RSA Algorithm (Rivest, Samir, Adlemann)

→ Trying to generate public key & private key

1) Choose 2 prime nos. → p & q

Let p = 61, q = 53

2) Compute : $n = p * q = 61 \times 53 = 3233$

3) $\phi(n) = (p-1) * (q-1)$: (Euler's totient function)

$= (61-1) * (53-1)$

$= 60 \times 52$

$= 3120$

4) Choose 'e' : $1 \le e < \phi(n)$, coprime to $\phi(n)$

e = 17 (Given, if)

$\gcd(17, 3120) = 1$

=> (e, n) = public key (17, 3233)

5) Determine 'd' as $ed \equiv 1 \bmod \phi(n)$

→ multiplicative Inverse

Here e & $\phi(n)$ are coprime)

$d = e^{-1} \bmod \phi(n)$

(d is MI of e)

$\Rightarrow 17 * d = 1 \bmod 3120$

$d = 2753$

=> (d, n) = private key

(2753, 3233)

finding 'd'

→ both are co-prime. Then d is MI of e.

$ed = 1 \bmod \phi(n)$

$$d = \frac{(\phi(n) * i) + 1}{e}$$ → MI formula. (Multiplicative Inverse)

$$d = \frac{(3120 \times 1) + 1}{17} = 183.58$$ × Point value will not be accepted.

$$d = \frac{(3120 \times 2) + 1}{17} = 367.11$$

$$d = \frac{(3120 \times 3) + 1}{17} = 550.647$$

$$d = \frac{(3120 \times 4) + 1}{17} = 734.17$$

$$d = \frac{(3120 \times 15) + 1}{17} = 2753$$

$d = (2753, 3233)$

RSA

Encryption (e, n) Public key.

Private key

Decryption (37, 143) (d, n)

plaintext

Let msg is in the form of binary

Now it will convert into decimal

P = 13 (let)
n = 143

$c = p^e \bmod n$ ∴ P < n

$c = 13^{13} \bmod 143$

Powers add up

⇒ $13 \bmod 143 = 13$

⇒ $13^4 \bmod 143 = 104$

⇒ $13^8 \bmod 143 = 91$

Modular Arithmetic Implementation

$c = [(13^8 \bmod 143)(13^4 \bmod 143)(13 \bmod 143)] \bmod 143$

$= [91 \times 104 \times 13] \bmod 143$

$C = 52$

$P = c^d \bmod n$

$= 52^{37} \bmod 143$

⇒ $52 \bmod 143 = 52$

⇒ $52^4 \bmod 143 = 26$

⇒ $52^{32} \bmod 143 = 130$

$P = [(52^{32} \bmod 143)(52^4 \bmod 143)(52 \bmod 143)] \bmod 143$

⇒ $P = [130 \times 26 \times 52]$ mod 143

multiplication → divided by 143

$P = 13$ ← reminder