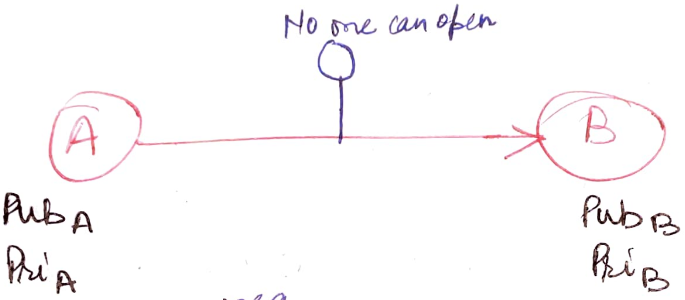
RSA - Algorithm (Public key cryptography)

Stands for Rivest Shamir Adleman. It is used for asymmetric ~~eg~~ cryptography. RSA is a block cipher and can use variable length block sizes. It uses blocks of 64 or 128 bits at a time. It is one of the first public key cryptosystem and is widely used for secure data transmission.

It is used for both public key encryption and digital signatures.



case-1: $Pub_A[\overset{msg}{M}] \longrightarrow \times$ ∵ at B, Pri_A is needed, but it will not there.

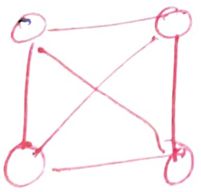
case-2: $Pri_B[M] \longrightarrow \times$ ∵ B's private key lies with B itself

case-3: $Pri_A[M] \longrightarrow \times$ ∵ Pub_A is available to all so anyone can open it in a way.

case-4: $Pub_B[M] \longrightarrow$ ✓ As public key is sharable and it might be broadcasted earlier, so this case is successful.

This is the concept of asymmetric key cryptography.

eg: If four devices are interconnected then how many keys are required.



① symmetric key cryptography - ${}^{n}C_2$ keys required $= {}^{4}C_2 = \frac{4!}{2!\,2!} = \frac{4 \times 3}{2} = 6$

② Asymmetric key cryptography - $2n$, where n is no. of nodes.

Quest: In a RSA cryptosystem, a particular A uses two prime nos $p=13$ and $q=17$ to generate his public and private keys. If the public key of A is 35. Then the private key of A is ________.

option [✓ A) =11] C) 16
B) 13 D) 17

Ans: **Algo is:**

1. choose 2-different large random prime nos.
2. calculate $n = p * q$
3. calculate $\phi(n) = (p-1) \times (q-1)$ e shouldn't be factor of $\phi(n)$
4. choose 'e' such that $1 < e < \phi(n)$
   and 'e' is coprime to $\phi(n)$, means $gcd(e, \phi(n)) = 1$
5. Calculate d, such that $d.e \equiv 1 \bmod \phi(n)$
6. Public key 'e', Private key 'd'.

Here, pubkey $= 35$, $d = ?$, $p = 13$, $q = 17$

Now, $n = p.q = 13.17 = 221$.

and $\phi(n) = 12.16 = 192$.

Now $1 < e < 192$, e is coprime to 192, means $gcd(e, 192) = 1$

given, $e = 35$
then $gcd(35, 192) = 1$ { using eulerian theorem
euclid. theorem.

Now $\underset{\text{congruent}}{d.e \equiv 1 \bmod \phi(n)}$ or $d.e \bmod \phi(n) = 1$

or, $d * 35 \bmod 192 = 1$
Now use, hit & trial method from solutions
we get $d = 11$.

can be written as
$de = 1 + K\phi(n)$
$d = \frac{1 + K\phi(n)}{e}$, $k = 0, 1, 2, 3$

when, $k = 0$
$d = \frac{1}{35} = .x$ pt value not considered.

when $k = 1$
$d = \frac{193}{35} = 5.5$ ✗

when $k = 2$
$d = \frac{385}{35} = \boxed{11}$ ✓

⊛ PGP! Pretty Good Privacy:

- It combines both conventional and Public key cryptography.
- During encryption, it first compresses the PT which saves disk space and modem transmission time.
- Compression removes the patterns which may be used by hackers to decrypt the msg.
- So it gives the better resistance to cryptoanalysis.
- It uses one-time only key called session key.
- Session key is a random generated numbers from the random movements of mouse and keystrokes.
- After data encryption the session key is encrypted to recipients public key and transmitted alongwith cipher text to recipient.
- Decryption in PGP works in reverse order. i.e. the recipient's copy of PGP uses private key to recover temporary session key and then cypher text is decrypted using it to get plain text.
- Key length is 128-bit.

⊛ Services in PGP:

It consist of 5-services.

1. Authentication: it is a digital signature scheme with hashing.
2. confidentiality: is maintained using D.Sign. through symmetric block encryption.
3. Compression: to remove pattern, compression is done. using ZIP and decompression using UNZIP.
4. E-mail compatibility! It overcomes the problem of non-correspondence of ASCII characters in encrypted data. PGP uses radix 64 conversion.

5. PGP segmentation: when msg is very long, PGP automatically, blocks into segments. and on receipts, segments are re-assembled before decryption.