は共に2の倍数であるから，$p\pm 1$，$q\pm 1$の最小公倍数は$\frac{(p\pm 1)(q\pm 1)}{2}$の約数である。

よって，kは以下のいずれかの類に属する。

$$x^{(p-1)(q-1)/2}\equiv 1,\ x^{(p+1)(q-1)/2}\equiv 1,\ x^{(p-1)(q+1)/2}\equiv 1,\ x^{(p+1)(q+1)/2}\equiv 1 \mod x^2-kx+1$$

(a) kが$x^{(p-1)(q-1)/2}\equiv 1$に属するようにする場合（x^2-ax+1，x^2-bx+1は共に既約多項式でない）

このとき，素数p，qは，素数p_1,q_1 $(p_1\neq q_1)$に対して

$$p=2p_1+1, q=2q_1+1$$

の形（p，qは安全素数）をとるように選ぶ。すると，

$$p-1=2p_1, q-1=2q_1$$

である。さらに

$$(a^2-4)^{\frac{p-1}{2}}\equiv 1 \pmod{p} \quad \text{かつ} \quad (b^2-4)^{\frac{q-1}{2}}\equiv 1 \pmod{q}$$

が成り立つようにa,bを選ぶと

$$x^{2p_1}\equiv 1 \mod x^2-ax+1 \quad \text{かつ} \quad x^{2q_1}\equiv 1 \mod x^2-bx+1 \quad (x^2\equiv 1 \text{ ではないとする})$$

よって，中国人剰余定理によりkを求めると

$$x^{2p_1q_1}\equiv 1 \mod x^2-kx+1$$

p_1,q_1は素数であるから，N＝pqについての剰余類上での基本周期はp_1q_1以上となる。

さらに，a^2-4 と ${a_n}^2-4$ および b^2-4 と ${b_n}^2-4$ が平方剰余・非剰余であるかは一致するから，k_n も $x^{(p-1)(q-1)/2}\equiv 1$ を満たす類に属し，x^2-k_nx+1 による基本周期も p_1q_1 以上となる。

(b) k が $x^{(p+1)(q-1)/2}\equiv 1$ に属するようにする場合（x^2-ax+1 が既約，x^2-bx+1 が既約でない）
このとき，素数 p，q は，素数 p_1, q_1 $(p_1\neq q_1)$ に対して

$$p=2p_1-1, q=2q_1+1$$

の形をとるように選び，さらに

$$(a^2-4)^{\frac{p-1}{2}}\equiv -1 \pmod{p} \quad \text{かつ} \quad (b^2-4)^{\frac{q-1}{2}}\equiv 1 \pmod{q}$$

が成り立つように a, b を選ぶ。このとき，中国人剰余定理により k を求めると，

$$x^{2p_1q_1}\equiv 1 \mod x^2-kx+1$$

N＝pq についての剰余類上での基本周期は p_1q_1 以上となる。

k が $x^{(p-1)(q+1)/2}\equiv 1$ や $x^{(p+1)(q+1)/2}\equiv 1$ に属するようにする場合も，同様に行う。

(s_i, t_i) の組と (k_i, k_{i+1}) の組の関係

x^i を x^2-kx+1 で割った余りを s_ix+t_i とすると，

$$k_i=\alpha^i+\beta^i=s_i(\alpha+\beta)+2t_i$$

より

$$k_i=ks_i+2t_i \qquad \cdots④$$
$$k_{i+1}=ks_{i+1}+2t_{i+1} \qquad \cdots⑤$$

また

$$x^i\equiv s_ix+t_i \mod x^2-kx+1$$

であるから

$$x^{i+1}\equiv x(s_ix+t_i)\equiv s_ix^2+t_ix\equiv s_i(kx-1)+t_ix\equiv (ks_i+t_i)x-s_i$$

よって

$$s_{i+1}=ks_i+t_i,\quad t_{i+1}=-s_i \qquad \cdots⑥$$

⑤に⑥に代入して

$$k_{i+1}=(k^2-2)s_i+kt_i \qquad \cdots⑦$$

④，⑦より

$$\begin{pmatrix} k_i \\ k_{i+1}\end{pmatrix}=\begin{pmatrix} k & 2 \\ k^2-2 & k\end{pmatrix}\begin{pmatrix} s_i \\ t_i\end{pmatrix}$$

ここで，$k^2 \neq 4$ であるから，$\Delta = k^2 - 2(k^2-2) = 4 - k^2 \neq 0$ である。

よって，$\begin{pmatrix} k & 2 \\ k^2-2 & k \end{pmatrix}$ に逆行列が存在し，(s_i, t_i) の数の組と (k_i, k_{i+1}) の数の組は 1 対 1 に対応する。

したがって，(k_i, k_{i+1}) の周期は (s_i, t_i) の周期と一致する。

ところで，与えられた k_i の値に対して k_{i+1} の値は最大で 4 個しかないから，異なる k_i の値は最小でも $\left\lceil \dfrac{\text{基本周期}}{4} \right\rceil$ 個ある。

安全性の証明（離散対数問題と素因数分解の関係）

この暗号は，多くの公開鍵において，離散対数問題の解が求まればNを素因数分解できる。したがって，その対偶をとれば，

Nの素因数分解ができない ⇒ 離散対数問題の解が求まらない

となる。これは，ラビン暗号や EPOC 暗号と同じように，この暗号が強固であることの根拠となる。

次に，そのことを示す。

恒等式

$$k_1 k_i k_{i+1} - k_1{}^2 - k_i{}^2 - k_{i+1}{}^2 + 4 = 0 \qquad \mod N$$

において　$k_1 = k$，$k_i = x$，$k_{i+1} = k_m$　とおくと

$$x^2 - k k_m x + k^2 + k_m{}^2 - 4 = 0 \qquad \mod N \quad \cdots①$$

また，　$k_1 = k$，$k_i = k_m$，$k_{i+1} = x$　とおいても，①が得られる。

よって，$x = k_{m-1}, k_{m+1}$ は，方程式①の解である。

方程式①には，さらに 2 つの解がある場合が多く，それらの解を　$x = k_{m'-1}, k_{m'+1}$ とする。

このとき，$k_{m'} = k_m$ である。

$\alpha = k_{m-1}, \beta = k_{m'-1}$ とすると，①より

$$\alpha^2 - k \cdot k_m \alpha + k^2 + k_m{}^2 - 4 = 0 \quad \cdots②$$

$$\beta^2 - k \cdot k_m \beta + k^2 + k_m{}^2 - 4 = 0 \quad \cdots③$$

②－③より

$$\alpha^2 - \beta^2 - k \cdot k_m (\alpha - \beta) = 0 \quad \mod N$$

$$(\alpha + \beta - k \cdot k_m)(\alpha - \beta) = 0 \quad \mod N$$

ところで，漸化式　$k_{n+2} = k \cdot k_{n+1} - k_n$　より

$$k_{m+1} = k \cdot k_m - k_{m-1}$$

よって

$$k_{m+1} + k_{m-1} - k \cdot k_m = 0 \qquad \mod N$$

$$k_{m'+1} + k_{m'-1} - k \cdot k_m = 0 \qquad \mod N$$

であるが，$\alpha = k_{m-1}, \beta = k_{m'-1}$ と，m と m'を用いているため

$\alpha+\beta-k\cdot k_m \neq 0 \mod N$

よって　$\alpha+\beta-k\cdot k_m$ と $\beta-\alpha$ はNの素因数を持つ。

したがって，離散対数問題が解けて m, m' が得られれば，$\alpha=k_{m-1}, \beta=k_{m'-1}$ が求まり，$\alpha+\beta-k\cdot k_m$ または $\beta-\alpha$ とNにユークリッドの互除法を用いて，Nの素因数が求まる。

２次式 x^2-ax+1，x^2-bx+1 による $\{a_i\},\{b_i\}$ の周期をそれぞれ，S，T とし，２次式 x^2-kx+1 による公開鍵を k_m とする。このとき，$2m$ が S, T の最大公約数の倍数であることが，離散対数問題が解ければN＝pq の素因数が求まる条件である。証明は補足 1 に記した。

以下は十進 BASIC のプログラムとその出力結果で，$p_1=\frac{p+1}{2}=4111, q_1=\frac{q+1}{2}=4507$ は共に素数である。このとき，必ず N の素因数が求まる。実際に，素因数 8221 と 9013 が求まっている。また，基本周期は p_1q_1 または $2p_1q_1$ となる。

```
DIM s(5)
LET p=8221
LET q=9013
LET n=p*q
FOR k=3 TO 20
    LET t=mod(k*k-4,p)
    LET a=1
    FOR j=1 TO (p-1)/2
        LET a=MOD(a*t,p)
    NEXT J
    IF a=p-1 THEN
        LET t=mod(k*k-4,q)
        LET a=1
        FOR j=1 TO (q-1)/2
            LET a=MOD(a*t,q)
        NEXT J
        IF a=q-1 THEN
            LET k0=2
            LET k1=k
            FOR j=2 TO   777
                LET x=MOD(k*k1-k0,n)
                LET k0=k1
                LET k1=x
            NEXT j
            LET key=k1
            LET kaisuu=0
            LET k0=2
```

```
            LET k1=k
            LET i=1
            DO
                IF k1=key THEN
                    LET kaisuu=kaisuu+1
                    LET s(kaisuu)=k0
                    PRINT USING "#### ######## ## ######## ######## ######## ########":
k,key,kaisuu,i,k0,k1,MOD(k*k1-k0,n);
                    LET sa=mod(s(kaisuu)-s(1),n)
                    LET a=n
                    LET b=sa
                    IF b<>0 THEN
                        LET r=mod(n,sa)
                        DO WHILE r>0
                            LET a=b
                            LET b=r
                            LET r=mod(a,b)
                        loop
                        IF b>1 THEN
                            PRINT USING "#######  ########  ######":b,sa,"  yes"
                        ELSE
                            PRINT USING "#######  ########  ######":b,sa,"  no"
                        END IF
                    ELSE
                        PRINT USING "#######  ########  ######":b,sa,"  no"
                    END IF
                    IF kaisuu=5 THEN Exit do
                end if
                LET x=MOD(k*k1-k0,n)
                LET k0=k1
                LET k1=x
                LET i=i+1
            loop
        END IF
    end if
NEXT k
END
    6  57608139    1         777  25672865  57608139  23592477        0        0      no
    6  57608139    2     9842511  61113596  57608139  62247619     8221 35440731     yes
    6  57608139    3    27214043  62247619  57608139  61113596     9013 36574754     yes
```

6	57608139	4	37055777	23592477	57608139	25672865	1	72015485	no
6	57608139	5	37057331	25672865	57608139	23592477	0	0	no
10	57193884	1	777	13739091	57193884	39528638	0	0	no
10	57193884	2	8685766	49106103	57193884	4161626	9013	35367012	yes
10	57193884	3	9842511	4161626	57193884	49106103	8221	64518408	yes
10	57193884	4	18527500	39528638	57193884	13739091	1	25789547	no
10	57193884	5	18529054	13739091	57193884	39528638	0	0	no
12	1300225	1	777	48511030	1300225	41187543	0	0	no
12	1300225	2	9842511	37429122	1300225	52269451	8221	63013965	yes
12	1300225	3	27214043	52269451	1300225	37429122	9013	3758421	yes
12	1300225	4	37055777	41187543	1300225	48511030	1	66772386	no
12	1300225	5	37057331	48511030	1300225	41187543	0	0	no
17	14235838	1	777	33321405	14235838	60496095	0	0	no
17	14235838	2	9842511	42578251	14235838	51239249	8221	9256846	yes
17	14235838	3	27214043	51239249	14235838	42578251	9013	17917844	yes
17	14235838	4	37055777	60496095	14235838	33321405	1	27174690	no
17	14235838	5	37057331	33321405	14235838	60496095	0	0	no

高速計算法

k_n を求めるには，前記の x^n を $x^2 - kx + 1$ で割った余り $sx + t$ を用いる方法より，さらに高速な方法が存在する。

$\alpha + \beta = k$ ， $\alpha\beta = 1$ ， $k_n = \alpha^n + \beta^n$ であるから

$$k_0 = 2 , k_1 = k$$

である。

(k_i, k_{i+1}) の組が与えられたとき， $k_{2i}, k_{2i+1}, k_{2i+2}$ は次のように求められる。

$$k_{2i} = \alpha^{2i} + \beta^{2i} = (\alpha^i + \beta^i)^2 - 2(\alpha\beta)^i = {k_i}^2 - 2$$

また，これより

$$k_{2i+2} = k_{2(i+1)} = {k_{i+1}}^2 - 2$$

も成り立つ。また，

$$k_i k_{i+1} = (\alpha^i + \beta^i)(\alpha^{i+1} + \beta^{i+1}) = (\alpha^{2i+1} + \beta^{2i+1}) + (\alpha\beta)^i(\alpha + \beta) = k_{2i+1} + k$$

よって

$$k_{2i+1} = k_i k_{i+1} - k$$

したがって， (k_i, k_{i+1}) の組が与えられれば

$$(k_{2i}, k_{2i+1}) = (k_i{}^2 - 2, k_i k_{i+1} - k) \qquad \cdots①$$

$$(k_{2i+1}, k_{2i+2}) = (k_i k_{i+1} - k, k_{i+1}{}^2 - 2) \quad \cdots②$$

が求まる。ここで

$$n = (\cdots(((0\cdot 2 + b_0)\cdot 2 + b_1)\cdot 2 + b_2)\cdot 2 + b_3)\cdot 2 + \cdots)\cdot 2 + b_\ell \quad \cdots③$$

b_i は 0 か 1 の値をとり，$b_0 = 1$

と表し，$(k_0, k_1) = (2, k)$ もしくは $(k_1, k_2) = (k, k^2 - 2)$ を初期値として，③の括弧の内側から，b_i が 0 ならば①を，b_i が 1 ならば②を繰り返し用いると，(k_n, k_{n+1}) を高速に求めることができる。

①，②では，積はそれぞれ，たった 2 回しか使われていない。

また，b_i が 0 でも 1 でも計算量が同じため，冪乗演算に対する電力解析攻撃ができない。

なお，①，②は三角関数の恒等式

$$\cos(2n\theta) = 2\cos^2(n\theta) - 1,\ \cos((2n+1)\theta) = 2\cos((n+1)\theta)\cos(n\theta) - \cos\theta$$

から求めることもできる。

次に，具体的な暗号化について考える。

公開鍵暗号

受信者の初期設定

・相異なる 2 つの素数 p，q を生成し，積 N＝pq を求める。（N は，RSA 暗号と同じく 2048bit 程度）
以下，mod N で考える。

・自然数 k を決める。（p，q を安全素数として，k を固定することもできる。補足 2 参照）

・128bit 程度の自然数の乱数 m を生成する。（共通鍵暗号と同じ bit 数）

・k_m を計算する。（k_m のとり得る値の個数は，最小でも $\frac{2^{128}}{4} = 2^{126}$ 個ほどある。）

・N, k, k_m を送信者の公開鍵とする。p, q, m が送信者の秘密鍵である。

送信者の作業

・128bit 程度の自然数の乱数 n を生成する

・k_n を計算する。

・k_m と n から k_{mn} を計算する。

・k_{mn} より共通鍵を作成し，共通鍵暗号でメッセージ M を暗号化して M' を得る。

・(k_n, M') を暗号文として受信者に送信する。

復号処理

・k_n と m から k_{nm} を計算する。（$k_{nm} = k_{mn}$）

・k_{nm} より共通鍵を作成し，M' を復号して M を得る。

ただし，受信者は N の因数 p，q を知っているため，p を法とする剰余類と q を法とする剰余類で，k_{nm} を別々に求め，2 つの k_{nm} を中国人剰余定理により 1 つに結合すると，処理が高速になる。さらに，

次の「ElGamal 暗号の復号の高速化法」を用いれば，公開鍵はさらに安全で高速になる。

ElGamal 暗号の復号の高速化法

冪乗の指数を 128bit 程度に小さくするのは抵抗があるかもしれません。そこで，ElGamal 暗号の復号処理を高速化する，次のような方法を考えました。

鍵作成

・素数 p，q を秘密鍵として $N=pq$ を計算する。

（このとき，通常は N と同じ程度の bit 数の乱数 m を秘密鍵として，公開鍵を N，a，$a^m = a \bmod N$ とするが，これを次のように変える。）

・$a_p = a \bmod p$，$a_q = a \bmod q$ とする。そして，小さな自然数 $m_p, m_q\ (m_p \neq m_q)$ を秘密鍵として，

$b_p = a_p{}^{m_p} \bmod p$ と $b_q = a_q{}^{m_q} \bmod q$ を計算する。

・中国人剰余定理により，$b \bmod p = b_p$ かつ $b \bmod q = b_q$ を満たす b を求め，N，a，b を公開鍵とする。

（$a^m \bmod N = b$ を満たす自然数 m が存在するのは，$a^i \bmod p, a^i \bmod q$ の基本周期をそれぞれ，S，T とするとき，$m_q - m_p$ が S，T の最大公約数の倍数であるときである。存在するときは N と同じ bit 数程度の大きな自然数になる。補足 3 を参照）

暗号処理

・自然数の乱数 n を生成する。

・$c = a^n \bmod N$ と $d = b^n \bmod N$ を計算する。

・d から共通鍵を作成し，共通鍵暗号でメッセージ M を暗号化して M' を得る。

・c，M' を受信者に送信する。

復号処理

・$c_p = c \bmod p$ と $c_q = c \bmod q$ を計算し，さらに，$x_p = c_p{}^{m_p} \bmod p$ と $x_q = c_q{}^{m_q} \bmod q$ を計算する。

・中国人剰余定理により，$x \bmod p = x_p$ かつ $x \bmod q = x_q$ を満たす x を求める。このとき，$x=d$ が成り立つ。

・x から共通鍵を作成し，共通鍵暗号でメッセージ M' を復号して M を得る。

m_p, m_q を極小さくとることができれば，復号が極端に速くなる。例えば，S，T が共に偶数となるような p, q, a を選び，$m_q - m_p$ が奇数となる m_q, m_p を選べば，$a^m \bmod N = b$ となる m は存在しない。

このとき，$m_p = 2, m_q = 3$ 程度に小さく選んでもよいように思われる。

この復号の高速化法は，チェビシェフ多項式型公開鍵暗号にも適用できる。以下に，十進 BASIC のコードと出力結果を示す。

```
!Chebyshev 多項式暗号
LET p=8747 !安全素数
LET q=5939
LET a=27246964 !公開鍵
LET a1=MOD(a,p)
LET a2=MOD(a,q)
LET m1=2 !秘密の乱数
LET m2=3

LET b1=Chebyshev(a1,m1,p)
LET b2=Chebyshev(a2,m2,q)
LET b=Chinese(b1,b2,p,q) !公開鍵を作成

LET m=Chinese(m1,m2,p-1,q-1) !周期から指数を求める。これで求まらない場合もある。
PRINT m
PRINT Chebyshev(a,m,p*q),b !一致するかを確認

LET s=2
LET t=a
LET N=p*q
LET flag=0
FOR i=2 TO N
    LET x=MOD(a*t-s,N)
    LET s=t
    LET t=x
    IF t=b THEN
        LET flag=1
        PRINT i,b,t,"あった"
    END if
NEXT I
IF flag=0 THEN PRINT "なかった"

LET n=123456 !秘密の乱数
LET c=Chebyshev(a,n,p*q)
LET d=Chebyshev(b,n,p*q)

LET x1=Chebyshev(MOD(c,p),m1,p)
```

```
LET x2=Chebyshev(MOD(c,q),m2,q)
LET x=Chinese(x1,x2,p,q)

PRINT d,x !一致を確認

END

EXTERNAL FUNCTION Chebyshev(k,r,N) !漸化式の第 r 項の計算
LET s=2
LET t=k
FOR i=2 TO r
    LET x=MOD(k*t-s,N)
    LET s=t
    LET t=x
NEXT I
LET Chebyshev=t
END function

EXTERNAL FUNCTION Chinese(a1,a2,p,q) !中国人剰余定理
CALL ExGCD(p,q,s,t,c)
LET x=a1*t*q+a2*s*p
LET Chinese=MOD(x/c,p*q/c)
End function

EXTERNAL SUB ExGCD(a,b,s,t,c) !拡張ユークリッドの互除法（再帰版）
IF b=0 THEN
    LET s=1
    LET t=0
    LET c=a
ELSE
    LET q=INT(a/b)
    LET r=MOD(a,b)
    CALL ExGCD(b,r,s1,t1,c)
    LET s=t1
    LET t=s1-t1*q
END IF
END SUB

 20483134
 24949923                    6152620
```

なかった

7505467　　7505467

デジタル署名

注意　「復号の高速化法」を用いた公開鍵とは，相性が悪い。

デジタル署名 1（N の素因数分解を知らないと 2 次方程式が解けないことを利用した。高速である。）

(1) 鍵ペア

N, k, k_m を送信者の公開鍵とする。 p, q, m が送信者の秘密鍵である。

(2) 署名

送信者は，文書 M に対して，文書 M のハッシュ値 e＝h(M)を求め，さらに $\sigma = k_{m+e}$ を求める。

σ が M の署名である。（安全のため，文書 M にはパディングをする。）

ここで，

$$k_m k_e k_{m+e} - k_m{}^2 - k_e{}^2 - k_{m+e}{}^2 + 4 = 0$$

であるから

$$k_m k_e \sigma - k_m{}^2 - k_e{}^2 - \sigma^2 + 4 = 0 \quad \cdots①$$

が成り立つ。

①は σ についての 2 次方程式となるが，送信者以外は，N の因数分解を知らないため，①から σ を求めることはできない。

送信者は，受信者に文書 M とその署名 σ を送る。

(3) 検証

受信者は，M からハッシュ e=h(M)を求める。

次に， k, e から k_e を求める。

さらに，①の左辺を計算し，それが 0 になれば，署名は正当なものである。

デジタル署名 2（デジタル署名 1 より署名が長く，署名・検証が低速。Schnorr 署名から着想した。）

(1) 鍵ペア

N, k, k_m を送信者の公開鍵とする。 p, q, m が送信者の秘密鍵である。

(2) 署名

送信者は，文書 M に対して秘密の乱数 i を選び，次の γ，文書 M と γ を合わせた文書のハッシュ値 e を求め，さらに δ を求める。

$\gamma = k_i$

e=h(M, γ)

$\delta \equiv i + me$　（m についての情報を与えないため，i は me 以上の bit 長にする）

(γ, δ)が M の署名である。

ここで，

$$k_i k_{me} k_{i+me} - k_i{}^2 - k_{me}{}^2 - k_{i+me}{}^2 + 4 = 0$$

であるから

$$\gamma k_{me} k_\delta - \gamma^2 - {k_{me}}^2 - {k_\delta}^2 + 4 = 0 \quad \cdots①$$

が成り立つ。

送信者は，受信者に文書 M とその署名(γ， δ) を送る。

(3) 検証

受信者は， M, γ からハッシュ e=h(M, γ)を求める。

次に， k_m, e から k_{me} を， k, δ から k_δ を求める。

さらに，①の左辺を計算し，それが 0 になれば，署名は正当なものである。

処理速度

RSA 暗号は暗号化と署名検証が極端に速く，復号と署名生成が遅い。一方，この暗号は，中国人剰余定理を用いない場合，暗号化は復号の 2 倍の時間を要し，署名検証は署名生成と同じ時間を要する。したがって，RSA 暗号で処理が遅い復号と署名生成について速度比較をする。

この暗号で， k から k_n を求めるバイナリ－法の処理で

$$(k_{2i}, k_{2i+1}) = ({k_i}^2 - 2, k_i k_{i+1} - k)$$

において積を 2 回

$$(k_{2i+1}, k_{2i+2}) = (k_i k_{i+1} - k, {k_{i+1}}^2 - 2)$$

においても積を 2 回行う。

一方，RSA 暗号においては， x を掛ける計算は，2 乗の計算 1 回につき，確率$\frac{1}{2}$で起こるから0.5回必要であると考えてよい。よって，RSA 暗号においては，2 乗の計算と x を掛ける計算を合わせると，2 乗の計算 1 回につき，積の計算は 1.5 回である。

したがって，1 回の 2 乗の計算に付き，この暗号の計算量は RSA 暗号に対して$\frac{2}{1.5} = \frac{4}{3}$倍と考えらる。

RSA 暗号 2048bit において，2 乗 1 回に付き行う計算の量を 1 とする。

暗号化処理では，RSA 暗号は冪乗の指数の値は 3 か 65537 を使うため，計算量は極めて少ない。

一方，この暗号では，冪乗の指数を 112bit 程度の抑えるとして

$$\frac{4}{3} \times 112 \times 2 = \frac{896}{3} \approx 299$$

復号処理では，中国人剰余定理を用いる。 p, q を法とし，計算量は bit 数の 3 乗に比例する。

RSA 暗号では，冪乗計算の指数の桁数を$\frac{1}{2}$にすることができるから，計算量は

$$2048 \times \left(\frac{1}{2}\right)^3 \times 2 = 512$$

一方，この暗号では，「復号の高速化法」を用い，指数 m_p, m_q を極端に小さくとれば，計算量は極めて少ない。

暗号化と復号を合わせると，この暗号の方が高速であると言える。
さらに，3072bit の暗号では，RSA 暗号の復号の計算量は

$$512\times\left(\frac{3072}{2048}\right)^3=1728$$

である。この暗号では，暗号化の指数を 128bit とすると，計算量は

$$\frac{4}{3}\times128\times2\times\left(\frac{3072}{2048}\right)^2=768$$

であり，暗号化と復号の合計の計算量の差はさらに広がる。

また，デジタル署名 1 においては，ハッシュ関数を 224bit とすると，e は 224bit であり，$m+e$ も 224bit 程度と考えてよい。署名生成では，中国人剰余定理を使うとして，冪乗計算の積の回数は，RSA 署名に対して，

$$\frac{4}{3}\times\frac{224}{2048\times\frac{1}{2}}=\frac{7}{24}\approx0.292\text{ 倍}$$

であるから，署名生成は RSA 署名に対して 3.4 倍ほど高速である。
次に，2048bit の ElGamal 暗号の復号における冪乗の計算量を 1 として，冪乗の計算量の見積もりを示す。Chebyshev 多項式による ElGamal 暗号型が最速である。

暗号強度	法の bit 数	RSA 暗号		この暗号		ElGamal 暗号		RSA 署名		この署名	
		暗号化	復号	暗号化	復号	暗号化	復号	生成	検証	生成	検証
112bit	2048bit	僅少	0.25	0.15	僅少	2	1	0.25	僅少	0.073	0.15
128bit	3072bit	僅少	0.84	0.38	僅少	6.8	3.4	0.84	僅少	0.19	0.38
192bit	7680bit	僅少	13.2	3.5	僅少	105	53	13.2	僅少	1.8	3.5

ただし，RSA 暗号や署名では，法とする数より小さい数を掛けるため，計算量は上記より減少する。また，積の計算量は法の bit 数の 2 乗で見積もっているが，Karatsuba 法を用いれば計算量は減少する。その場合でも，同じ暗号強度で比べれば，各暗号の計算量の比は変わらない。

補足 1

p（素数）の同値類において，a^2-4 が平方剰余，非剰余となる a の個数を求める。

補題 1　a^2-4 は平方剰余 $\Leftrightarrow$ ある u が存在して $a=u+u^{-1}$,$u\neq\pm1$ とおける

証明　$\Rightarrow$　a^2-4 は平方剰余であるから，c を用いて

$$a^2-4=c^2$$

とおける。変形して

$$\frac{a+c}{2}\cdot\frac{a-c}{2}=1$$

よって，$\frac{a+c}{2}=u$ とおくと，$\frac{a-c}{2}=u^{-1}$ であるから，$a=u+u^{-1}$ となる。

ただし，$a^2-4\neq0$ より $a\neq\pm2$ であるから，$u\neq\pm1$

$\Leftarrow$　　$a=u+u^{-1}$ より

$$a^2-4=(u+u^{-1})^2-4=(u-u^{-1})^2$$

$u\neq\pm1$ より，$a^2-4\neq0$ であるから，a^2-4 は平方剰余である。

補題 2　$a=u+u^{-1}$，　$b=v+v^{-1}$ とするとき，「$a\neq b \Leftrightarrow u,u^{-1}$ と v,v^{-1} の組は異なる」

証明　$a=b$ とすると

$$u+u^{-1}=v+v^{-1}$$

両辺に u を掛けて，変形すると

$$u^2+1=(v+v^{-1})u$$

$$(u-v)(u-v^{-1})=0$$

したがって

$$u=v \text{ または } u=v^{-1}$$

$u=v$ のとき，$u^{-1}=v^{-1}$，$u=v^{-1}$ のとき，$u^{-1}=v$ であるから，u,u^{-1} と v,v^{-1} の組は一致する。

逆に u,u^{-1} と v,v^{-1} の組が一致するとき，$a=b$ は明らか。よって

$$a=b \Leftrightarrow u,u^{-1} \text{ と } v,v^{-1} \text{ の組は一致する}$$

対偶をとると，この補題となる。

a^2-4 が平方剰余，平方非剰余になる場合の，それぞれの a の個数を求める。

$u=u^{-1}$ とすると，$u^2=1$　よって　$u=\pm1$。逆も成り立つ。よって

$$u\neq\pm1 \Leftrightarrow u\neq u^{-1}$$

(1)　a^2-4 が平方剰余であるとき

u の考えられる p 個の元から，$u=0$，$u=\pm1$ を除くと，u の個数は $p-3$ 個

$u\neq u^{-1}$ であるから，u と u^{-1} の組は $\dfrac{p-3}{2}$ 個あり，$a=u+u^{-1}$ の個数も $\dfrac{p-3}{2}$ 個ある。

(2)　$a^2-4=0$ であるとき，$a=\pm2$ の 2 個ある。

(3)　a^2-4 が平方非剰余であるとき，a の個数は $p-\dfrac{p-3}{2}-2=\dfrac{p-1}{2}$ 個ある。

次に，(a_i,a_{i+1}) の数の組の個数について考える。

$$aa_ia_{i+1}-a^2-{a_i}^2-{a_{i+1}}^2+4=0$$

より a_{i+1} は 2 次方程式

$$x^2-aa_ix+a^2+{a_i}^2-4=0 \quad \cdots①$$

の解である。この方程式の判別式を D とすると

$$D=(aa_i)^2-4(a^2+{a_i}^2-4)=(aa_i)^2-4a^2-4{a_i}^2+16=(a^2-4)({a_i}^2-4)$$

$a^2-4\neq0$ であるから，①は，${a_i}^2-4\neq0$ のとき異なる 2 つの解を，${a_i}^2-4=0$ のとき重解を持つ。

$a_i^2-4\neq 0$ のとき，a_i^2-4 の平方剰余・非剰余は a^2-4 の平方剰余・非剰余と一致する。

まず，a^2-4 が平方剰余のときを考える。

(1) $a_i^2-4\neq 0$ のとき，

a_i^2-4 の平方剰余・非剰余は a^2-4 の平方剰余・非剰余と一致するから，(a_i, a_{i+1}) の数の組の個数は

$\dfrac{p-3}{2}\times 2=p-3$ 個である。

(2) $a_i^2-4=0$ のとき

①より，(a_i, a_{i+1}) の数の組は $(2, a)$，$(-2, -a)$ の 2 個である。

以上より，(a_i, a_{i+1}) の数の組の個数は $(p-3)+2=p-1$ 個である。

したがって，(a_i, a_{i+1}) の基本周期が $p-1$ であるとき，(a_i, a_{i+1}) の数の組はすべての場合をとる。

同様にして，a^2-4 が平方非剰余のとき，(a_i, a_{i+1}) の数の組の個数は $(p-1)+2=p+1$ 個であり，

(a_i, a_{i+1}) の基本周期が $p+1$ であるとき，(a_i, a_{i+1}) の数の組はすべての場合をとる。

離散対数問題が解けたとき，N＝pq の素因数が求まる条件

次に，２次式 x^2-ax+1，x^2-bx+1 による $\{a_i\}, \{b_i\}$ の基本周期をそれぞれ，S，T とし，２次式

x^2-kx+1 による公開鍵を k_m とする。

すると $a_0=2$，$a_S=2$，$b_0=2$，$b_T=2$　であり，任意の i について $a_{-i}=a_i$，$b_{-i}=b_i$ であるから，ℓ を整数として

$$a_m=a_{m+\ell S},\quad b_m=b_{m+\ell T},\quad a_m=a_{-m+\ell S},\quad b_m=b_{-m+\ell T}$$

が成り立つ。

$a_n=a_m$ かつ $b_n=b_m$ となる n の値を求める。x, y を整数として次の 4 つの場合がある。

$$\begin{cases} n=m+xS \\ n=m+yT \end{cases} \cdots①\qquad \begin{cases} n=-m+xS \\ n=m+yT \end{cases} \cdots②$$

$$\begin{cases} n=m+xS \\ n=-m+yT \end{cases} \cdots③\qquad \begin{cases} n=-m+xS \\ n=-m+yT \end{cases} \cdots④$$

①のとき，$k_{n-1}=k_{m-1}, k_n=k_m, k_{n+1}=k_{m+1}$ である。

④のとき，$k_{n-1}=k_{m+1}, k_n=k_m, k_{n+1}=k_{m-1}$ である。

②と③のときは，k_n の前後の値は k_{m-1}, k_{m+1} とは異なる。

②のとき

$$-m+xS=m+yT$$

変形して

$$Sx+T(-y)=2m\quad \cdots⑤$$

この不定方程式に解が存在するのは，$2m$ が S, T の最大公約数の倍数であるときである。

特に，$S = p \pm 1 = 2p_1$，$T = q \pm 1 = 2q_1$（p, q, p_1, q_1 は素数）のときを考える。このとき，方程式⑤は

$$p_1 x + q_1(-y) = m \quad \cdots⑥$$

となる。p_1, q_1 は素数であるから，p_1, q_1 の最大公約数は 1 である。よって，解は存在する。

③のときも同様にして

$$S(-x) + Ty = 2m$$

となり，この不定方程式に解が存在するのは，$2m$ が S, T の最大公約数の倍数であるときである。

特に，$S = p \pm 1 = 2p_1$，$T = q \pm 1 = 2q_1$ のときは

$$p_1(-x) + q_1 y = m$$

となり，同様にして，解は存在する。

$S = p \pm 1 = 2p_1$，$T = q \pm 1 = 2q_1$ のとき，$x^2 - kx + 1$ による $\{k_i\}$ は S, T の最小公倍数 $2p_1q_1$ が基本周期となり，$0 < i < 2p_1q_1$ の範囲に①～④の解は，それぞれ $k_m, k_n, k_{2p_1q_1-n}, k_{2p_1q_1-m}$ と 1 個ずつ存在する。

また，⑥より $x = mp_1^{-1} \pmod{q_1}$ であるから，$n = -m + 2p_1 \cdot (mp_1^{-1} \pmod{q_1})$ である。

よって，n が $2p_1q_1$ に比べて極めて小さな値となる確率は無視できるくらい小さい。

補足 2

安全素数とは，素数 p_1 を用いて $p = 2p_1 + 1$ と表される素数 p である。（p≧5）

7 より大きい安全素数を法とするとき，$a = 4$ とすると，$a^2 - 4$ は平方剰余であることを示す。

補題 1　5 以外の安全素数は 4 で割ると 3 余る。

証明　p_1 は奇素数だから，自然数 k を用いて $p_1 = 2k + 1$ と表される。よって $p = 4k + 3$

証明終り

補題 2　7 以外の安全素数は 3 で割ると 2 余る。

証明　p は素数であるから，3 の倍数でない。よって $p = 3k + 1$（k は自然数）と仮定すると

$$p = 3k + 1 = 2p_1 + 1 \quad \text{より} \quad 3k = 2p_1$$

これより p_1 は 3 の倍数となり，p_1 が 3 以外の素数であることに反する。

証明終り

補題 3　7 より大きい安全素数を法とするとき，3 は平方剰余である。

証明　3 と p は共に 4 で割ると 3 余るから，（補題 1）

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) \qquad \text{（平方剰余の相互法則）}$$

$$= -p^{\frac{3-1}{2}} \mod 3 \quad \text{（オイラーの基準）}$$

$$= -p \mod 3$$

$$= -2 \mod 3 \qquad \text{（補題 2）}$$

$$= 1$$

よって，3 は平方剰余である。

証明終り

$a=4$ のとき $a^2-4=12=2^2\cdot 3$ であり，3 は平方剰余であるから，a^2-4 は平方剰余である。

さらに，

$$a_0=2, a_1=4,\quad a_{n+2}=4a_{n+1}-a_n \quad (n=0,1,2,3,\cdots)$$

で定義される数列 $\{a_n\}$ の各項も，a_1 と平方剰余・非剰余が一致するから，この性質を満たす。

列挙すると，次のようである。

4 , 14 , 52 , 194 , 724 , 2702 , 10084 , 37634 , 140452 , 524174 , 1956244 , 7300802 , 27246964 , …

公開鍵 k として，これらの数列の奇数項を N＝pq（p，q は安全素数）で割った余りを用いればよい。

補足 3

$a^m \bmod N=b$ を満たす自然数 m を求めるには，$a^i \bmod p, a^i \bmod q$ の基本周期をそれぞれ，S，T とするとき，

$$m=m_p+xS=m_q+yT$$

を満たす最小の自然数 x, y を求めればよい。これより

$$xS-yT=m_q-m_p$$

となるから，m_q-m_p が S，T の最大公約数の倍数であるときは，解 x, y が存在する。このとき，

$m \bmod S=m_p$，$m \bmod T=m_q$ となる最小の自然数 m を中国人剰余定理の拡張により求めればよい。

定理　中国人剰余定理の拡張

自然数 m, n に対して，m, n の最大公約数を g，最小公倍数を l とおくとき，連立合同式

$$\begin{cases} x\equiv a \pmod m \\ x\equiv b \pmod n \end{cases} \quad \cdots①$$

が整数解を持つための必要十分条件は，$a\equiv b \pmod g$ である。また，この条件が成り立つとき，整数解 x は l を法として一意的に定まる。

証明

①が整数解を持つとすると，

$$x=a+sm=b+tn$$

となる整数 s, t が存在する。これより

$$sm-tn=b-a \quad \cdots②$$

よって，$b-a$ は g の倍数であるから，$a\equiv b \pmod g$

逆に，$a\equiv b \pmod g$ のとき②は整数解 s, t をもつから，$x=a+sm=b+tn$ とおけば①の解になる。

また，x, x' が共に①の整数解であるとすると，

$$x\equiv x' \pmod m \text{ かつ } x\equiv x' \pmod n$$

であるから　$m \mid x-x'$ かつ $n \mid x-x'$

したがって，$x-x'$ は m, n の公倍数である。よって $l \mid x-x'$ であるから $x\equiv x' \pmod l$

すなわち，x は l を法として一意的に定まる。

証明終り

次に，実際に①の解を求める。まず，拡張ユークリッドの互除法により

$$sm+tn=g \cdots ③$$

となる整数 s, t を求める。このとき

$$(b-a)sm/g+(b-a)tn/g=b-a$$

よって，

$$x=a+\{(b-a)/g\}sm=b+\{(a-b)/g\}tn$$

は①の解である。③を用いて変形すると

$$x=a(1-sm/g)+bsm/g=atn/g+bsm/g$$

これを l で割った余りを求めればよい。

参考文献

[1] 石井雅治, 2 冪剰余環上の Chebyshev 多項式の周期性と電子署名, 日本応用数理学会論文誌 Vol.18, No.2, (2008), 257-265

[2] 石井雅治, Chebyshev 多項式の不変集合を利用した公開鍵暗号, 日本応用数理学会論文誌 Vol.20, No.1, (2010), 45-56