R.S.A :- (Rivest - Shamir - Adleman)

→ used to encrypt and decrypt messages.
→ Asymmetric cryptographic algorithm.
→ Two different keys. (public key and private key)
→ A public key is shared publicly and a private key is secret and must not be shared with anyone. (Also known as public key cryptography).
→ used for security services. which enables public key encryption.
→ Range of web browsers, emails, VPNs.
* Increase in key size ⇒ Encryption strength increases.

⟶

• Generating public key :-

① select two prime numbers. P, Q.

Let P = 53, Q = 59.

$n = P * Q = 3127$

→ A small exponent let take e :

→ e should be an integer.
→ not be a factor of n. ⇒ $1 < e < \phi(n)$. (let e=3)

∴ $n = 3127$, $e = 3$.

caution :- (note)
$\gcd(e, \phi(n)) = 1$ ⇒ e, $\phi(n)$ should be co-prime)
if not ⇒ e++

• Generating private key :-

$\phi(n) = (P-1)(Q-1)$

$\phi(n) = 3016$.

private key = d

$d = \frac{((k * \phi(n)) + 1)}{e}$ (for some int k)

if k = 2 ⇒ d = 2011

∴ Now Public key ($n = 3127, e = 3$) | private key ($d = 2011$)

Let encrypt "HI"

$H = 8, I = 9$ ($89 = "HI"$)

encrypted data $c = 89^e \bmod n$,

$\therefore c = 89^3 \bmod 3127$

$\therefore c = 1394$

Now decrypt $c = 1394$.

$\therefore$ decrypted data $= c^d \bmod n$

$\Rightarrow (1394)^{2011} \bmod 3127$

$\Rightarrow 89$

$\therefore 8 = H$ and $I = 9 \Rightarrow$ "HI".

→ RSA keys can be typically 1024 or 2048 bits long. But experts believe that 1024 bit keys could be broken in the near future.