SL Exp 4 RSA Encrypt

i) Select two large prime numbers p & q

ii) Calculate $n = p * q$

iii) Calculate $\phi(n) = (p-1) * (q-1)$ // eulers toient function

iv) Choose value of d such that

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

private key $\equiv \{d, n\}$ public key $= \{e, n\}$

Plaintext M

$C = M^e \bmod n \implies$ Encryption

$M \equiv C^d \bmod n \implies$ Decryption

SL Exp 4

Two prime numbers

$p = 53$ $\quad q = 59$.

i) Public key $n = p \times q = 3127$

↳ We also need a small exponent e: (Should be an Integer)

& not a factor of $\phi(n)$

$1 < e < \phi(n)$

ii) Generating private key:

such that $\phi(n) = (p-1)(q-1)$

$= 52 \times 58 = \underline{3016}$

Now calculate private key d;

$d = (k \times \phi(n) + 1)/e$ for some integer k,

when $k = 2$

$d = (2 \times 3016 + 1)/e$ consider $e = 3$.

$\therefore \boxed{d = 2011}$

Hence public key: $(n = 3127, e = 3)$ Private key $(d = 2011)$

Now say for eg, we want to encrypt (HI)

$H = 8$

$I = 9.$

Encrypted data $= c = (89^{e}) \bmod n.$

Decrypted data $= (c^{e}) \bmod n.$

$\phi(n) = 32$

$1 < e < 32.$

gcd ( )

$2 \longrightarrow$.

$3 \longrightarrow$

$4 \longrightarrow$

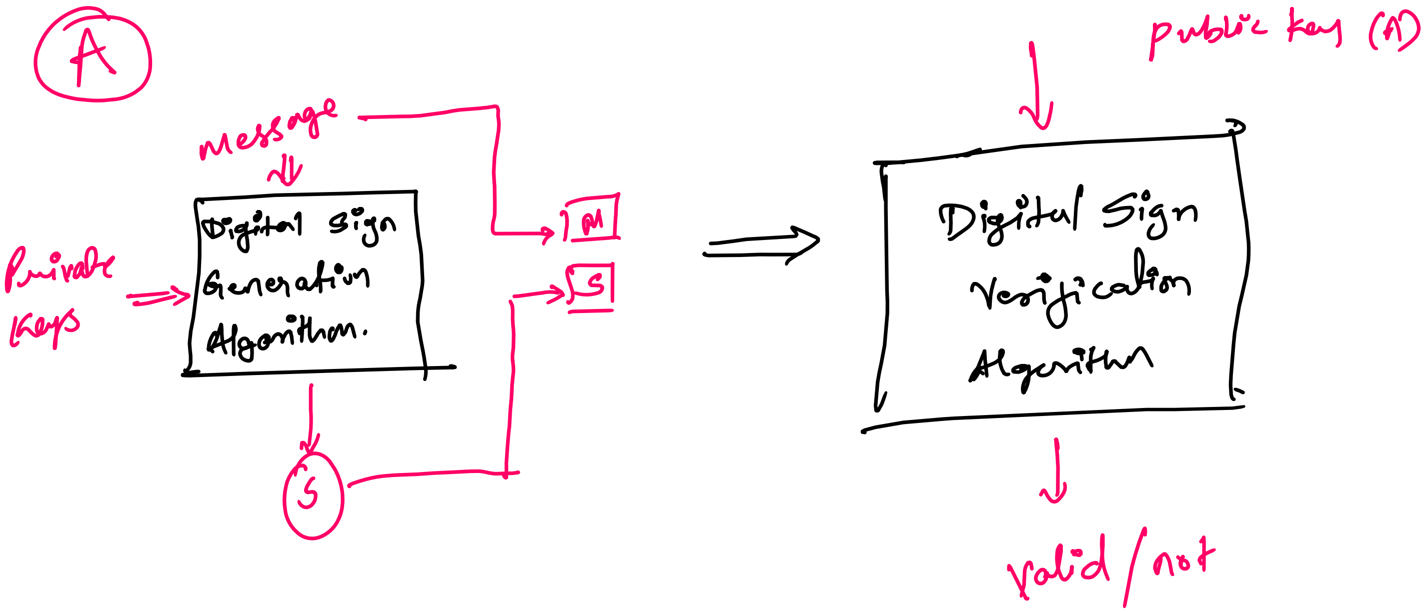
$4)\cancel{2}$. gcd =

Digita Signature Scheme (EXP 5)

- ↳ Assymmetric cryptography
- ↳ Encryption (private key)
- ↳ Decryption (public key)
- ↳ Used for authentication & Non-Repudiation.

authentication: correct person

Non-Repudiation: cannot deny



Diffie - Hellman key exchange. Exp 6.

↳ Not an encryption algorithm..

↳ Used to exchange secret keys.

↳. Assymmetric encryption is used to exchange the secret key.

Why we use this algorithm? –

Coz. key can be attacked while sending

i) prime number 'q'   ii) 'α' such that it must be primitive root of q.

a is a primitive root of q if

$a \bmod q$

$a^2 \bmod q$

$a^3 \bmod q$ . . ——— - - — $a^{q-1} \bmod q$ give results $\{1, 2, \ldots \ldots q-1\}$

* Key generation of person 1.

$x \Rightarrow$ private key

$y \Rightarrow$ public key

Let prime number $q = 7$

Let $\alpha = 5$ ---- primitive root

Let $X_A = $ (private key of A) & $X_A < q$ $\quad X_A = 3$

Calculate $\boxed{y_A = \alpha^{X_A} \bmod q}$

$\therefore y_A = 5^3 \bmod 7 = 6$

* Key generation of person 2

Let private key $X_B = 4$

Calculating public key $y_B = \alpha^{X_B} \bmod q = 5^4 \bmod 7 = 2$

Calculate secret key of A

$K_A = y_B^{X_A} \bmod q$

$= 2^3 \bmod 7$

$K_A = 1$

Calculate secret key of B

$K_B = y_A^{X_B} \bmod q$

$= 6^4 \bmod 7$

$K_B = 1$.