1　RSA 暗号の仕組み (2012 9/22)

RSA 暗号の仕組みについて簡単な説明をしてみます.

1.1　鍵生成

まず，秘密鍵と公開鍵をどのように生成するかということを説明しよう.

送信者（以下ボブと言う）はランダムに続けて二つの大きな素数 p, q を選び，二つの積 $N = pq$ を計算する．さらに自然数 e を

$$1 < e < (p-1)(q-1) \text{ かつ } \gcd(e, (p-1)(q-1)) = 1$$

をみたすように選び，自然数 d を

$$1 < d < (p-1)(q-1) \text{ かつ } de \equiv 1 \pmod{(p-1)(q-1)}$$

となるように選ぶ．$(e, (p-1)(q-1)) = 1$ であるので，こういう性質を持つ自然数 d は存在する．この d は，拡張ユークリッドアルゴリズムで計算される．ここで，e は常に奇数であることに注意しておこう．公開鍵はこの 2 組の数 (N, e) である．秘密鍵は d である．N をRSA **モジュール**，e を**暗号化指数**，d を**復号化指数**と呼ぶ.

1.2　暗号化

平文が数値化され（たとえば ASKII コードによるアルファベットの 2 進数表示など）

$$0 \leq m < N$$

である全ての自然数 m よりなるとする．一つの平文 m は公開鍵 e を用いて暗号化され

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

になる．公開鍵 (N, e) を知っている人なら誰でも，暗号化を実行することができる.

1.3　復号化

RSA 方式の復号化は次の定理がもとになっている.

定理

RSA 方式で (N, e) を公開鍵，d をそれに対応した秘密鍵とする．その時，任意の自然数 m $(0 \leq m < N)$ に対して

$$m \equiv (m^e)^d \pmod{N}$$

が成立する．

証明

$ed \equiv 1 \pmod{(p-1)(q-1)}$ であるので

$$ed = 1 + l(p-1)(q-1)$$

となる $l \in \mathbb{Z}$ が存在する．よって

$$(m^e)^d = m^{ed} = m^{1+l(p-1)(q-1)} = m(m^{(p-1)(q-1)})^l$$

である．この等式により

$$(m^e)^d \equiv m(m^{(p-1)})^{(q-1)l} \equiv m \pmod{p}$$

が成立することが分かる．p が m の約数でない場合，この合同式はフェルマーの小定理[1]から導かれる．その他の場合は，この合同式の両辺は $0 \pmod{p}$ であるから自明である．全く同様に

$$(m^e)^d \equiv m \pmod{q}$$

であることが分かる．p と q は異なった素数であることから

$$(m^e)^d \equiv m \pmod{N}$$

が分かる．ここで $0 \leq m < N$ であるので定理が成立する．

この定理により秘密鍵 d を知っている唯一の受信者（アリスと言う）は，c を (1) 同様に計算して，m を

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

により求めることができる．したがって，RSA 方式が実際に暗号系であること，すなわち任意の暗号化関数に対して復号化関数が存在することが分かる．

注）RSA 暗号の RSA とは，1978 年にこの暗号システムを考え出した MIT の 3 人の数学者 Rivest, Shamir, Adleman の頭文字を取ってつけられたものである．RSA 暗号を含む暗号にまつわる歴史については，サイモン・シン著，青木薫翻訳の「暗号解読」（新潮社）が面白い．

[1] フェルマーの小定理とは素数 p，$n \in \mathbb{Z}$ に対して $n^p \equiv n \pmod{p}$ が成り立つという定理