柴　直樹 作成

2016 年 3 月 3 日 (Ver. 1.1)

柴・水上著「経営情報システム入門」—第 6 章補足資料

RSA 暗号

非対称鍵暗号アルゴリズム RSA って何だろう？

「経営情報システム入門」の第 6 章で述べたように、RSA はリヴェスト (R. Rivest), シャミア (A. Shamir), エイドルマン (L. Adleman) の 3 人により考案されたもので、非対称鍵暗号アルゴリズムとして広く使用されています。これは、大きな数の素因数分解が困難である（時間がかかる）という数学的性質を基礎とした方式です。

以下では、まず RSA アルゴリズムによる暗号化・複合処理の手順を示し、簡単な例を用いて RSA アルゴリズムによる暗号通信の例を示します。最後に、これらの RSA 暗号の原理について簡単に述べます。

RSA アルゴリズムによる暗号化と複合

以下に暗号化／復号処理を示します。

1. 鍵の生成

   (a) 2 つの異なる大きな素数（現在では、10 進数にして 300 桁を超える数が用いられる）

   $$p, q$$

   を用意し、両者の積 $n = pq$ を求める。

   (b) $(p-1)(q-1)$ に対して互いに素 [1] である 2 以上の任意の整数 e を選ぶ。

   (c) $(p-1)(q-1)$ を法とする掛け算のもとでの e の逆数、つまり、

   $$ed = N(p-1)(q-1) + 1 \quad (N \text{ は整数})$$

   なる数 d を求める [2] 。

   (d) 以上で得られた 2 つの数の組 (n, e) が公開鍵、d が秘密鍵となる。

2. 暗号化
   送りたいメッセージを m とし [3] 、

   $$c = m^e (\mathrm{mod}\ n)$$

   が暗号文 [4] 。

3. 復号

   $$m = c^d (\mathrm{mod}\ n)$$

[1] 2 つの整数 m,n が 1 以外の公約数を持たないとき、m と n は互いに素であるといいます。例えば、20 と 21 は互いに素です。

[2] この式を満たす d が必ず存在することは、数学的に証明できます。本資料の後半にある「定理」がそれです。

[3] 例えば、テキスト（文字列）を送りたい場合は、文字のコードを数値として読み下す等の方法で整数化します。例えば、メッセージが “IBM” であるとして、この文字列の ASCII コードを 10 進数として読み下すと、736677(I=73, B=66、M=77)。これを 10 進表記による整数として、$m = 736677$ となります。

[4] $m^e (\mathrm{mod}\ n)$ は、m^e を n で割った余りを表します。

RSA による暗号通信の例

受信者 B はあらかじめ以下の手順で鍵を生成する。

1. 鍵の生成
   (a) $p = 3, q = 11$ とする（実際は 10 進数にして 300 桁超の数が用いられる）。$n = 33$。
   (b) $(p-1)(q-1) = 20 = 2^2 \times 5$ に対し、互いに素である数を $e = 3$ とする。
   (c) $d = 7$ とすると、
   $$ed = 3 \times 7 = 21$$
   (d) B は $(33, 3)$ を公開し、7 を秘密鍵として保管する。
2. 暗号化
   発信者 A が B にメッセージを送りたいとする。送りたいメッセージを $m = 2$ とすると、B の公開鍵 $(33, 3)$ を使って、
   $$c = 2^3 (\text{mod } 33) = 8$$
   8 を B に送る。
3. 復号 [5]
   $c = 8$ を受け取った B が、B の秘密鍵を使って復号する。
   $$m = 8^7 (\text{mod } 33) = (8^3)^2 \times 8 (\text{mod } 33) = (31 \times 8)^2 \times 8 (\text{mod } 33) = 17^2 \times 8 (\text{mod } 33) = 25 \times 8 (\text{mod } 33) = 2$$

RSA 暗号の原理

上記の RSA 暗号の原理である数学理論（整数論）ついて簡単に示しますが、さらに詳しく知りたい人は、例えば、文献 [1] の No.10 に分かりやすい解説があります。また、文献 [2] にも簡単な解説があります。以下の解説は、後者を参考にしています。

まず，整数に関して以下が成り立ちます。

フェルマの小定理

素数 p と互いに素な任意の整数 x に対し，

$$x^{p-1} (\text{mod } p) = 1$$

が成立する．証明は例えば，参考文献 [3]p.37 を参照せよ．

補題 1 任意の整数 $n(\geq 2)$ について，n と互いに素な 2 以上の整数が存在する．

これはほとんど自明である．n の素因数でない素数を考えればよい．

補題 2 互いに素な整数 a, b について，

$$au + bv = 1$$

[5] この計算過程においては、
$$x \cdot y (\text{mod } n) = [x (\text{mod } n) \cdot y (\text{mod } n)] (\text{mod } n)$$
という性質を使用しています。

なる整数 u, v が存在する．

例えば，参考文献 [3]p.9〜12 を参照せよ．

定理

p, q を異なる素数とし，

$$n = pq$$

とする．このとき，$(p-1)(q-1)$ と互いに素な任意の整数を e とするとき，

$$ed(\mathrm{mod}\ (p-1)(q-1)) \quad = \quad 1 \tag{1}$$

なる整数 d が存在する．さらに，$m < n$ について，

$$c = m^e(\mathrm{mod}\ n)$$

とすると，

$$c^d(\mathrm{mod}\ n) = m$$

である．

（証明）まず，補題 1 より p, q を十分大きくとれば（少なくとも 3 以上），$(p-1)(q-1)$ と互いに素な整数 e が存在する．さらに，補題 2 より

$$eu + (p-1)(q-1)v = 1$$

なる整数 u, v が存在し，$d = u$ とすれば，

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

より，

$$ed(\mathrm{mod}\ (p-1)(q-1)) = 1$$

(1) より，整数 k を用いて

$$ed = 1 + k(p-1)$$

と書ける．

(i)m と p が互いに素なら，フェルマの小定理より，

$$m^{p-1}(\mathrm{mod}\ p) = 1$$

よって，

$$\begin{aligned}
(m^e)^d(\mathrm{mod}\ p) &= (m)^{ed}(\mathrm{mod}\ p) \\
&= (m)^{1+k(p-1)}(\mathrm{mod}\ p) \\
&= m \cdot (m^{p-1})^k(\mathrm{mod}\ p) \\
&= m[(m^{p-1}(\mathrm{mod}\ p))^k](\mathrm{mod}\ p) \\
&= m(\mathrm{mod}\ p)
\end{aligned}$$

(ii)m と p が互いに素でない時，p は素数より m は p の倍数．このとき，

$$\begin{aligned}(m^e)^d(\mathrm{mod}\ p) &= [m(\mathrm{mod}\ p)]^{ed}(\mathrm{mod}\ p)\\ &= 0\\ &= m(\mathrm{mod}\ p)\end{aligned}$$

よって，(i)(ii) いずれの場合も $(m^e)^d - m$ は p で割り切れる．同様にして，$(m^e)^d - m$ は q で割り切れる．p, q は異なる素数より，$(m^e)^d - m$ は $n = pq$ で割り切れる．よって，$(m^e)^d = ln + m$ と書ける．

$$\begin{aligned}c^d(\mathrm{mod}\ n) &= (m^e)^d(\mathrm{mod}\ n)\\ &= (ln + m)(\mathrm{mod}\ n)\\ &= m\end{aligned}$$

である．(証明終り)

練習問題

1. 本文中にあった RSA 暗号アルゴリズムにおける、次の鍵の例を使い、平文 $m = 3$ を暗号文にせよ。さらにこの暗号文を復号することでもとの平文が得られることを確かめよ。

   公開鍵 :$(33, 3)$

   秘密鍵 :7

2. RSA 暗号アルゴリズムにおける鍵の生成においては、整数のもついくつかの性質が使われているが、本文中にもあったとおり、次はその 1 つである。

   任意の整数 $n(\geq 2)$ について、n と互いに素な 2 以上の整数が存在する。

   本文中の鍵生成の手続きにおいて $p = 13, q = 11$ としたとき、$(p-1)(q-1)$ と互いの素な 2 以上の整数 e を求めよ。

参考文献

[1] 岡本、「明るい情報化社会の実現を目指す暗号技術」、bit, Vol.23, No.8–13, 共立出版, 1991（DES に関しては No.9 に、RSA に関しては No.10 に分かりやすい解説がある）

[2] 稲村、「メールにもっとプライバシー」、bit, Vol.27, No.5,6, 共立出版, 1995 （DES、RSA の簡単な解説がある）

[3] 松坂和夫,「代数系入門」, 岩波書店、1975