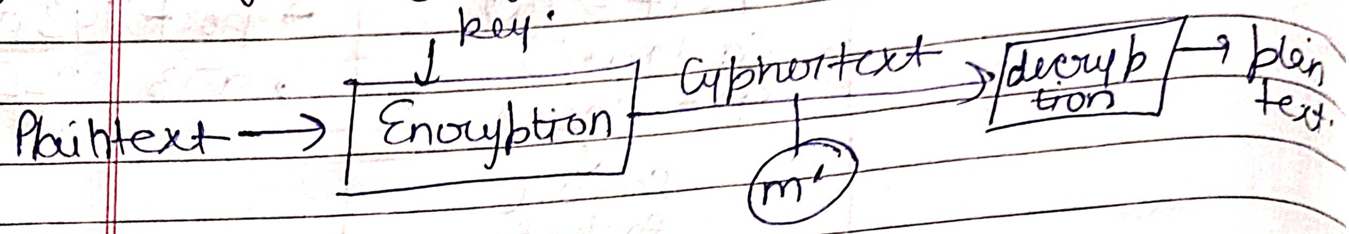
Cryptography →

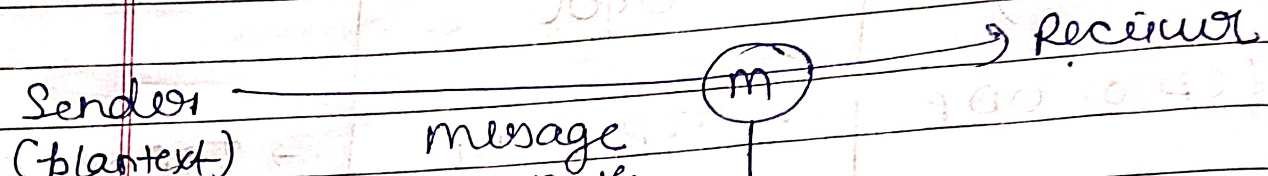
Technqiue which is use to convert plain text to Cipher text or vice versa. to achieve Confidentiality.

Cipher ↓ Secret message

CIA

- Confidentiality
- Integrety
- Availability.





message sent directly without encryption

any hacker can get the message and also can read the message.

Types of keys

Symmetric

if only one key is used for both encrypting and decrypting it is called Symmetric key

Asymmetric

If two different keys are used for encryption and decryption is known as Asymmetric.

Symmetric Key

→ DES   Data Encryption Standard

↓

56 bits

→ 3DES   tripple Data Encryption std.

↓

192 bits

→ AES   Advanced Encryption std

↓

128 bits, 192, 256 bits

$\boxed{2^{56} \text{ \{possible\}}}$

unsecure channel

Sender ———————— Receiver

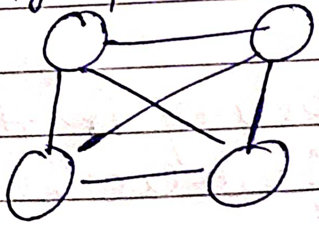
$C = [k, [m]]$ $m = [k, [c]]$

challenge → key exchange (how to give ~~give~~ key to sender to open)

↓

decode.

Q If four devices are connected then how many symmetric key is required.



$$^{n}C_2 = \frac{n(n-1)}{2} \Rightarrow \frac{\cancel{4}^{2}(3)}{\cancel{2}} = 6$$

#Important Question for Network Security

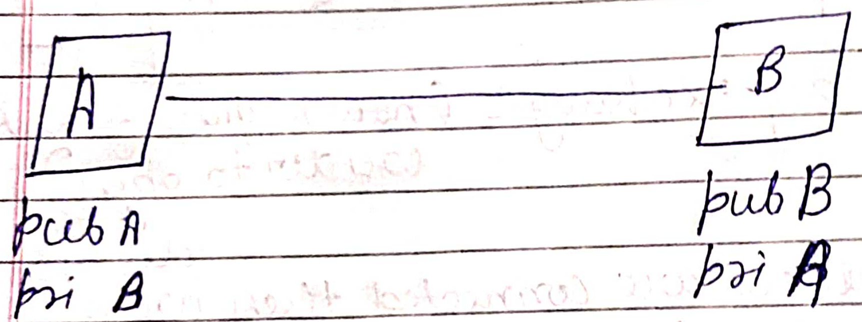
Ques Suppose in group of N people, everyone wants to communicate securely with n-1 others using symmetric and Assymmetric Cryptography. The communication between any two people should not be decodable by othersin group The no of keys required in both cases are?

Solⁿ

Symmetric key	Asymmetric key
$\frac{n(n-1)}{2}$	2N

Asymmetric key

each network has its own private and private key



If we encrypt with private key of A then this code is decrypted by public key of A. or wice versa

C1 $Pub_A[M] \longrightarrow$ X becz A ki pri key A ke pas A B ke ni

C2 $Pri_B[M] \longrightarrow$ X bcz B ki public k B ke paas hai A k

(3 $P_{ri}[m] \longrightarrow$ X   B can decode by using A's public key but vo public sabke pas hai to Encryption hua hi nahi

C4

3. $Pub_B[m] \longrightarrow Priv_B[m]$

for Encryption

keys required for n nodes = 2n.

RSA

In a RSA Cryptosystem a particular A uses two prime no p = 13 and q = 17 to generate his public & private keys. If the public key of A is 35, then the private key of A is

A) 11 B) 13 C) 16 D) 17 .

1. Choose two different large random prime no.
2. Calculate $n = p * q$.
3. Calculate $\phi(n) = (p-1) * (q-1)$
4. Choose 'e' s.t. $1 < e < \phi(n)$
   e is coprime to $\phi(n)$, $gcd(e, \phi(n)) = 1$
5. Calculate d s.t. $de = 1 \equiv 1 \mod \phi(n)$
6. public key 'e'   private key = 'd'

Soln.

1. $p = 13$ $q = 17$
2. $n = 13 \times 17 = 221$
3. $\phi(n) = (p-1) * (q-1) = 12 \times 16 \Rightarrow 192$
4. $e = 35$ $gcd(35, 192) = 1$
5. $de \mod \phi(n) = 1$ $d \times 35 \mod 192 = 1$

put value of d from options and that is answer

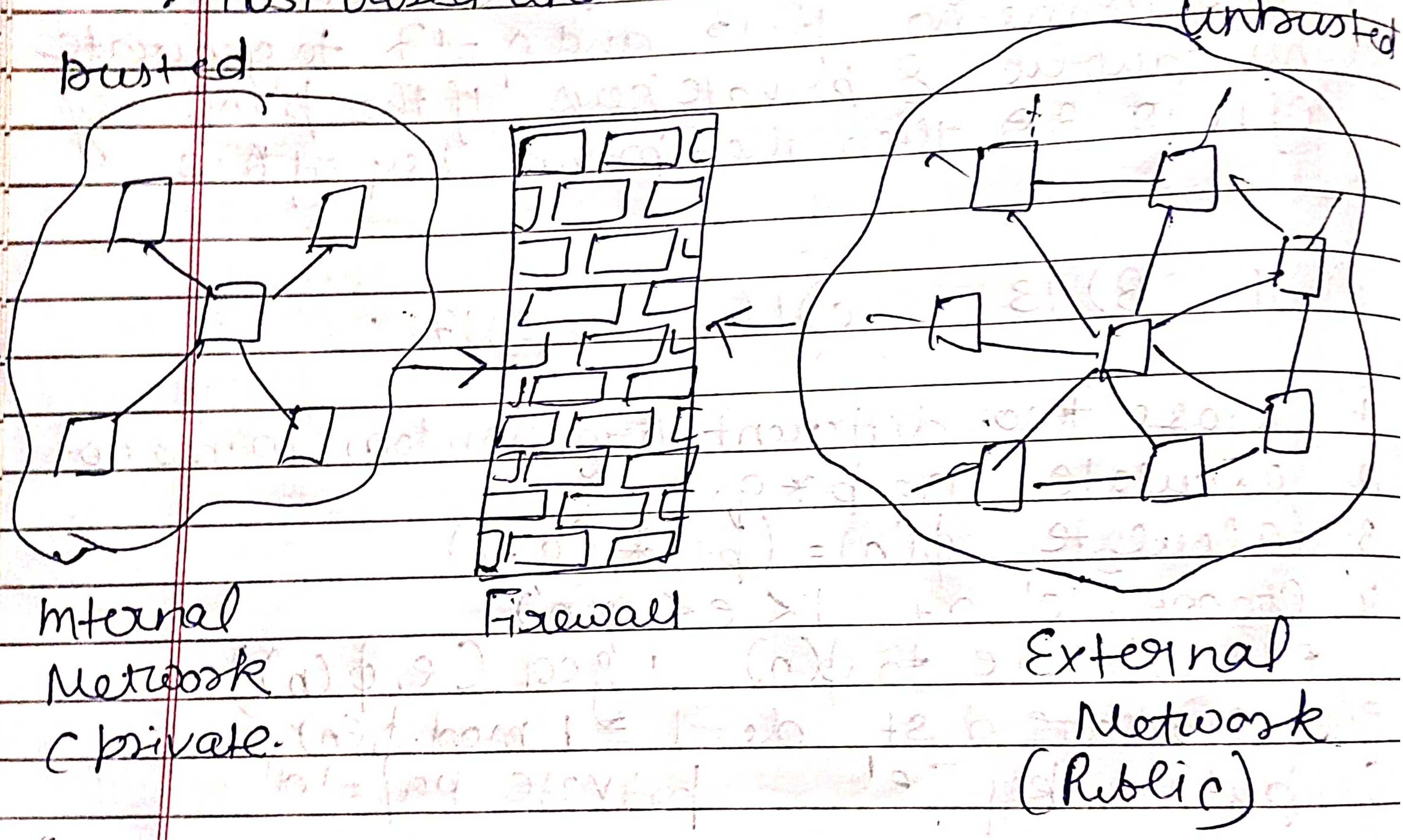
$$\boxed{\begin{aligned} d_0 &= 1 + k\,\phi(n) \\ d &= \frac{1 + k\,\phi(n)}{e} \qquad k = 0, 1, 2, 3, \ldots \end{aligned}}$$

Firewalls < packet filtering firewall / proxy firewall

→ Monitors and Control Incomming and outgoing traffic based on predefined rules.

→ Acts likes a barrier.

→ Host based and Network based Firewall



Packet filtering firewall

→ Check IP header, TCP header

→ works on Network and Transport layer

→ can block IP address, full Network

→ can block a service (http, ftp etc)

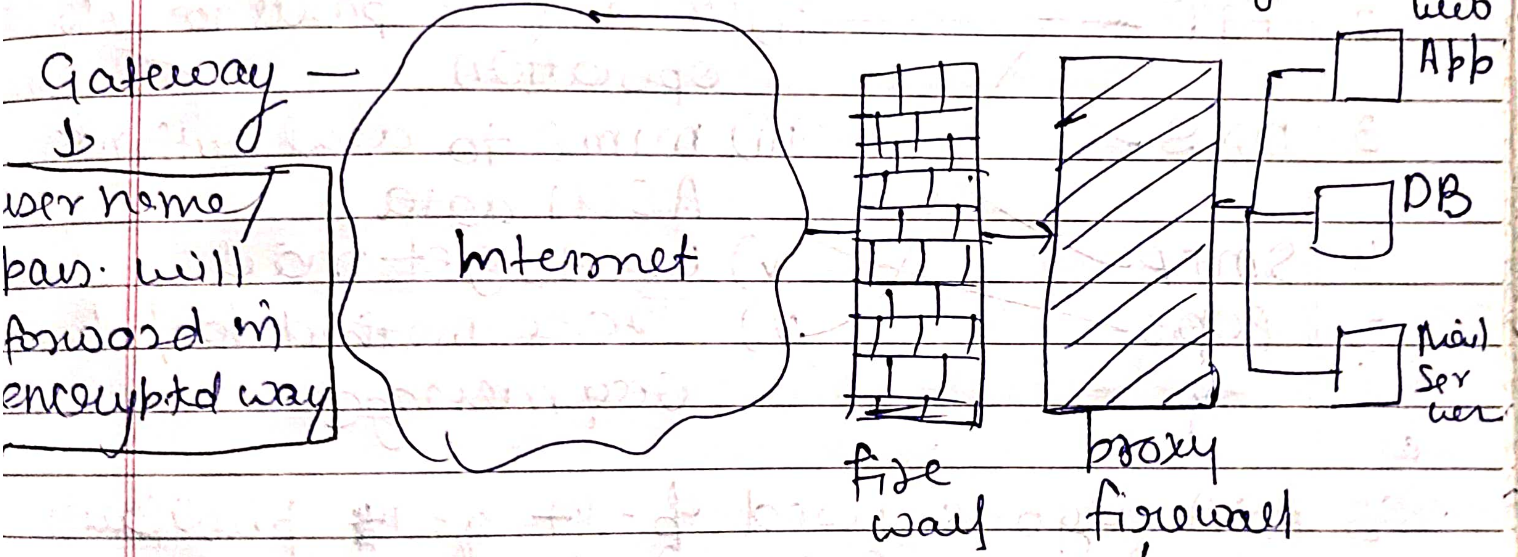
Rules. (These rules in tables are blocked else are alowed)

Rule No	Source IP	Source port	Destination ID	Dest Port
1	179.2.4.80	Any	Any	Any
2	152.32.0.0	Any	Any	Any
3.	Any	Any	72.9.0.3	Any
4	Any	80	Any	Any
5.	Any	Any	Any	21

Abblication/ broxy firewall

→ Monitors and Control incomming & outgoing traffic based on rules

→ Work on Layer 5 Abblication Layer



user name/ pass will forward in encrypted way

it check user id & password and the data that is requested If user is authorised then request will forward else discarded