RSA 暗号アルゴリズムの正当性証明

—情報セキュリティ補足資料—

村川 猛彦

2005 年 5 月 20 日

1 前提

1.1 使用する文字とその関係

- p, q は相異なる素数
- $N = pq$
- $L = \mathrm{lcm}(p-1, q-1)$
- $1 \leq E < L$, $1 \leq D < L$, $ED \ \% \ L = 1$

1.2 証明したいこと

$0 \leq M < N$ の任意の整数 M に対して, $(M^E \ \% \ N)^D \ \% \ N = M$

1.3 剰余に関して活用する性質

分配法則 $(x \times y) \ \% \ z = ((x \ \% \ z) \times (y \ \% \ z)) \ \% \ z$

剰余演算を含む指数法則 $x^{y_1 y_2} \ \% \ z = (x^{y_1} \ \% \ z)^{y_2} \ \% \ z$

中国人剰余定理 (2 元連立 1 次合同式の場合) y と z が互いに素 (最大公約数が 1) であり, $(x-\alpha) \ \% \ y = 0$ と $(x-\beta) \ \% \ z = 0$ がともに成り立つなら, $(x-\gamma) \ \% \ yz = 0$ を満たす γ が $0 \leq \gamma < yz$ の範囲でちょうど一つ存在する. 具体的には, $yy' + zz' = 1$ を満たす整数 y', z' を一組求めれば, $\gamma = (\alpha z z' + \beta y y') \ \% \ yz$ により求められる.

フェルマーの小定理 x が素数であり, y が x の倍数でなければ, $y^{x-1} \ \% \ x = 1$.

2 証明

M が p と q の両方で割り切れるとき，どちらでも割り切れないとき，一方で割り切れるときの 3 つに分けて証明する．

(i) M が p と q の両方で割り切れるとき: $0 \leq M < N$ の範囲では，$M = 0$ のみである．このときは，$(M^E \ \% \ N)^D \ \% \ N = 0 = M$.

(ii) M が p と q のいずれでも割り切れないとき: まず，$M^{ED-1} \ \% \ p = 1$ であることを示す．$ED - 1$ は L の倍数，したがって $p - 1$ の倍数であるので，$ED - 1 = r(p - 1)$ を満たす整数 r が存在する．すると，

$$\begin{aligned} M^{ED-1} \ \% \ p &= M^{r(p-1)} \ \% \ p \\ &= (M^{p-1} \ \% \ p)^r \ \% \ p \\ &= 1^r \ \% \ p \qquad (\text{フェルマーの小定理を用いた．}) \\ &= 1 \end{aligned}$$

となる．同様に，$ED - 1 = s(q - 1)$ を満たす整数 s も存在し，

$$\begin{aligned} M^{ED-1} \ \% \ q &= (M^{q-1} \ \% \ q)^s \ \% \ q \\ &= 1 \end{aligned}$$

が成り立つ．

これらの式および中国人剰余定理を用いると，$M^{ED-1} \ \% \ pq = 1$ を得る．

この両辺に M をかけて N で割った剰余を求めても，等号は変わらない．このとき左辺は

$$\begin{aligned} ((M^{ED-1} \ \% \ pq) \times M) \ \% \ N &= (M^{ED-1} \times M) \ \% \ N \\ &= M^{ED} \ \% \ N \\ &= (M^E \ \% \ N)^D \ \% \ N \end{aligned}$$

であり，右辺は M である．

(iii) M が p と q のいずれか一方で割り切れるとき: 一般性を失うことなく，M が p で割り切れず，q で割り切れるとする．このとき，(ii) と同様に，$M^{ED-1} \ \% \ p = 1$ であり，この両辺に M をかけて p で割った剰余を求めると，$M^{ED} \ \% \ p = M \ \% \ p$ すなわち $(M^{ED} - M) \ \% \ p = 0$ となる．

次に q に関しては，$M \ \% \ q = 0$ なので $M^{ED} \ \% \ q = 0$ である．

これらと中国人剰余定理を用いて式計算を行うと，$M^{ED} \ \% \ pq = M$ を得る．

(証明終)