Mathematic Theory for RSA

if $C = M^e \bmod n$

then $M = C^d \bmod n$

Lemma 1

If a is a relatively prime to n and

$(a \times b) \bmod n = (a \times c) \bmod n$,

then $b \bmod n = c \bmod n$.

Proof: $b \bmod n = c \bmod n$ iff $\exists p \in \mathbb{Z}$

s.t. $(b - c) = pn$

Let $(a \times b) \bmod n = (a \times c) \bmod n = r$

Then $\exists p_1, p_2$ s.t. $\begin{cases} a \times b = p_1 n + r & ① \\ a \times c = p_2 n + r & ② \end{cases}$

① − ②, $a \times (b - c) = (p_1 - p_2) n$

Since a is relatively prime to n,

then $(b - c)$ is an integer Multiple of n

i.e. $(b - c) = kn$, for some n

Thus, $b \bmod n = c \bmod n$

Lemma 2.

$ab \bmod n = (a \bmod n)(b \bmod n) \bmod n$

Proof: Let $a \bmod n = r_1 \Rightarrow a = p_1 n + r_1$

$b \bmod n = r_2 \Rightarrow b = p_2 n + r_2$

then $ab = (p_1 n + r_1)(p_2 n + r_2) = p_1 p_2 n^2 + p_1 r_2 n + r_1 p_2 n + r_1 r_2$

$ab \bmod n = r_1 r_2 \bmod n = (a \bmod n)(b \bmod n)$

Fermat's Theorem

If p is prime and a is a positive integer not divisible by p,

then $a^{p-1} \bmod p = 1 \bmod p$

Proof: According to Lemma 3, $Z_p^a = Z_p$

Since $Z_p^a = Z_p$, the products of all the elements in Z_p^a and Z_p are the same.

Thus $(a \times 2a \times \cdots \times (p-1)a) \bmod p = ((a \bmod p)(2a \bmod p) \cdots ((p-1)a \bmod p)) \bmod p$

$= (p-1)! \bmod p$ (右边)

Note that $a \times 2a \times \cdots \times (p-1)a = a^{p-1}(p-1)!$

Therefore $(a^{p-1}(p-1)!) \bmod p = (p-1)! \bmod p$

Since $a^{\cancel{p-1}}$ ~~an~~ $\cdot (p-1)!$ is relatively prime to p,

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

Lemma 3

Let $Z_p^a = \{0, (a \bmod p), (2a \bmod p), \cdots, ((p-1)a \bmod p)\}$

If p is prime and a is a positive integer not divisible by p,

then $Z_p^a = Z_p$