# RSA Cryptosystem.

## Key generation

e is coprime to $n$ & $< n$ //

$\underline{pk} \Rightarrow n = pq \; ; \; e \in \phi(n)$

euler totient function.

another definition of $\phi(n)$

$\phi(n) = |\mathbb{Z}_n^*|$

$\underline{sk}$ : $d$ s.t $ed \equiv 1 \bmod \phi(n)$

## Encryption.

$c \equiv m^e \bmod N$

## Decrypt^n

$m \equiv c^d \bmod N$

## Correctness Proof.

$c \equiv m^e \bmod N$

$c^d \bmod N \equiv m^{ed} \bmod N$

Thm :- In any group $G$ $\forall g \in G$

$g^{|G|} = 1$ $\quad |G|$ = order of group

Here we are working with $\mathbb{Z}_n^*$.

$\therefore m^{|\mathbb{Z}_n^*|} = \boxed{m^{\phi(N)} \bmod N = 1}$ → Euler's Extension of Fermat's Little Theorem.

now $m^{ed} \bmod N = m^{ed \bmod N} \bmod N$

$= m^1 \bmod N$ (By definiⁿ of $d$)

Proof for Thm.

for any Group $G$ with order $|G|$

elements are $g_1, g_2 \cdots g_{|G|}$

if $gg_i = gg_j \Rightarrow g_i = g_j$ (multiply with inverse on both sides)

$g_1 \cdot g_2 \cdots g_{|G|}$

$= (gg_1)(gg_2)(gg_3)\cdots(gg_{|G|})$

$\therefore g^{|G|} g_1 g_2 \cdots g_G = g_1 g_2 \cdots g_G$

$g^{|G|} = 1 \bmod N$ ↳ note that we are assuming that group is commutative.

(similar proof to FLT)

## Attacks on Textbook RSA.

→ small exponent attack. (Common modulus)

→ assume very small value of $e$ $(=3)$

→ and very small message size $(\leq n^{1/3})$

Common modulus attack.

$c_1 \equiv m^{e_1} \bmod N$

$c_2 \equiv m^{e_2} \bmod N$

assume $\gcd(e_1, e_2) = 1 \Rightarrow \exists x, y$ s.t $e_1 x + e_2 y = 1$ (extended euclid) algo.

$c_1^x c_2^y \equiv m^{e_1 x} m^{e_2 y}$

$\equiv m^{e_1 x + e_2 y}$

$\equiv m$ // → get message directly.

→ same message, small exponent, different $N$ (can occur when Broadcasting a message)

$$\left.\begin{aligned} c_1 &\equiv m^3 \bmod N_1 \\ c_2 &\equiv m^3 \bmod N_2 \\ c_3 &\equiv m^3 \bmod N_3 \end{aligned}\right\} \text{calculate } m$$

Can use Chinese Remainder Theorem.

$x \equiv a_1 \bmod p_1$

$x \equiv a_2 \bmod p_2$

$\vdots$

$x \equiv a_n \bmod p_n$.

$$\left.\begin{aligned} m^3 &\equiv c_1 \bmod N_1 \\ m^3 &\equiv c_2 \bmod N_2 \\ m^3 &\equiv c_3 \bmod N_3 \end{aligned}\right.$$

$\therefore$ unique $m^3 \leq N_1 N_2 N_3$

Unique $x \in [0, \prod p_i]$ which satisfies above condiⁿ

### Proof for CRT

Case I

$a_1 = a_2 = \cdots\cdots a_k = 0$

$\therefore a_i = \prod_i p_i$

Case II

$a_1 = 1 \quad a_2 = \cdots = a_k = 0$

$$x_2 = \left(\prod_{i=2}^{k} p_i\right) \cdot \left(\left(\prod_{i=2}^{k} p_i\right)^{-1} \bmod p_1\right) \bmod \prod_i p_i$$

Case III

$a_2 = 1 \quad$ rest $= 0$

$$x_2 = \overbrace{\left(\frac{\prod_i p_i}{p_2}\right)}^{P} \left[P^{-1} \bmod p_2\right] \bmod \prod p_i$$

$\therefore$ For general case.

$x = a_1 x_1 + a_2 x_2 + \cdots a_n x_k$.

$$= \sum_{i=1}^{k} a_i \left[\left(\frac{\prod_j p_j}{p_i}\right) \cdot \left[\left(\frac{\prod p_j}{p_i}\right)^{-1} \bmod p_i\right] \bmod \prod_j p_j\right]$$

$\therefore$ TextBook RSA is insecure.

## Industry version : PKCS v 1.5

Idea : Padded RSA

$c = (r \| m)^e \bmod N$.

$r \Rightarrow$ not sent with ciphertext (obviously)

How to get $r$ back?

Cutoff pt. for $r$ known?

attacks still possible.

random cut off pt $\Rightarrow$ not possible to attack.

where to put $r$?

HCP for RSA = LSB (No Proof given)

easier to find first few bits

$\Rightarrow$ put random noise there

$\therefore$ put at prefix.

### PKCS - v1.5

$r$ = Min 64 bits (8 bytes)

$r$ cannot be all $0_s$

$$c = [00000000 \| 00000010 \| r \| \underbrace{00000000}_{} \| m]^e \bmod N$$

$r$ might be huge in size

but $r$ cannot be all zeros

This helps to find cut off pt.