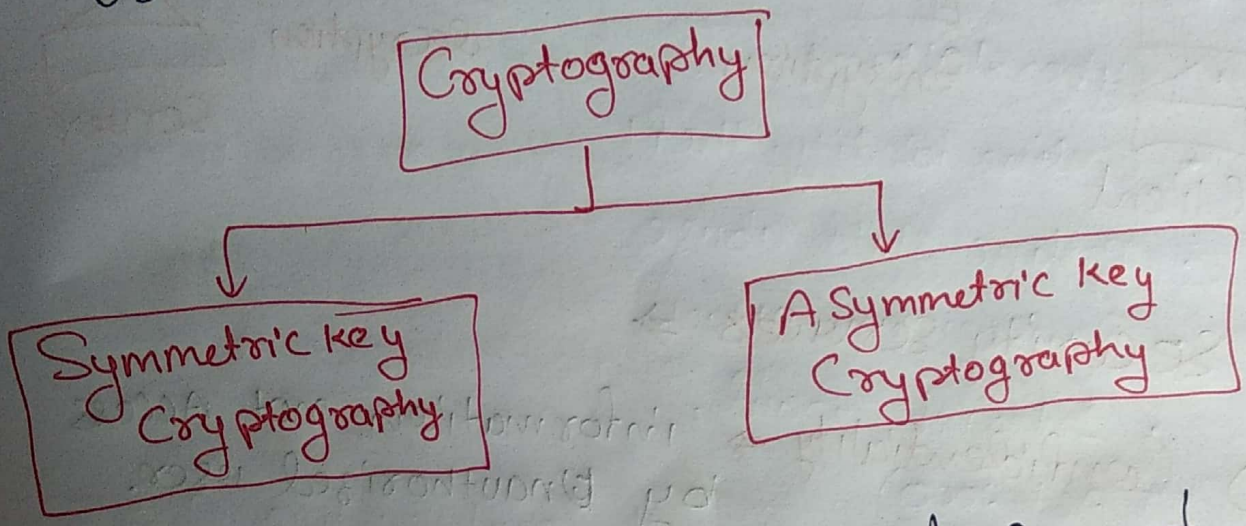
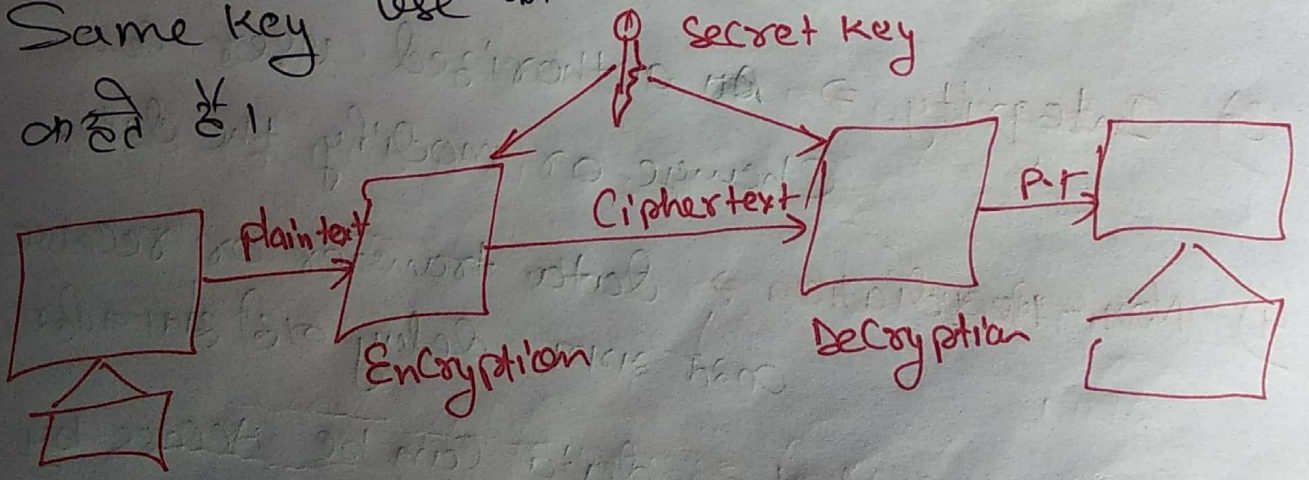
Cryptography & Network Security

Cryptography ⇒ इसकी सहायता से network को secur किया जाता है ताकि unauthorized user data को easily Access नहीं कर सके।

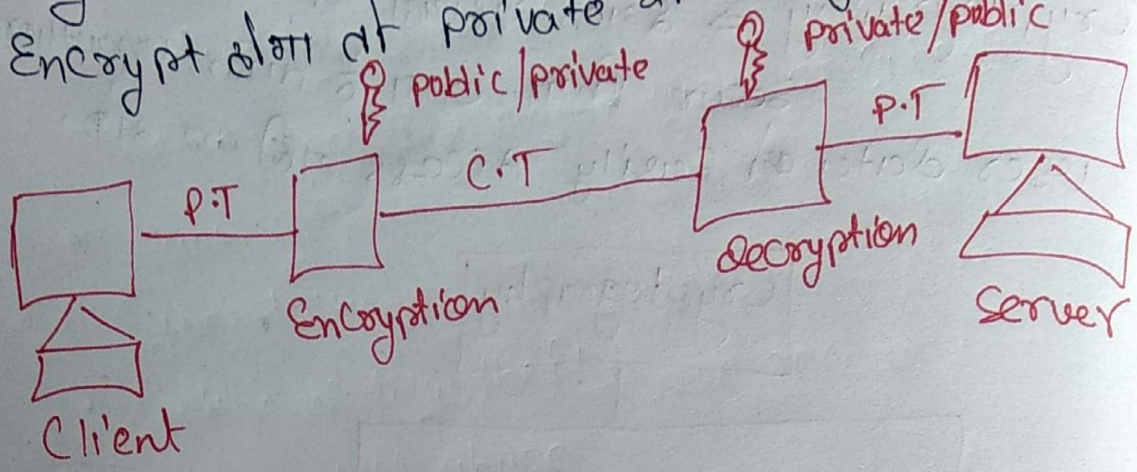


Symmetric key Cryptography ⇒ इसमें data को Send तथा receive करने के लिए secret key use की जाती है जिसे Same key कहते हैं।



Asymmetric ⇒ इसमें दो अलग-अलग key data को Encrypt तथा decrypt करने के लिए किया जाता है। इसे public or private key use की जाती है।

यदि data public key से Encrypt होगा तो private key से decrypt होगा और यदि private key से Encrypt होगा तो private से decrypt होगा।



Security services ⇒

1) Confidentiality ⇒ information not Access by Unauthorized user.

2) Authentication ⇒ data या information को Easily identify किया जाता है।

3) Integrity ⇒ authorized user Can Change or modify the data.

4) Non-Repudiation ⇒ data transfer or receive करते समय delay नहीं होना चाहिए,

5) Access Control ⇒ data Can be Access by the target Computer.

6) Availability ⇒ data authorized party को Easily available होना चाहिए।

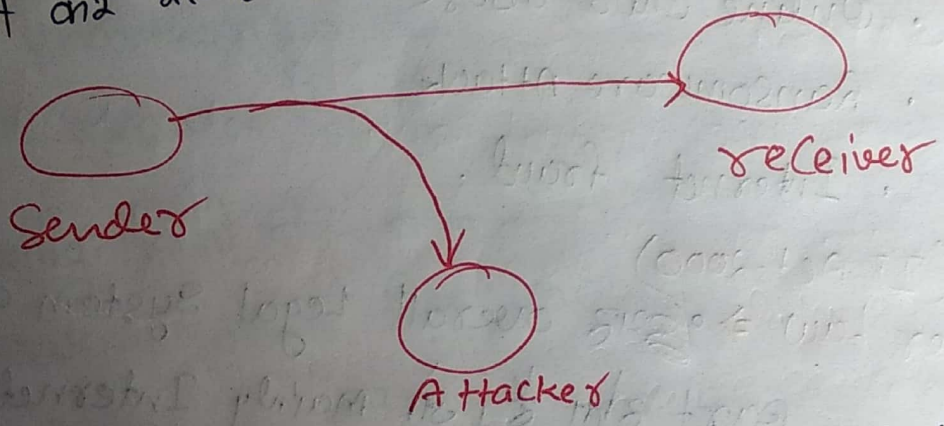
7) Privacy ⇒ network secure.

(2)

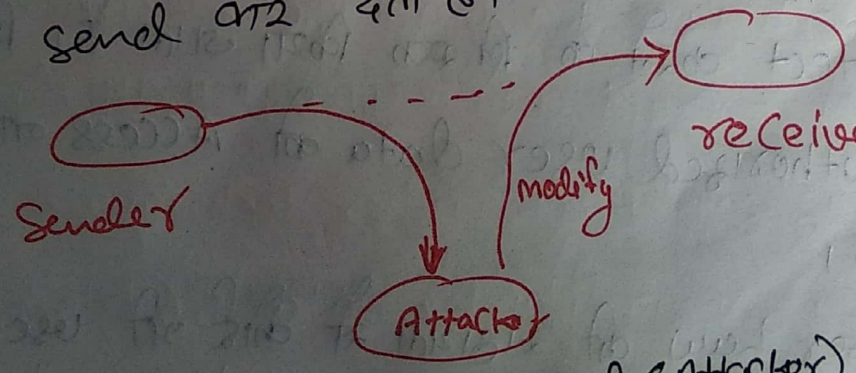
Security Attacks ⇒ security attacks are four types.

Interruption ⇒ इसमें Attacker hardware या Software को remove कर देता है। इसमें Attacker Communication Line पर Attack करता है।

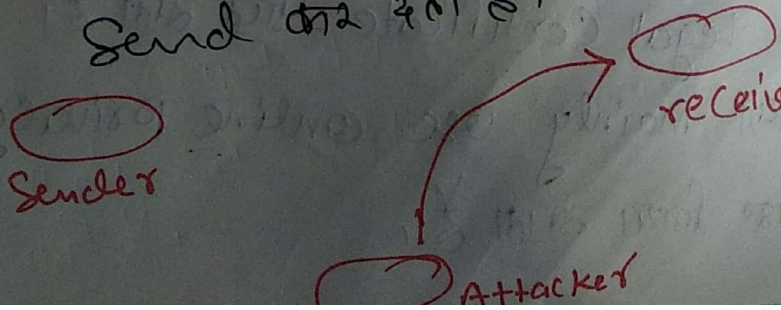
Interception ⇒ इसमें Attacker Communication Line को Access करता है But modify नहीं कर सकता है।



modification ⇒ इसमें Attacker Communication Line को destroy करके modify data receiver को send कर देता है।



fabrication ⇒ इसमें unauthorized (Attacker) data Send कर देता है।



Cybercrime ⇒ यह एक type का Computer Crime जो computer तथा network को distroy करता है।

There are Six major types of Cybercrime.

- Hacking
- Cyberstalking
- Online identity theft
- Online child abuse
- Ransomware Attack
- Internet fraud.

Cyber Law ⇒ (IT Act-2000)

- यह overall Legal System का एक part होता है, जो mainly Internet, Cyber Space तथा Legal issues पर deal करता है।
- Cyber Law का use Internet Crime को protect करने के लिए किया जाता है। जिससे Unauthorized user data को Access न कर सके।
- Cyber Law की सहायता से कोई भी user Online purchase कर सकता है। जिससे उसे एक Legal Certificate प्राप्त होता है।
- इसका mainly use online privacy के लिए किया जाता है।

- IT Act 2000 Cyber law are use in India for focus on information technology.
- IT Act 2000 की सहायता से hacking तथा trojan attacks को Easily remove किया जाता है।

Hacking ⇒ • hacking एक Technique है जिससे unauthorized user Computer तथा network को Access कर लेता है।

- hacking किसी भी system की weakness or network की weakness होती है जिसे unauthorized user Easily Access कर लेता है।
- जो person hacking Activity को perform करता है उसे hacker कहते हैं।
- hacker three types के होते हैं।

1) white hat hacker ⇒ यह ethical hackers होते हैं जो mainly Company के data को Access करते हैं।

2) Black hat hacker ⇒ इनका main focus money को Access करना होता है। he is bad guy.

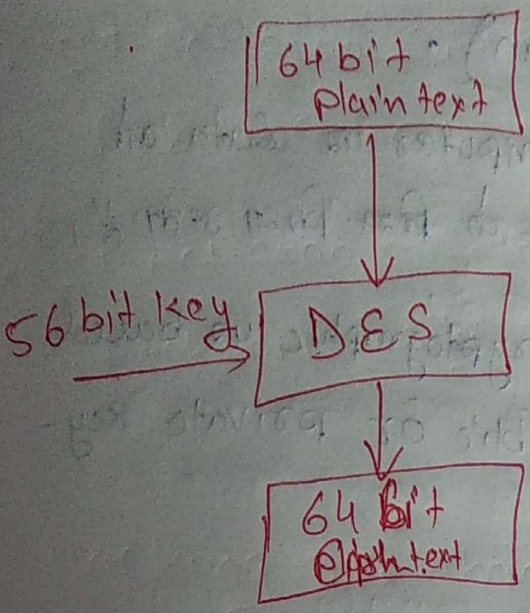
3) grey hat hacker ⇒ यह बिना किसी virus program के ही data को Access कर लेते हैं।

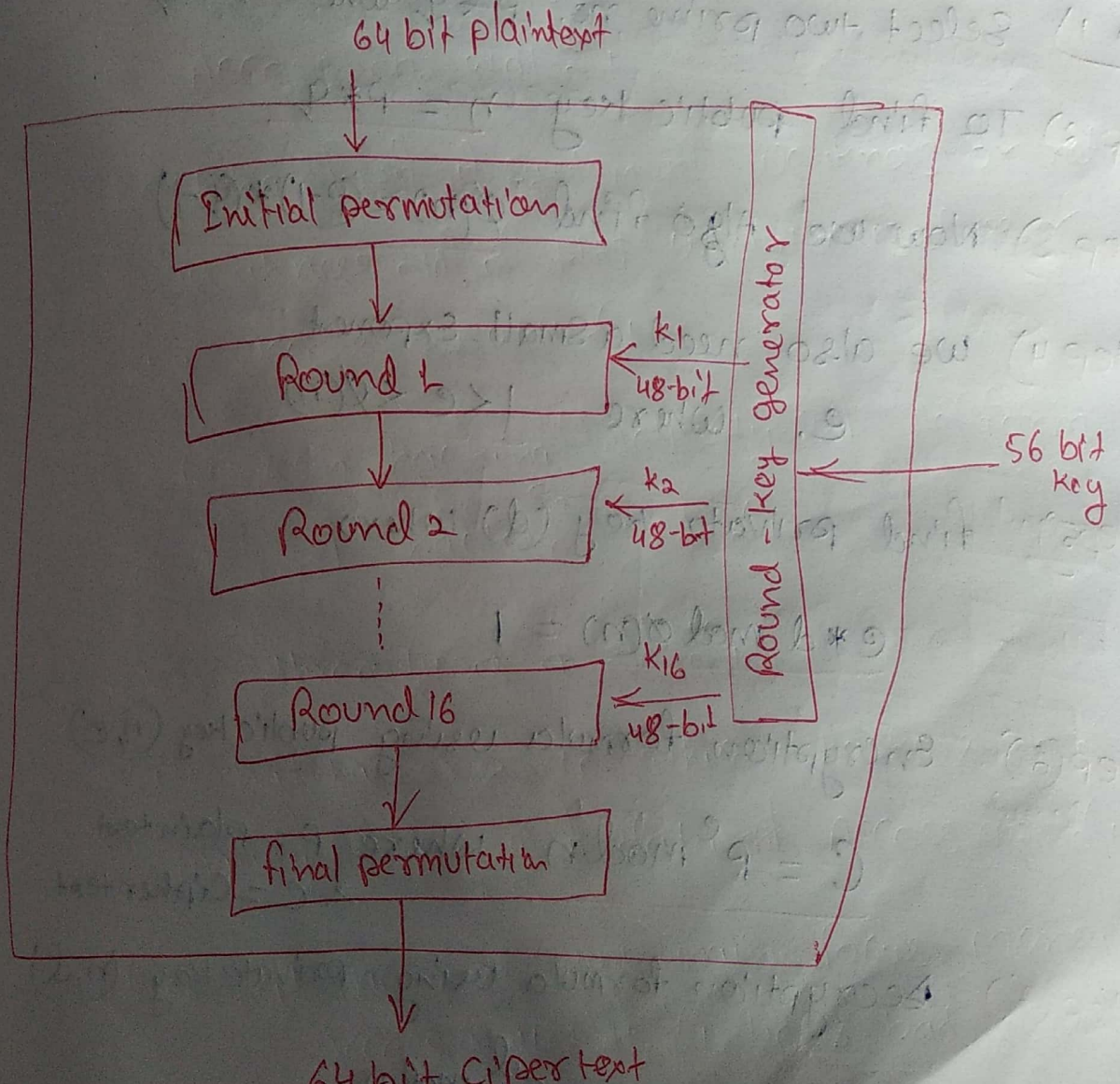
PPTP (Point to point Tunneling protocol) ⇒

- इसकी सहायता से Encrypted data, packet को Securly LAN तथा WAN Network पर Send or Receive किया जाता है,
- PPTP की सहायता से Unsecured network (internet) पर securly data send तथा receive किया जाता है,
- इसका use Virtual Private network (VPN) में securly data को send करने के लिए किया जाता है,

DES ⇒ (Data Encryption standard) ⇒

- यह एक Symmetric-key Encryption Technique है, जिसका use Electronic data को Encrypt करने के लिए किया जाता है,
- यह एक Block Cipher technique है जिसमें 64 bit का plaintex data 56 bits key help से 64 bit Cipher text में Convert होता है,


64 bit plain text
56 bit key
DES
64 bit cipher text


64 bit plaintext
Initial permutation
Round 1
Round 2
Round 16
final permutation
K1
48-bit
K2
48-bit
K16
48-bit
Round - key generator
56 bit key
64 bit Ciper text

DES process

RSA ⇒ (Rivest-Shamir-Adleman).

- इसका use Modern Computer पर data को Encrypt तथा decrypt करने के लिए किया जाता है।
- यह Asymmetric key Cryptographic पर based algorithm है, जिसमे public or private key का use किया जाता है।

Steps ⇒

Step 1) Select two prime no. p & q where p ≠ q

Step 2) To find public key $n = p * q$

Step 3) Now we Algo find $\phi(n) = (p-1) * (q-1)$

Step 4) we also need a small Exponent e. where $1 < e < \phi(n)$

Step 5) find private key (d) where

$$e * d \bmod \phi(n) = 1$$

Step (6) Encryption formula using public key (n, e)

$$C = P^e \bmod n$$ where P = plain text, C = Cipher text

Step (7) Decryption formula using private key (n, d)

$$\text{plain text } (P) = C^d \bmod n$$

Ex ⇒ 1) Choose two prime no. P & q

$p = 3$ & $q = 11$

2) $n = p \times q$

$= 3 \times 11$

$n = 33$

3) find $\phi(n) = (p-1) \times (q-1)$

$= 2 \times 10$

$= 20$

4) find value of e

$1 < e < \phi(n)$

$1 < e < 20$ $\boxed{e = 7}$

5) find d

$e * d \bmod \phi(n) = 1$

$7 \times 3 \bmod 20 = 1$

$\boxed{d = 3}$

6) Encryption $C = P^e \bmod n$

Let $\boxed{P = 2}$ plain text message.

$C = 2^7 \bmod 33 = 29$

7) for decryption $P = C^d \bmod n$

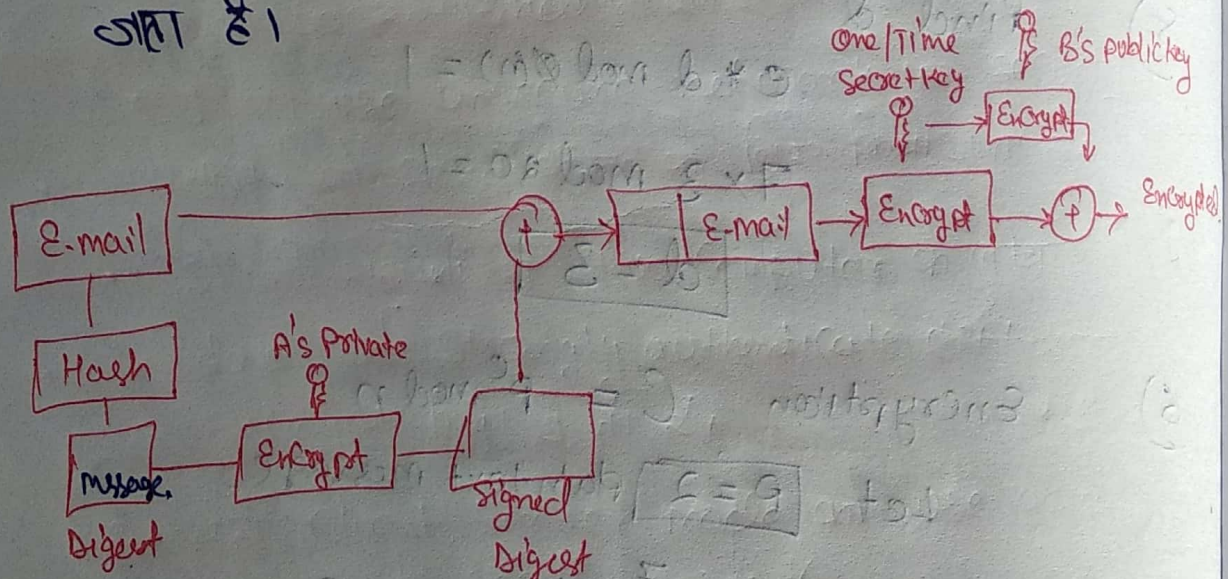
$P = 29^3 \bmod 33$

$\boxed{P = 2}$

$C = 29, P = 2, e = 7, d = 3$

PGP (Pretty Good Privacy) ⇒

- PGP एक opensource तथा freely available SW package है जिसका use Email security security के लिए किया जाता है।
- PGP Digital signature और use करके data को secret key की help से secure करता है।
- PGP network security की privacy, integrity authentication तथा non-repudition को use करके data को secure करता है।
- इसका mainly use E-mail security के लिए किया जाता है।

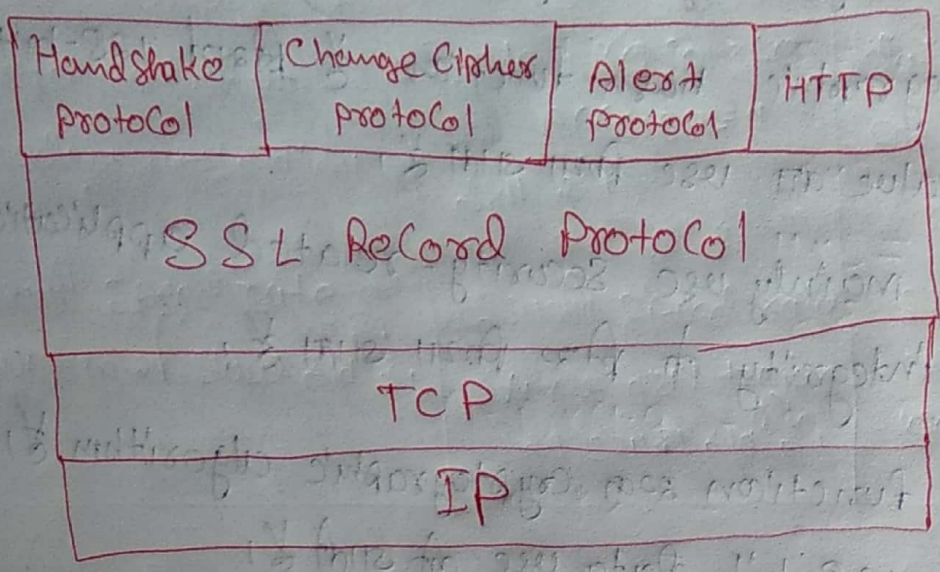


MD5 ⇒ (Message - Digest Algorithms) • यह एक Cryptographic hash function है जिसमें 128-bit hash value का use किया जाता है।

- इसका mainly use security-related application तथा integrity के लिए किया जाता है।
- MD5 function एक cryptographic algorithm है। जिसमें 128 bit data use की जाती है।
- इसे fingerprint security भी कहते है।

SSL ⇒ (Secure Socket Layer) ⇒

- यह एक Transport Layer security है।
- इसका use Computer network security के लिए किया जाता है।
- यह एक Asymmetric key cryptography पर कार्य करता है जिसमें दो key use की जाती है। public or private key.
- SSL का use internet पर securly data को Send तथा receive करने के लिए किया जाता है।
- SSL में privacy, Integrity तथा authentication technique के through data को secure किया जाता है।
-



SSL Layer architecture

SSH ⇒ • इसे Secure shell or Secure Socket shell कहते हैं।

- इसका use unsecure network पर securly data को send करने के लिए किया जाता है।
- इसकी सहायता से two Computer के बीच data को strongly authenticate तथा Encrypt किया जाता है।
- यह Client Server mode को use करके data को secure करता है।
- इसका use ID तथा password security के लिए किया जाता है।

Digital Signature ⇒

- यह एक mathematical technique है जिसका use message, S/w तथा digital document को secure करने के लिए किया जाता है।
- Digital signature एक electronic signature होता है, जिससे यह ज्ञात होता है कि data एक authorized person ने send किया है।
- Digital signature author, date तथा time of signature को Authorized करता है जिससे data securly send or receive किया जाता है।
- यह एक public key Cryptography technique है।

Virus worms & Trojans

Virus

- यह Software तथा Computer program होते हैं जो दूसरे S/w or program के साथ Connect हो जाते हैं तथा Computer को harm पहुचाते हैं।
- यह अपने आप replace हो जाते हैं।
- इसे remotely Control नहीं किया जाता है।

worms

- यह अपने-आप generate होते हैं तथा Computer की processing को slow कर देते हैं।
- यह भी Automatic replace हो जाते हैं।
- इसे remotely Control भी किया जाता है।

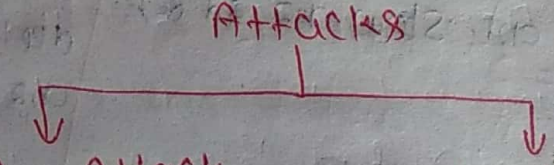
Trojans

- यह Computer System में automatic generate होकर important information तथा data को remove कर देते हैं।
- यह Automatic replace नहीं होते हैं
- इसे भी remotely Control किया जा सकता है।

• इसका main objective information को modify करना होता है,	इसका main objective System resource को Access करना होता है,	इसका main objective data को destroy कर देना होता है,
इसकी speed rate worm से slow होती है,	इसकी speed rate virus तथा trojan से ज्यादा होती है,	इसकी speed rate virus तथा worm से कम होती है,

Computer network Attacks ⇒

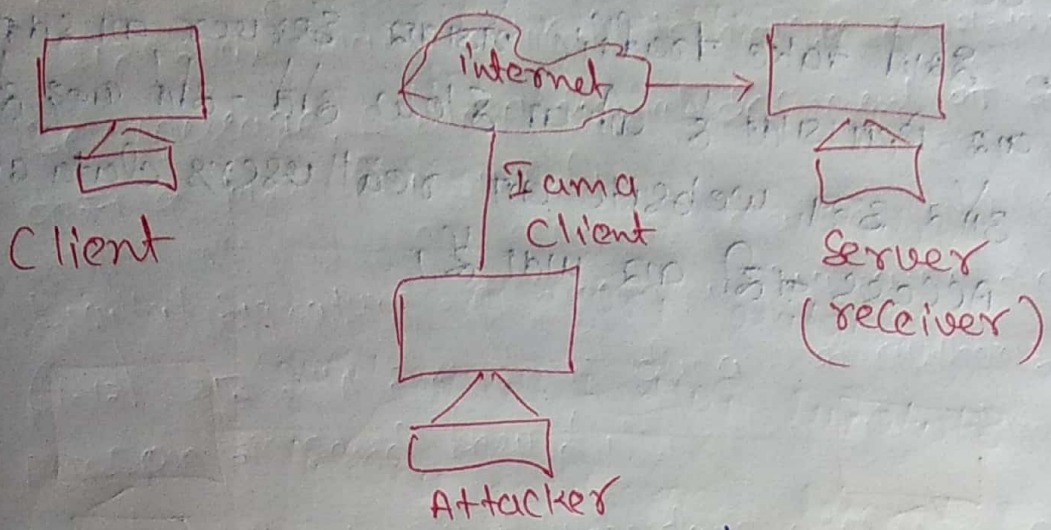
- Attack एक information security threat होती है जिससे data को Access, destroy तथा modify कर दिया जाता है, बीना किसी Authentication के,
- Attack एक process है जिसकी सहायता से data को Access किया जाता है,
- Attack many two types के होते हैं,



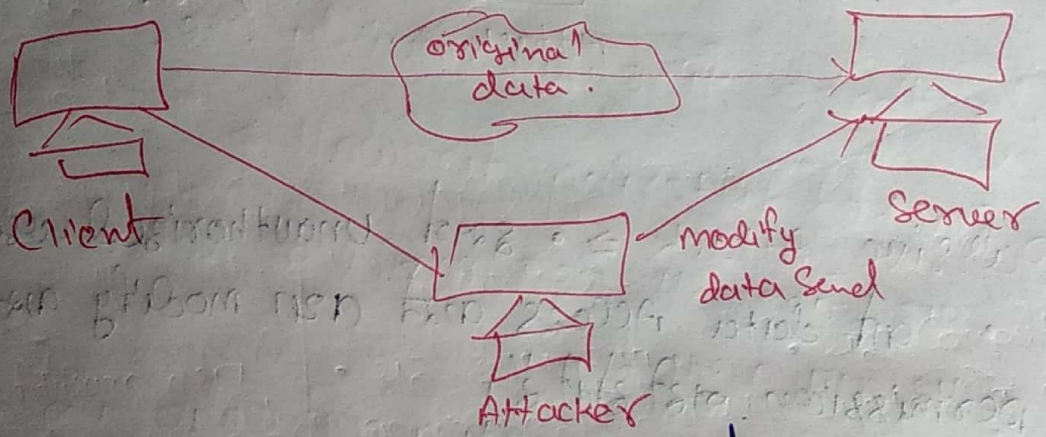
1) Active attack ⇒ इसमें unauthorized user को data को Access तथा modification करने की permission होती है,
यह विभिन्न ways में होता है,

a) Masquerade ⇒ इसमें unauthorized user

as a Client करके data send करता है। (8)

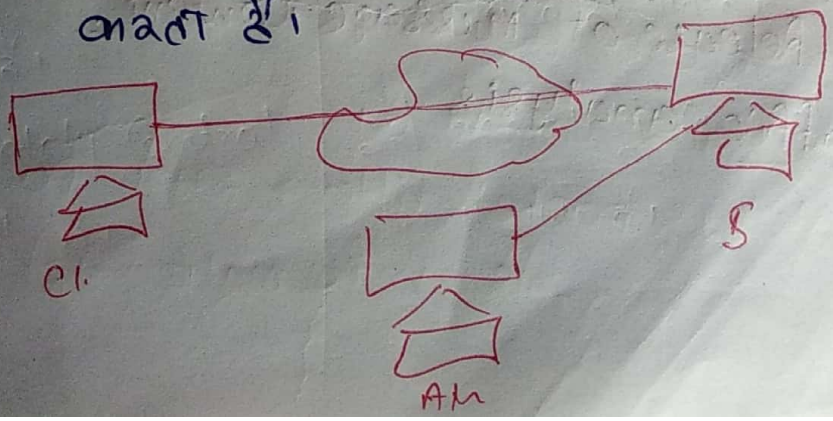


b) modification of message ⇒ इसमें unauthorized user data or information को modify करके server को send कर सकता है।



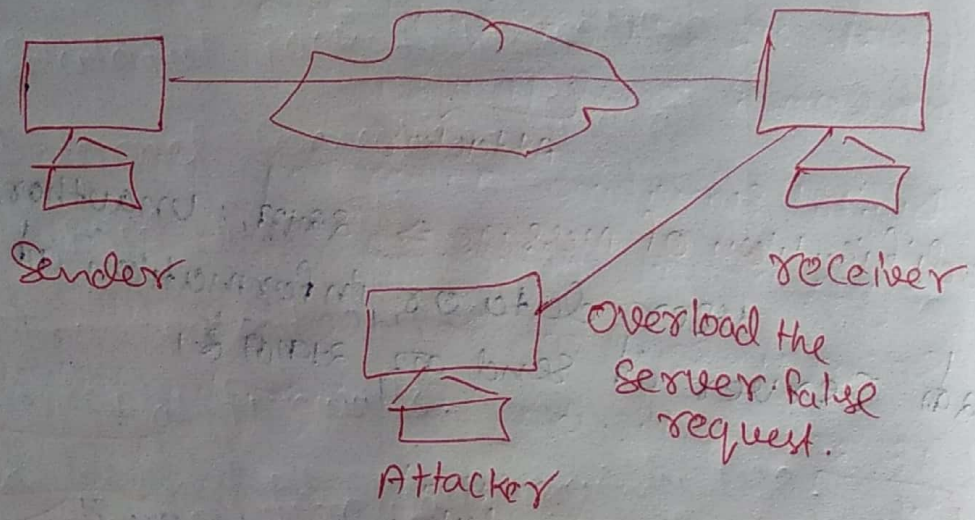
c) Repudiation ⇒ इसमें data को send तथा receive करने में time delay हो जाता है।

d) Replay ⇒ इसमें unauthorized user बीच permissio
के fault data को server पर send
करता है।



e) Denial of Service ⇒ (DOS Attack)

- इसमें fake traffic भेजकर server को इतना Busy कर दिया जाता है की वो slow होते - होते बन्द हो जाता है और उस website का real users data का Access नहीं कर पाता है।



2) Passive Attack ⇒ • इसमें unauthorized user का data Access करने तथा modify करने की permission नहीं होती है।

- इसमें Unauthorized हो System को monitor करता है। वह message तथा information जो हो System के मध्य transmit हो रही है उसे monitor करता है but Change नहीं कर सकता है,

Types ⇒

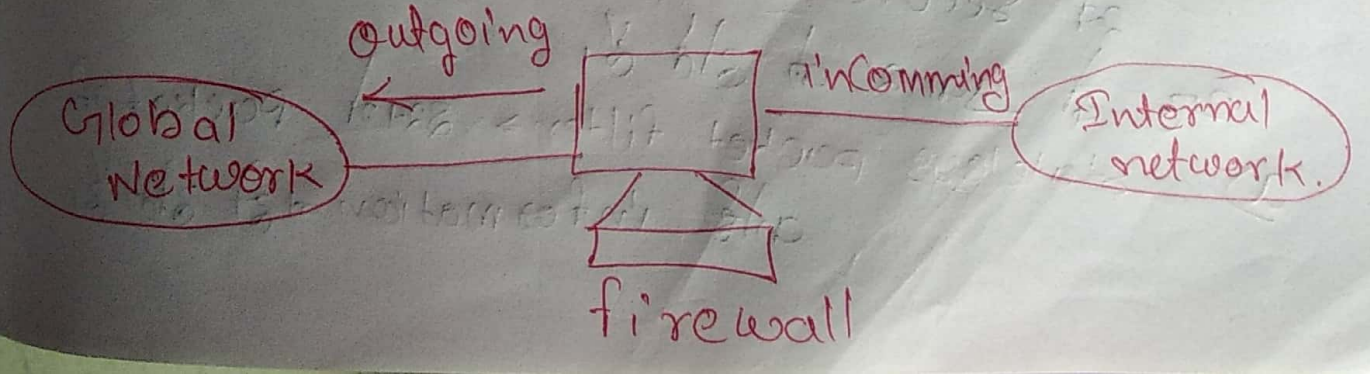
a) The Release of message Content.

b) traffic analysis

backdoor ⇒ • एक एक malware (virus) है। जो authentication process को destroy करके access करने की कोशिश करता है।
• यह किसी भी S/w के background पर कार्य करता है जो user से hides होता है।

firewall

• firewall एक network security system होता है जो Computer System पर incoming तथा outgoing network traffic को control करता है।
• firewall को trusted internal network तथा untrusted External network (internet) के बीच एक barrier की तरह ~~के~~ Established किया जाता है। ताकि data securely send or receive हो सके.
• यह एक network security device होता है, जो hardware or S/w based भी रूप में incomming or outgoing network को control करता है।
• firewall की सहायता से private network को unauthorized access से secure किया जाता है।



There are different types of firewall

1) Packet filtering firewall
2) Circuit Gatways
3) Application Level proxy
4) Adaptive Proxies
5) Stateful Packet Inspection
6) Internet Connection firewall
7) Mybrid firewall
8) Transparent firewall
9) Virtual firewalls.

only three firewall mainly use.

1) packet filtering firewall ⇒

- यह firewall OSI model की Network layer पर कार्य करता है।
- यह firewall incomming तथा outgoing packets को analyze करता है।
- यह केवल उन्हीं packets को आगे जाने देता है, जो firewall policy को follow करते हैं।
- इसकी सहायता से private network को Attacker से secure किया जाता है।

यह दो प्रकार के होते हैं।

a) Stateless packet filter ⇒ इसमें Packet की कोई information नहीं होती है।

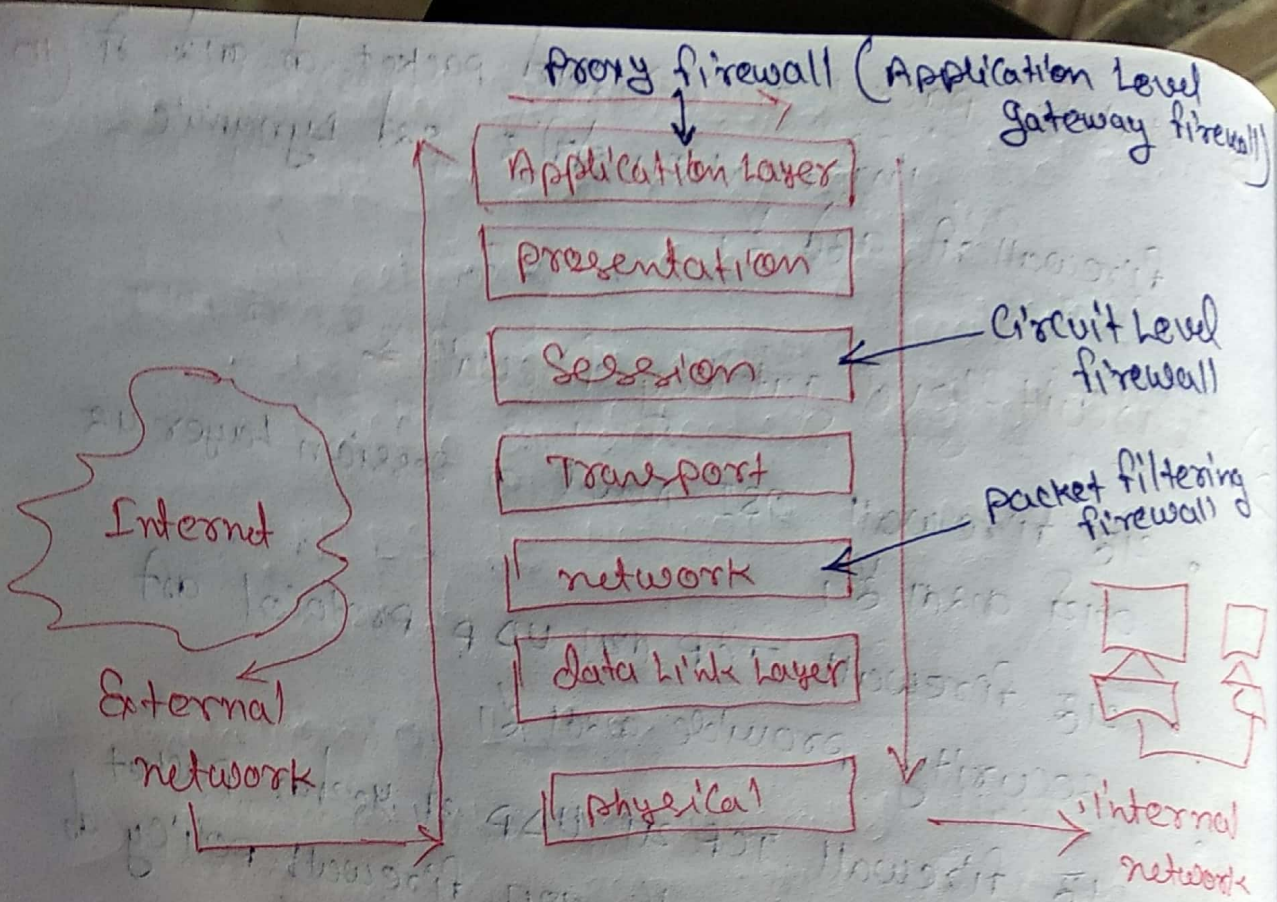
b) Stateful packet filter ⇒ इसमें packet के बारे में information होती है। इसे Dynamic firewall भी कहते हैं।

2) Circuit-Level gateway firewall ⇒

- यह firewall OSI model के session Layer पर कार्य करता है।
- यह firewall TCP तथा UDP protocol की security provide करता है।
- यह firewall TCP या UDP में प्रत्येक packet का Analysis करता है, तथा firewall policy के According action perform करता है।
- इसमें एक Time पर एक से ज्यादा packet send or receive किये जा सकते हैं।

3) Application Gateway firewall ⇒

- इसे Application proxy भी कहते हैं।
- इसका use OSI model की Application Layer पर किया जाता है।
- यह firewall Application की information के According package के आगे से गुजरने देता है या पीछे का रोक देता है।
- यह एक type का proxy server है जो Securly packet को incomming or Outgoing पूरा करता है।



Access Control policies ⇒

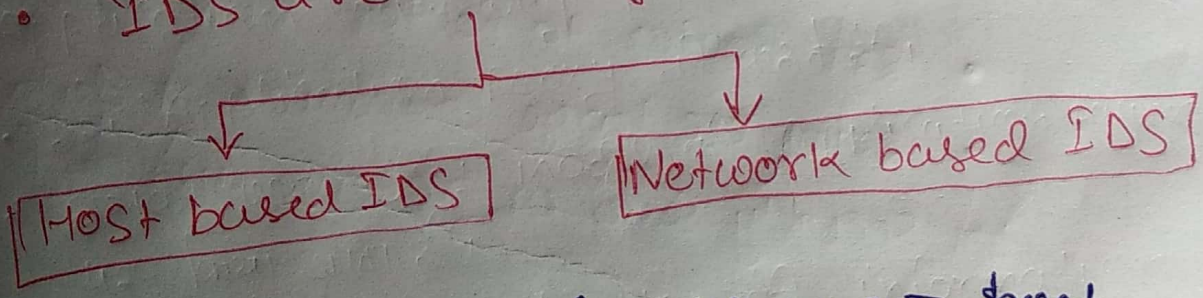
- यह 2nd Electronic Security Technique है। जिसकी help से many Application का Control किया जाता है।
- यह दो प्रकार का होता है।

1) Physical Access Control ⇒ इसको use Building Campus, physical ID से किया जाता है।

2) Logical Access Control ⇒ इसका use Computer Connection, files का data Access करने के लिए किया जाता है।

IDS (Instrusion Detection System) ⇒

- यह एक type का security Software है।
- इसका use System तथा Network को unwanted तथा unauthorized access से safe करना होता है।
- यह hacker, attacker तथा अन्य attackers से System को safe करता है।
- इसका use network तथा System में instrusions को detect करने के लिए किया जाता है और ही को instrusions मिलता है तो यह System or network को alert कर देता है।
- इसका प्रयोग विभिन्न तरीके से malicious traffic को Control करने के लिए किया जाता है।
- IDS are two types



1) Host based IDS ⇒ (HIDS) ⇒ • यह Host Computer पर install होता है।
- यह केवल उस traffic को Control करता है। जो host द्वारा design होता है या जो host से होकर गुजरता है।
- यदि कोई malicious activity दिखाई देती है तो यह उसे detect करता है।

2) Network based IDS (NIDS) ⇒

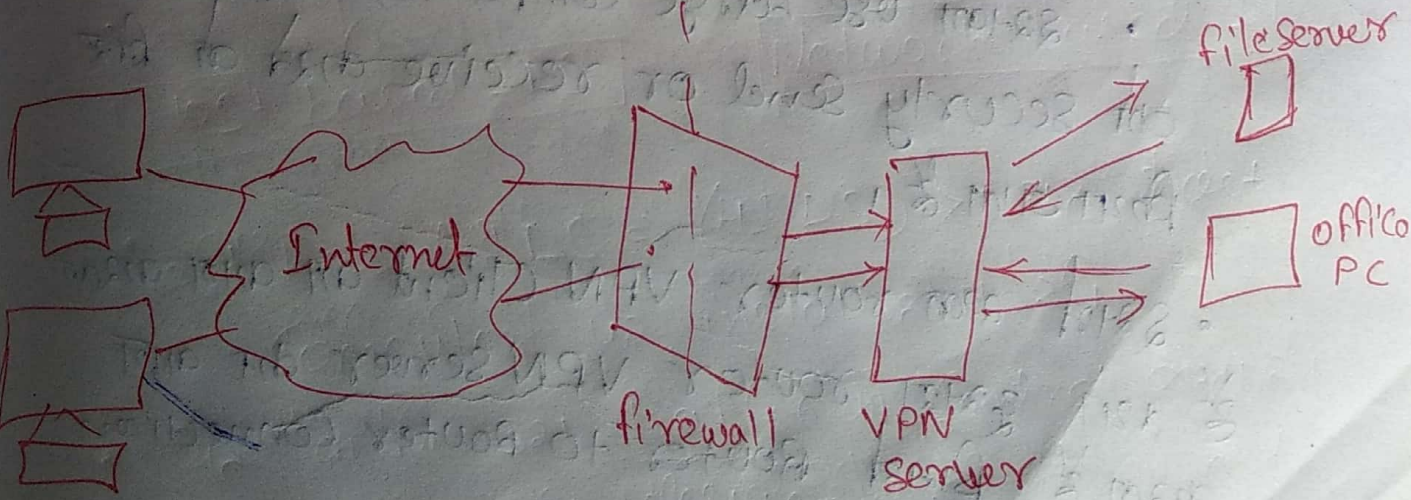
- यह उस सभी hosts का control करता है, जो network में create होते हैं,
- यह network में होने वाले malicious traffic का detector control करता है,
- NIDS पूरे Network का monitor करता है,

Limitation of IDS ⇒

1) many Attacks are generated
2) Noise can effect IDS
3) Encrypted packet are not processed by most IDS.
4) It's difficult to measure and adjust.

VPN (Virtual private Network)

- यह एक तरह का Network है जिसका use private network (wifi or hotspot) को secure करने के लिए किया जाता है।
- इसका सहायता से user अपने personal data को hacker से secure करके कहीं भी send कर सकता है।
- VPN एक technology है, जिसकी सहायता से Less secure network (internet) को safe तथा encrypted connection provide किया जाता है।
- VPN की सहायता से private network पर as a public network का तरह work किया जाता है।
- VPN tunneling protocols का create करके secure connection provide करता है।



VPN are two types

- Remote Access VPN
- Site to Site VPN

1) Remote Access VPN ⇒

- इसमें user private network की services तथा resources को remotely Access करता है।
- इसमें user तथा private network के बीच Connection Secure तथा private होता है।
- यह Business user तथा Home user दोनों के लिए useful होता है।

2) Site to Site VPN ⇒

- इसे Router to Router VPN भी कहते हैं।
- इसका use large Companies में data को securly Send or receive करने के लिए किया जाता है।
- इसमें एक router VPN Client का काम करता है तथा दूसरा router VPN Server का काम करता है जिससे Router to Router Connection होता है।

It's two types.

1) Intranet based VPN 2) Extranet Based VPN

VPN protocols ⇒

1) IPSec (Internet Protocol Security)
2) L2TP (Layer 2 Tunneling protocol)
3) Point-to-Point Tunneling Protocol (PPTP)
4) SSL and TLS [(secure Socket Layer) and (Transport Layer Security)]
5) SSH (secure shell)

Key Exchange in VPN ⇒

- Internet Key Exchange (IKE) एक standard method है, जिसकी सहायता से secure, authenticate communication create किया जाता है।
- यह VPN के IPSec (Internet Protocol Security) का भाग होता है।
- Key Exchange एक secure connection provide करता है।