## Example

### step 1 key generation

let's take $p = 7$ and $q = 19$.

2.) let $n = p \times q = 7 \times 19 = 133$

3) let $m = (p-1)(q-1) = (7-1)(19-1) = 108$

4.) choose a small number, e coprime to m, (gcd b/w 2 is 1).

$e = 2 \Rightarrow GCD(e, 108) = 2$

$e = 3 \Rightarrow GCD(e, 108) = 3$

$e = 4 \Rightarrow GCD(e, 108) = 4$

$e = 5 \Rightarrow GCD(e, 108) = 1$ (so we can take this value).

5-) now find d such that $de \% m = 1$.

this can be rewritten as.

$$d = \frac{(1 + nm)}{e}$$

→ now, we keep iterating the eqn where $n \in W$

$n = 0 \Rightarrow d = 1/5$

$n = 1 \Rightarrow d = 109/5$

$n = 2 \Rightarrow d = 217/5$

$n = 3 \Rightarrow d = 325/5 = 65$

now, we will take up this value for d.

so, PK = $n = 133, e = 5$

SK = $n = 133, d = 65$.

### Next step:

$$C = m^e \% n$$

Encryption → $C = P^e \% n$.

now, message must be smaller than p and q..

A key board must be published,

$C = P^e \% n \Rightarrow 6^5 \% 133$

$\Rightarrow 7776 \% 133$

$= 62$

Decryption:

$P = C^d \% n.$

$\Rightarrow 62^{65} \% 133$

$\Rightarrow 62 * 62^{64} \% 133$

$\Rightarrow 62 * (62^2)^{32} \% 133$

$\Rightarrow 62 * (3844)^{32} \% 133$

$\Rightarrow 62 * (3844 \% 133)^{32} \% 132$

$\Rightarrow 62 * 120^{32} \% 133$

this is repeated until we reach single exponent value

$62 * 36^{16} \% 133$

$62 * 99^8 \% 133$

$62 * 92^4 \% 133$

$62 \times 85^2 \equiv 133$

$62 \times 43 \equiv 133$

$2666 \equiv 133$

$= 6$

this matches PT (plain text) so, it
works