Prof. D.K. Ghosh
Lec. 41 Date: 27/6/2016

Trap door Function.

f : Easy problem
(Polynomial time)

f^{-1} : Hard Problem.

RSA : f: Multiplication of 2 Large primes.

f^{-1} : Given the result of multiplication, to find prime factors.

p ; $a \in \mathbb{Z}$ $\quad a \not\equiv 0 \mod p^2$

$$\boxed{a^{p-1} \equiv 1 \mod p}$$

S: $1, 2, 3, 4, \ldots (p-1)$

$r \in S$

$s \in S$

$ar \equiv as \pmod p$

$a(r-s) \equiv 0$

$r-s$ is divisible by p.

~~r, s~~

S: $1, 2, 3, \ldots \quad p-1$

S': $a, 2a, 3a, \ldots \quad a(p-1) \pmod p$

$$1 \cdot 2 \cdot 3 \ldots (p-1) = a^{p-1} \cdot (\underbrace{1 \cdot 2 \cdots p-1}_{})$$

$$\boxed{a^{p-1} = 1}$$

Fermat's Little Theorem

Euler's Theorem

$\phi(18) = 6$

1, 5, 7, 11, 13, 17

If n is a prime

$\phi(n) = n - 1$