# RSA 暗号の仕組み

## 【フェルマーの小定理】

p を素数とし、a を p と互いに素な整数としたとき、次の式が成り立つ。

$$\mathrm{a}^{p-1} \equiv 1 \pmod{\mathrm{p}}$$

p を素数,k を整数とする。すべての整数mに対して、次の式が成り立つ。

$$\mathrm{m}^{k(p-1)+1} \equiv m \pmod{\mathrm{p}}$$

## 【オイラーの定理】

n は自然数、1 以上 n 以下の数で n と互いに素な自然数の個数をφ（n）とする。このとき、次の式が成り立つ。

$$\mathrm{a}^{\varphi(n)} \equiv 1 \pmod{n}$$

さらに、 k を整数として、すべての整数mについて、次の式が成り立つ。

$$m^{\varphi(n)\times k+1} \equiv m \pmod{n}$$

ここで、$\mathrm{ed} = \varphi(n) \times k+1$が成り立つとすると

$$m^{ed} \equiv m \pmod{n}$$

※ n が素数 p,q の積である場合、$\varphi(n) = (p-1)(q-1)$ である。このとき、

$\mathrm{ed} = (\mathrm{p}-1)(\mathrm{q}-1) \times k+1$ を満たす整数 e,d と n を用いて

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

が成り立つ。

$m^e$を暗号文 c とすると、$\mathrm{c}^{\mathrm{d}} = (m^e)^d \equiv m \pmod{\mathrm{n}}$

となり平文に戻る。