Fermat's Little Theorem

$a^{p-1} = 1 \mod p$ if a is not divisible by p.

$$a^{\phi(m)} \equiv 1 \mod m.$$

$S: \quad 1 = b_1 < b_2 < b_3 \cdots < b_{\phi(m)}$

$$\phi(18) = 6$$

$S: \quad 1, 5, 7, 11, 13, 17$

Let $a = 5$

$S': \quad 5', 25 \equiv 7', 35 \equiv 17', 55 \equiv 1', 65 \equiv 11', 85 \equiv 13' \pmod{18}$

$$\boxed{a^{\phi(m)} \equiv 1 \mod m}$$

✱ Chinese Remainder Theorem.

$m_1, m_2, \ldots m_k$ } Coprime sets
$a_1, a_2 \ldots a_k$ }

$$x = a_i \pmod{m_i}$$

has a unique solution

$$x_k = \sum_i a_i M_i y_i$$

$$M = \prod_{i=1} m_i \quad , \quad M_i = \frac{M}{m_i}$$

$$y_i = (M_i^{-1}) \bmod m_i$$

$m_i = 7, 10, 9$

$$\left.\begin{aligned} x &= 5 \mod 7 \\ x &= 3 \mod 10. \\ x &= 7 \mod 9 \end{aligned}\right|$$

$$M = 7 \times 10 \times 9 = 630$$

$$\left.\begin{aligned} M_1 &= 90 \\ M_2 &= 63 \\ M_3 &= 70 \end{aligned}\right\}$$

$$y_1 = 90^{-1} \bmod 7$$

$$\Rightarrow 90 y_1 = 1 \bmod 7.$$

$$y_1 = 6$$

$$y_2 = 7$$

$$y_3 = 4$$

Bob

p, q primes

$N = pq$

$\phi(N) = (p-1)(q-1)$

Let $p = 7$, $q = 5$ | $N = 35$.

$\phi(35) = 6 \times 4 = 24$.

e coprime with $\phi(N)$

(N, e) : Public Code for Bob

$p = 7$

$q = 5$

$\phi(35) = 24$ $\quad e = 7.$

$(35, 7)$. : Public.

m is to be encoded

$$C = m^e \bmod N$$ Code.

Let $m = 3$

$C = 3^7 \bmod 35.$

$= 2187 \bmod 35.$

$= 17$

(N, e). : Public

Bob's Private key.

$$ed = 1 \mod \phi(N)$$

$$7d = 1 \mod 24. \qquad 24$$

$$\boxed{d = 7}$$

$C = 17$

$$17^7 = 410338673.$$

$$\equiv 3 \mod 35$$

$$=$$

$$\boxed{C^d \mod N}$$

$$=$$

$$m.$$