RSA 暗号

1977 年 R. L. Rivest, A. Shamir, L. M. Adleman は新しい公開鍵暗号システムを発明した．この暗号は 3 人の名前を取って RSA 暗号と呼ばれ，現在インターネット上で広く使われている．この方式の重要な部分は「大きい数の素因数分解は困難である」ということである．発明者 3 氏は，この功績によって 2002 年のチューリング賞[*1]を受賞した．RSA 暗号のアルゴリズムは，1983 年にアメリカ合衆国で特許を取得し，RSA Security 社がライセンスを独占していたが，2000 年，特許期間が満了した．

扱う文字は全て整数とする．

定義 1 （公開鍵） p, q を 2 つの異なる大きな素数とする．

$$L = \mathrm{lcm}(p-1, q-1)$$

とする．e を L と互いに素な数とする．

$$N = pq$$

とする．e と N を公開する．

定義 2 （暗号） $x < N$ に対し，

$$y = x^e \pmod N$$

を暗号とする．

定理 1 （複合）

$$d = e^{-1} \pmod L$$

とすると，

$$x \equiv y^d \pmod N$$

で復号できる．

[証明]L はいわゆる $\lambda(N)$ であり, N を法として, 任意の N と互いに素の数を L 乗した場合, 必ず $1 \pmod N$ となる．そのような数の最小のものである．よって kL 乗した場合も 1 となる．つまり $kL+1$ 乗した場合，もとの数となるわけである．x, y も N と互いに素であるから，

$$\begin{aligned} y^d &\equiv x^1 \pmod N \\ &= x \end{aligned}$$

[証明おわり]

$\lambda(N)$ の代わりに $\phi(N)$ を用いることもできるが，一般に $\lambda(N)$ の方が値が小さいので便利である．

[**例**] 実際は大きい素数を用いるが小さい素数を用いる．今，

$$p = 17, q = 23$$

[*1] チューリング賞 (A.M. Turing Award) は，計算機科学分野で革新的な功績を残した人物に年に 1 度 ACM から贈られる賞であり，世界最高の権威を持ち，ノーベル賞と同クラスの賞とされている．

とする．つまり

$$N = 17 * 23 = 391$$

である．また

$$L = \lambda(pq) = \mathrm{lcm}((p-1),(q-1)) = \mathrm{lcm}(16,22) = 2^4 * 11 = 176$$

L と互いに素である数,

$$e = 19$$

を選び，N, e を公開する．

$$19d \equiv 1 \pmod{176}$$

より（適当な方法で合同式を解いて）

$$d = 139$$

d を秘密とする．
$x = 100$ という平文を暗号化する．

$$y = x^e = 100^{19} \equiv 349 \pmod{391}$$

複合化する．

$$y^{139} = 349^{139} \equiv 100 \pmod{391}$$

参考文献

[1] 桔梗宏孝「現象の数理 講義ノート 2（オイラーの定理とフェルマーの小定理)」
http://kurt.scitec.kobe-u.ac.jp/~kikyo/lec/07/gensho/code14_15.pdf
[2]「ウィキペディア」<http://ja.wikipedia.org/wiki/>