平文 M $\longrightarrow$

$\mathbf{C = M^e \ (mod\ n)}$

暗号化鍵 (e, n)

暗号文 C $\longrightarrow$

$\mathbf{M = C^d \ (mod\ n)}$

複合化鍵 (d, n)

パラメータ ：

(1) $\mathbf{n = p \cdot q}$ **(素数)**

(2) $\mathbf{e \cdot d \ (mod\ r) = 1}$

(3) $\mathbf{r = LCM\ (p - 1,\ q - 1)}$

LCM; 最大公約数

フェルマーの定理 ：

p が素数のとき p と互いに素な整数に対し

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

M		
	ϕ	
		W