1　RSA 暗号の原理

RSA 暗号は，公開鍵暗号系の一種である．

RSA 暗号の安全性は次の経験的な事実に基づいている：異なる 2 つの巨大な素数 p, q の積であるような自然数 N が与えられたとき，p, q をあらかじめ知らなければ，N から p, q を特定することは難しい．

以下，数値の暗号化，復号化，署名について説明している．それらを普通の文章に応用したい場合，例えば JIS コード表を用いて，文字を一つ一つ数値に直せばよい．

1.1　暗号化

m を与えられた自然数とする．いま，m を暗号化することを考える．自然数 N を

$$N = pq, \qquad p, q \text{ は素数}, \qquad m < N$$

を満たすようなものとする．

ϕ を Euler 関数とし，$\phi(N)$ と互いに素な 1 より大きい自然数を一つ選んでそれを e とする．ここで $\phi(N)$ は

$$\phi(N) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$$

なる関係式によって求めることができる．このとき

$$c \equiv m^e \pmod{N} \tag{1}$$

で定まる c が，m を暗号化したものである．

例 1.1.　$m = 59$ とする．例えば $N = 65$ とすると

$$N = 65 = 5 \times 13, \qquad m < N,$$
$$\phi(N) = \phi(65) = \phi(5)\phi(13) = 4 \times 12 = 48 = 2^4 \times 3$$

そこで $e = 5$ とすると

$$59^5 = 714924299 \equiv 24 \pmod{65}$$

よって $c = 24$ が $m = 59$ を暗号化したものである．

1.2　復号化

m, e, N を先に述べた通りとする．d を未知数とする一次合同式

$$ed \equiv 1 \pmod{\phi(N)}$$

を考える．e と $\phi(N)$ とは互いに素なので，この合同式は $\phi(N)$ を法としてただ一つの解 d を持つ．d として自然数のものをとる．ある自然数 k を用いて

$$ed = 1 + k\phi(N)$$

と書くことができる．(**??**) の両辺を d 乗すると

$$c^d \equiv m^{ed} \pmod{N}$$

ここで

$$m^{ed} = m^{1+k\phi(N)} = m \cdot (m^{\phi(N)})^k$$

を用いて

$$c^d \equiv m \cdot (m^{\phi(N)})^k \pmod{N}$$

を得る．さらに Euler の定理

$$a^{\phi(n)} \equiv 1 \pmod{n}, \qquad a,\, n \text{ は互いに素}$$

を右辺に用いれば

$$m \equiv c^d \pmod{N}$$

これにより m が得られる．

例 1.2. 例 **??** において m を暗号化してできた c を復号化しよう．$N = 65$, $e = 5$, $c = 24$ とする．$\phi(65) = 48$ だったから，一次合同式

$$5d \equiv 1 \pmod{48}$$

を解けばよい．一般解は

$$d \equiv 29 \pmod{48}$$

となる．そこで $d = 29$ とおいて

$$m \equiv 24^{29} \pmod{65}$$

を計算すればよい．計算すると

$$m \equiv 59 \pmod{65}$$

よって $m = 59$ が得られた．

N の桁数として 300 桁以上とったとき，N の素因子 p, q を知らないと，c を復号化して m を得ることは困難になる．すなわち，d を未知数とする一次合同式を解く際，$\phi(N)$ の値を計算するためには膨大な時間を必要とするのである．p, q を知っていれば

$$\phi(N) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$$

なる関係式を用いて $\phi(N)$ を容易に計算することができる．一方，p, q を知らないで $\phi(N)$ を求める効率的な方法は現時点では知られていない．

1.3 署名

m, e, N, d を先に述べた通りとする．

$$r \equiv m^d \pmod{N}$$

を満たす自然数 r を一つ選ぶ．この r が m に署名を施したものである．

両辺を e 乗すると，$ed \equiv 1 \pmod{N}$ だったので，ある自然数 k が存在して

$$r^e \equiv m^{de} = m \cdot (m^{\phi(N)})^k \pmod{N}$$

となる．よって Euler の定理から

$$m \equiv r^e \pmod{N}$$

こうして m が復元できる．

例 1.3. $m = 59$, $N = 65$, $e = 5$, $d = 29$ とする．このとき

$$r \equiv 59^{29} \equiv 24 \pmod{65}$$

よって $r = 24$ である．

$r = 24$ に $e = 5$ 乗すれば

$$m \equiv 24^5 \equiv 59 \pmod{65}$$

となり，$m = 59$ が復元できる．

r と m が与えられたとき，関係式 $r \equiv m^d \pmod{N}$ から d を特定することは一般には難しい．よって e, N を用いて m が得られるような r を作ることができるのは d を知る者のみ，ということになる．

1.4 秘密性と正当性

m, e, N, c, d, r を先に述べた通りとする．このとき m が**平文**，e, N の組 $\{e, N\}$ が**公開鍵**，c, r が**暗文**，d が**秘密鍵**である．

送信者を A, 受信者を B とする．送信する内容 m の秘密を守るには次のようにすればよい．いま，B は B 自身の公開鍵 $\{e_B, N_B\}$ を公開しているとする．A が B に平文 m を送るとき，B の公開鍵 $\{e_B, N_B\}$ を用いて m を暗号化して c_B を作り，c_B を B に送信する．B は暗文 c_B を受け取った後，B 自身の秘密鍵 d_B を用いて c_B から m を復元する．c_B を復号化できるのは B しかいないので，送信した内容 m の秘密は守られる．

$$A \Rightarrow m \xrightarrow[\text{暗号化}]{e_B, N_B} c_B \xrightarrow[\text{復号化}]{d_B} m \Rightarrow B$$

ところが，B の公開鍵 $\{e_B, N_B\}$ は公開されているので，A 以外の送信者 A' が暗文 c_B の代わりに別の平文 m' を $\{e_B, N_B\}$ を用いて暗号化した c'_B を B に送ることができる．したがって c_B が本当に B から送信されたという正当性が保証されない．例えば A' が A のフリをして間違った情報を B に送るという危険がある．

自分が正当な発信者であることを A が主張するためには次のようにすればよい．いま，A は A 自身の公開鍵 $\{e_A, N_A\}$ を公開しているとする．A は送信したい平文 m に A 自身の秘密鍵 d_A を用いて署名を施して r_A を作り，r_A を B に送信する．B は r_A を受け取った後，A の公開鍵を用いて r_A から m を復元する．署名が間違っていると m が正しく復元されないので，A が送信者であるという正当性が保証される．

$$A \Rightarrow m \xrightarrow[\text{署名}]{d_A} c_B \xrightarrow[\text{復元}]{e_A, N_A} m \Rightarrow B$$

ところがこの場合，A の公開鍵を使って第三者 B' も r_B から m を復元することができてしまう．これでは送信した内容 m の秘密は守られない．

秘密性と正当性を同時に実現するためには，次のようにすればよい．まず，A が平文 M を A 自身の秘密鍵 d_A を用いて署名し，次にその結果 r_A を B の公開鍵 $\{e_B, N_B\}$ で暗号化する．こうしてできた暗文 c_B を B に送信する．B は初めに自分の秘密鍵 d_B を用いて復号化し，その結果 r_A から A の公開鍵 $\{e_A, N_A\}$ を用いて平文 m を得る．

$$A \Rightarrow m \xrightarrow[\text{署名}]{d_A} r_A \xrightarrow[\text{暗号化}]{e_B, N_B} c_B \xrightarrow[\text{復号化}]{d_B} r_A \xrightarrow[\text{復元}]{e_A, N_A} m \Rightarrow B$$

参考文献

[1] 澤田秀樹：暗号理論と代数学，海文堂（1997）

[2] 吉田武：素数夜曲，海鳴社（1994）

[3] 和田秀男：数の世界，岩波書店（1981）