★ Stream Ciphers.

Advantage ① Fast speed

Disadvantage
① less security
② Not widely used.

② Size of plaintext = size of ciphertext.

① perform operation only on bits of message by performing XOR of the message with generated key.

Ciphertext = M ⊕ key generated.

Eg
$$\begin{array}{r} 1\,0\,0\,1\,1\,1\,0\,0\,1 \rightarrow M \\ 0\,1\,0\,1\,0\,1\,1\,1\,0\,0 \rightarrow k \\ \hline 1\,0\,0\,0\,1\,1\,0\,0\,1\,0\,1 \rightarrow C \end{array}$$ } sender.

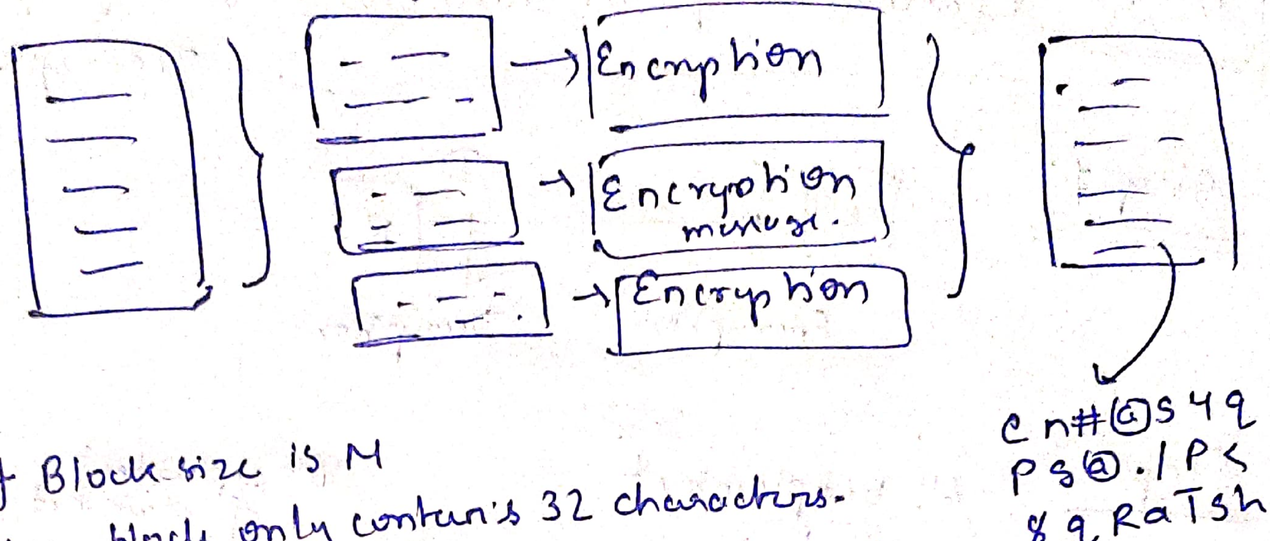
must be same

$$\begin{array}{r} 1\,0\,0\,0\,1\,1\,0\,0\,1\,0\,1 \rightarrow C \\ 0\,1\,0\,1\,0\,1\,1\,1\,0\,0 \rightarrow k. \\ \hline 1\,1\,0\,0\,1\,1\,1\,0\,0\,1 \rightarrow P/M \end{array}$$

★ Block Ciphers.

Message to send is divided into blocks & Then message blocks are of equal size and Then, encryption is performed of those message blocks.

Block.



① If Block size is N
then each block only contain's 32 characters.

② If any blocks have less than N characters
then padding is performed.

③ padding simply Refer's to adding temporary information.
to Blocks that contain's less N characters.

Eg
- DES (Data Encryption Standard)
- AES (Advanced Encryption standard)

Advantage

① Most commonly used technique.
② High security.

Dissadvantage

① Require More time
i.e. ~~low~~ speed
less encryption

Similarities

Stream & block
① Both are Symmetric Encryption method.
② used for converting plaintext → ciphertext

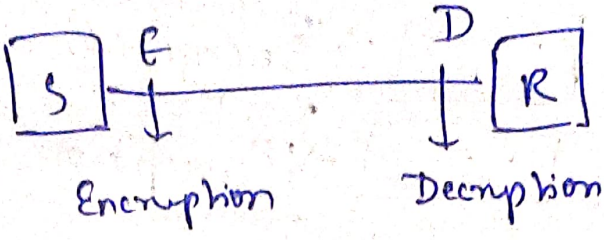
Difference

Stream cipher	block cipher.
① converts message in cipher text by using every 1 bit of ~~the~~ at a time.	① converts message in cipher text by dividing message into equal size blocks.
② uses 8 bits. message	② generally uses 64 or more than 64 bit message.
③ keylength = 256 bits.	③ key length 128 or 256
④ less secure.	④ more secure → conversion.
⑤ fast calculation Speed	⑤ slow calculation speed

DES (Data Encryption Standard)

used for plaintext Decryption.

Step 1:

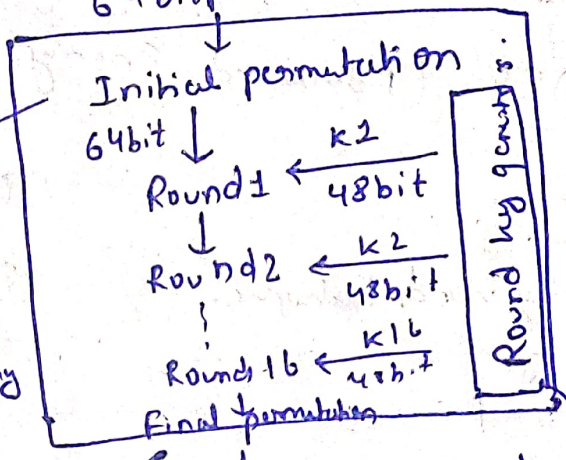


Step 2:

64 bit plaintext → DES cipher. → 64 bit ciphertext

64 ~~ciphertext~~ plaintext. ← DES reverse cipher ← 64 bit ciphertext

Step 3: Inside DES Cipher.

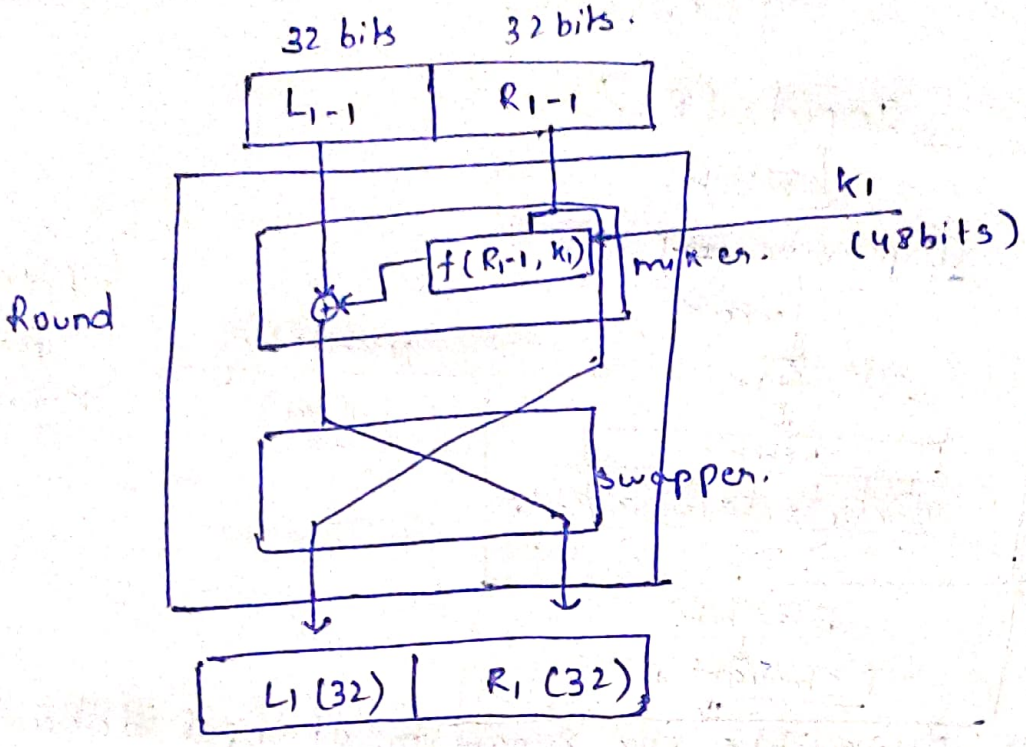


① Initial permutation will decide the position of bits in plaintext.
② simply perform shifting of plain bits.

① Final permutation is just opposite of initial permutation & perform function in just Reverse order.

Responsible for generation of 48 bit key. Which is used by Round 1.

Step4: Inside Round function.



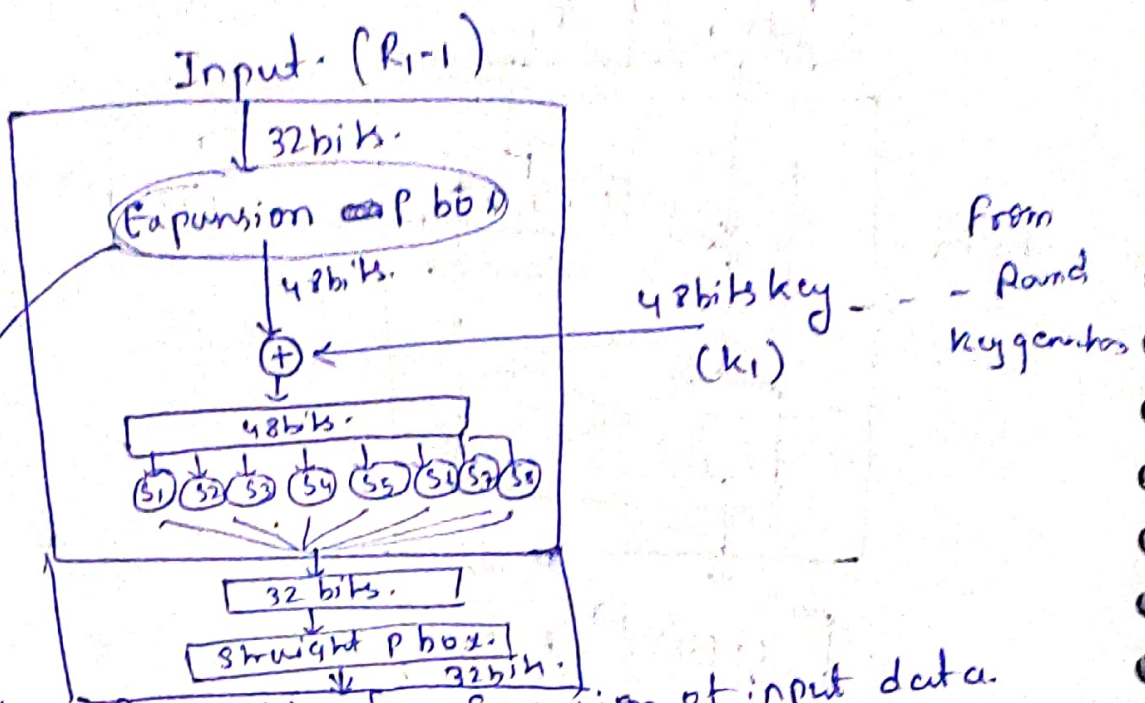
$f(R_{i-1}, K_i)$ ⇒ also know DES function that accepts a key from Round key generate ie (48bits length) & 32bit from previous Round ie, R_{i-1}.

This function responsible for converting 48bit key & 32bit input into 32 bits output so that XOR operation can be performed blw output $(f(R_{i-1}, K_i) \oplus L_{i-1}$

Swapper. ⇒ Swapper is Responsible for swapping output $[L_{i-1} \oplus f(R_{i-1}, K_i)]$ and R_{i-1} each of 32bit and again convert them into 64 bit data for nex Round.

Step 5: Inside DES round function

$f(R_{i-1}, k_i)$

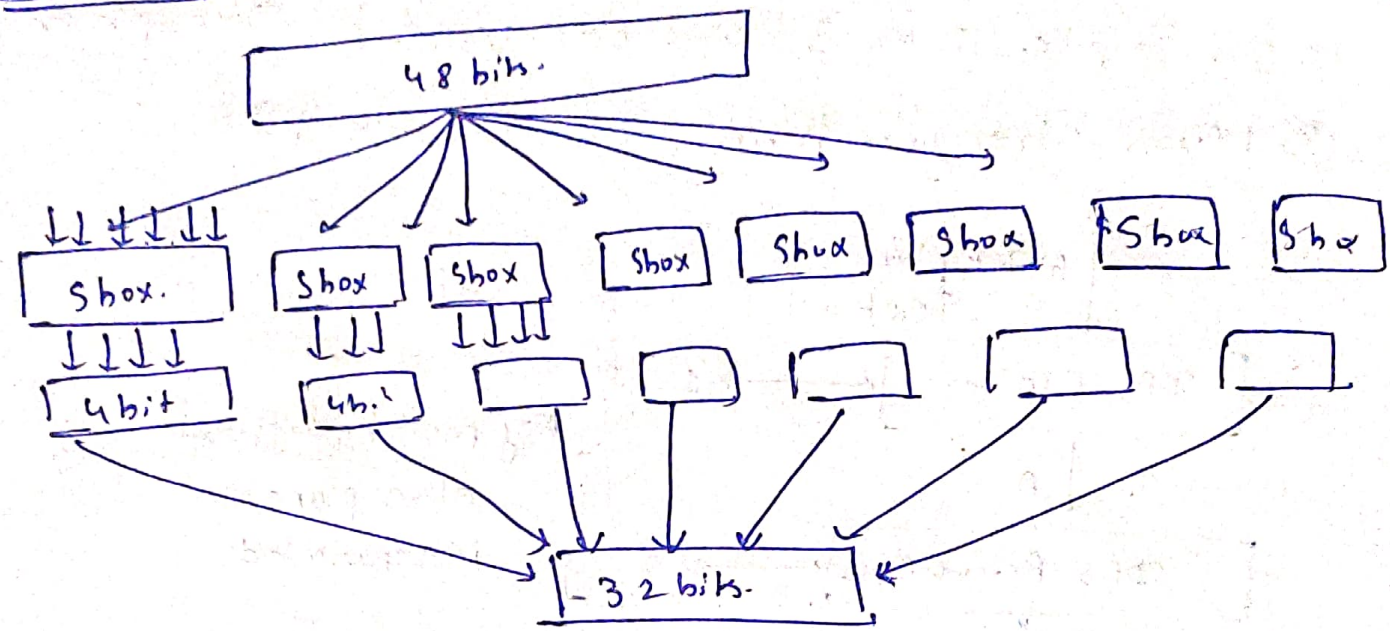


(a) Expansion Pbox: Responsible for expansion of input data. In which some bits of input data is repeated and convert into 64 bits data. This done because to perform ⊕ operation in further stages. b/w output (Expansion p box) ⊕ 48 bit key from Round key generator.

(b) Now output of ~~Sbox~~ ~~given~~ XOR operation given to the S box that will convert 48 bit input into 32 bit output, that contain smaller s function and responsible 48 bit $\longrightarrow$ 32 bit data.

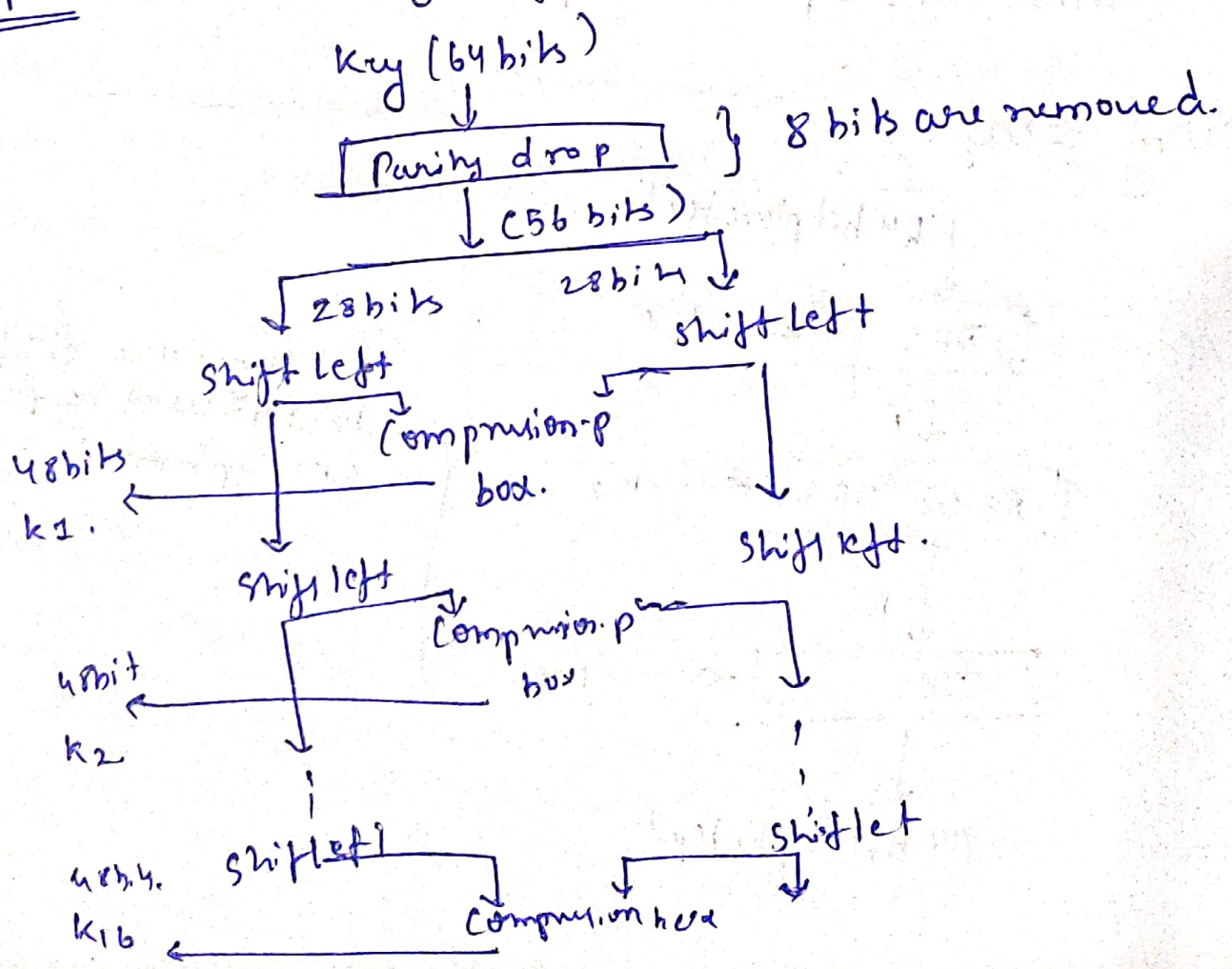
(c) Straight pbox: Now Straight p box will perform Suffling of data. I/p for the pbox is 32 bits & output is also 32 bits.

Step-6: S - Box.



Each Sbox will get input as 6 bits that are converted to 4 bits using an predefined algorithm.
Now, 4 bits output from each small Sbox is combined as 32 bits.

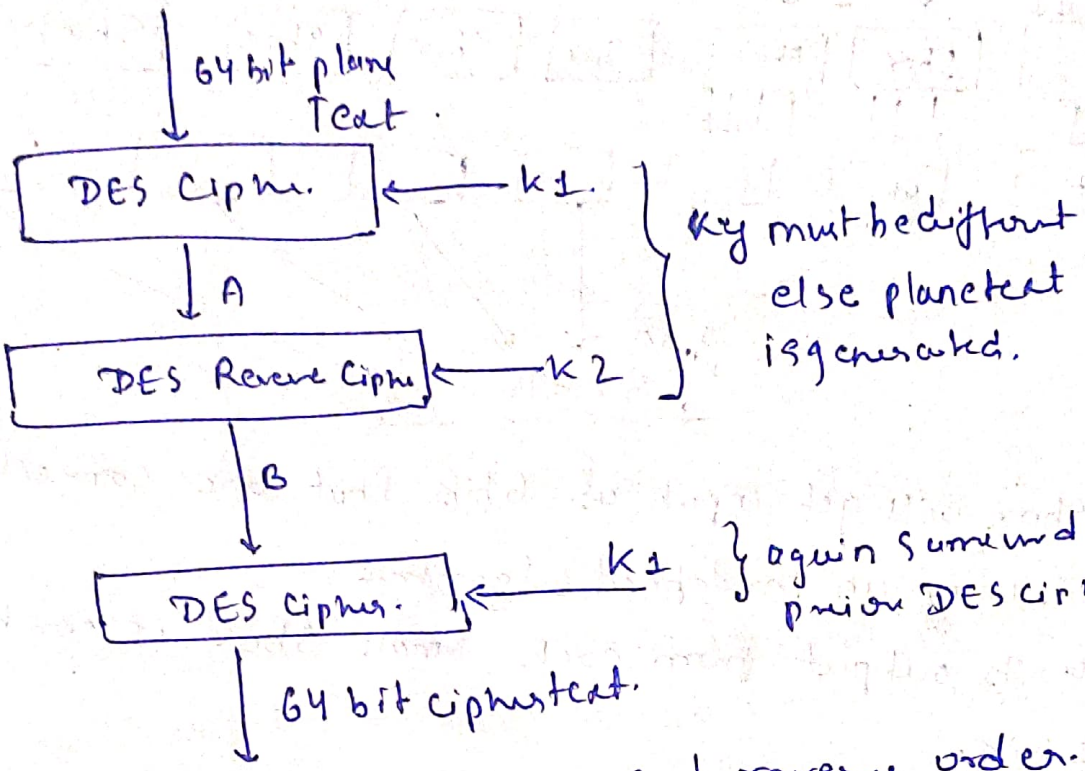
Step-7 How round key is generated.



Triple DES

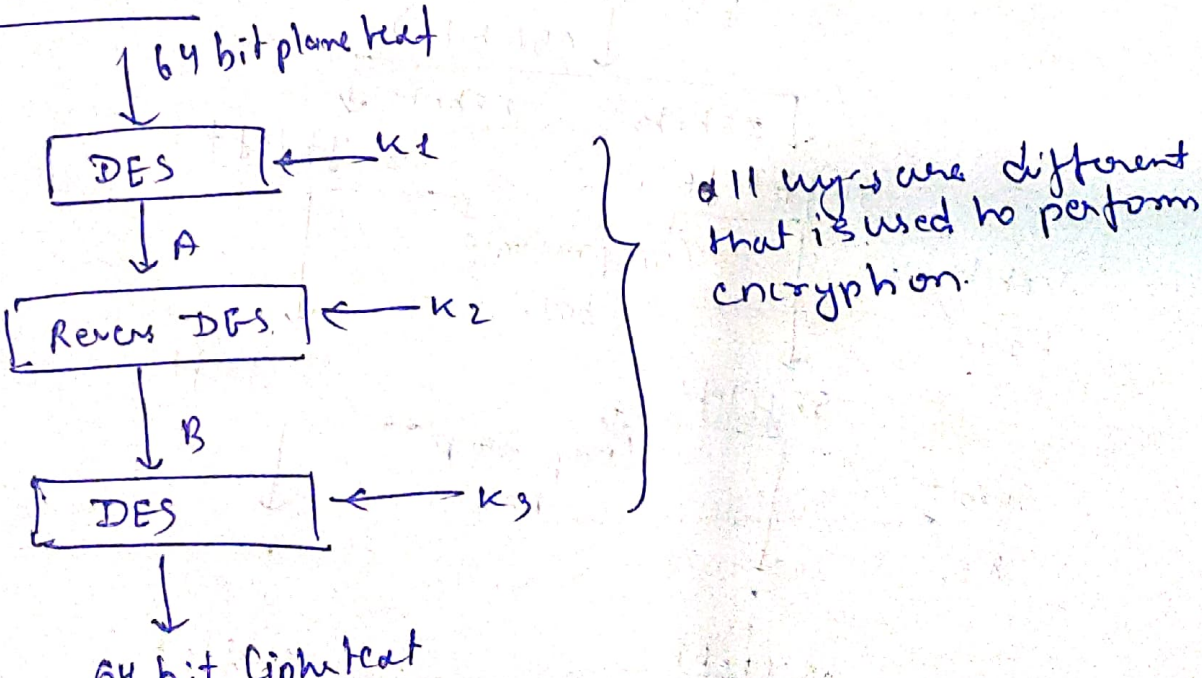
(1) In Triple 2 or 3 keys are used for Decryption

(2) Much stronger than DES, double DES.



(3) Decryption is performed in just reverse order.
when DES ciphr is replaced ⟷ reverse DES ciphr and vice versa.

Using 3 keys.



★ AES (Advanced Encryption Standard)

① Symmetric key block cipher → Same key for encryption + decryption

② Fixed block size = 128 bits

③ More secured than DES

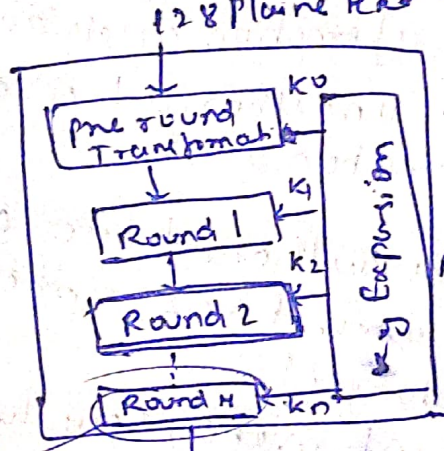
Round	no. of bits key.
10	128
12	192
14	256

④ Depending upon key size changes. Round.

∴ 1 word = 32 bits = 4 byte.

⑤ for each N rounds N+1 keys generated.

Step 1:



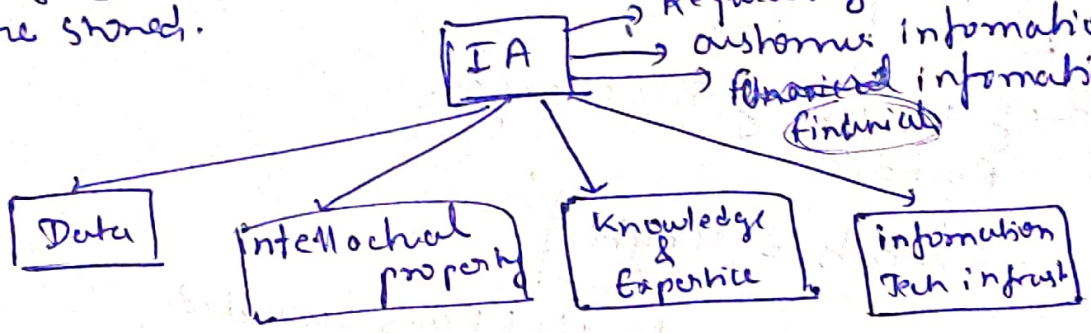
State 16 byte (4×4)

Stores intermediate results.

CSF Assignment Overview

Ans-1 **Information assets** - Any valuable information owned by any individual or organization is know IA. (Information assets).

~~Based upon~~ Information assets are classified into various category based upon their nature, importance, where they are stored.



Ans-2 ① Confidentiality. = prevent unauthorized access of information attacks assets

② Integrity = prevent unauthorized modification of information assets.

③ ~~Accessibility~~ Availability : allow authorized access of information assets when it was required.

Ans-3 **Information Security**: information security (IS) is way to prevent any individual or organization from any malicious attacks. These attacks can be active & passive. Active attacks are more difficult to remove by relocating, migrating services

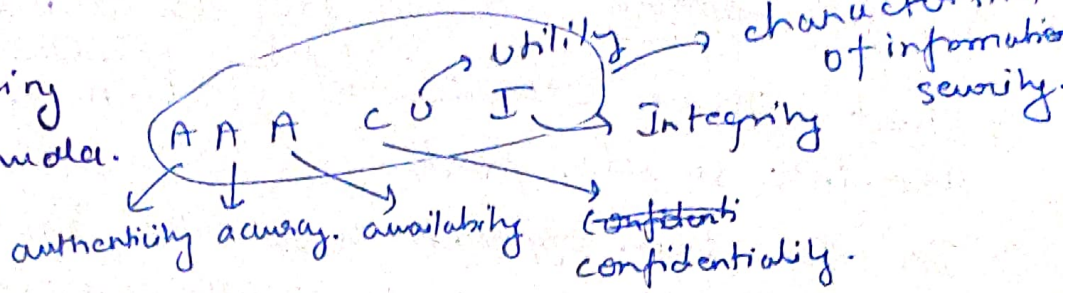
Security: free from danger.

Different layers of security

① physical security → actual assets can be implemented by applying lock & key.
② personal security → security from employee ~~→~~ film policy.
③ operation security → security related to any patony task.
④ Communication security → communication with a organization must be through secured network
⑤ Network security → securing network components private (using VPN)
⑥ Information security → by implementing security policy.

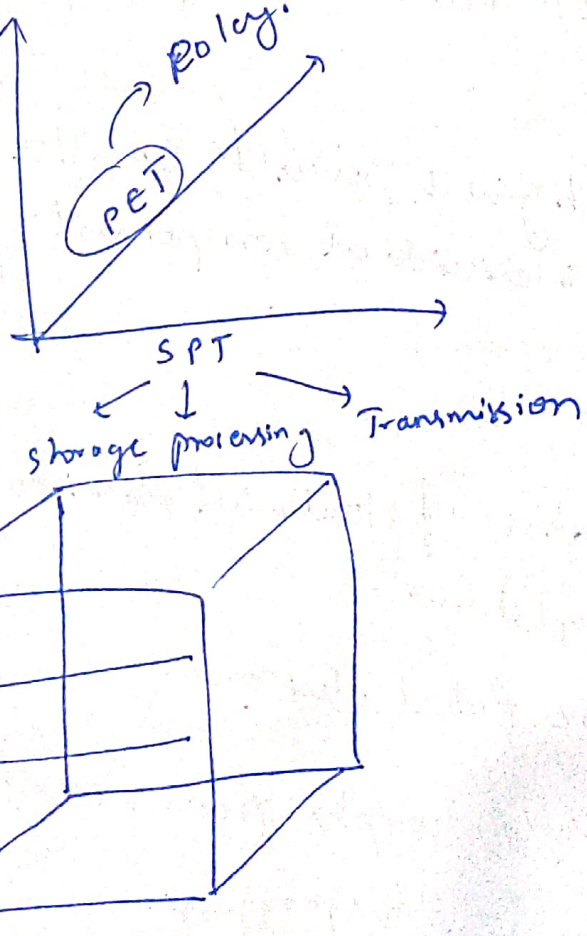
Information security is implemented using.
policy, training, education, awareness & technology.

Any useful Thing
Shortcut formula.



NSTISSC Model

* National security Telecommunication Information System Security Committie.
* NSTISSC fixed the National training standard for IT security. profft profft professionals.
* It is an 3D - dimensional model consist of CIA triple
* These are the set of guidlins & policy established by United State government for securing communication blw Computer & Telecommunication System.
* Developed Member.
* Provide model on security perspective.



✱ Two Approaches for implementing Information security.

Top-down approach → Initiated by Higher/upper management: like; CFO, CIO, COO, CEO

① Start with an overview of problem and breaking them into smaller parts.

② In Top-down approach a complex system is generally ~~done~~ divided into smaller sub-complex system or manageable components.

③ ensure each manageable components solve individually.

④ ~~Directing~~ leading to the solution of overall problem ultimately.

Disadvantages

① It doesn't ~~contain~~ involves interaction of lower post/scale employee before making any ~~decisions~~ decision.

Bottom-up approach.

① Start working of individual components and building the larger systems.

② ~~If~~ This approach give is power to smaller management teams or individual administration for implementation of individual component.

Advantage

① Individual expertise of technical administration.

② Flexible to adapt change

③ Robustness: more Robust solution.

Disadvantages. ① complex management for larger project.

② Slow progress.

CEO → chief Executive officer.
COO → chief operating officer.
CFO → chief finical officer.
CIO → chief information officer.
CISO → chief Information security offer.

Threats

↳ any potential process that may cause damage to our system.
↳ any potential access & occurance that affect our information assets. -vely.
↳ CIA affect CIA trade -vely.

Classification of threat

① physical threat → damage to our Hardware.
② Accidental threat → corruption of data by programs with prgm. bad programing practice
③ Unauthorized access → access to authorized person.
④ Malicious access → Trojan horse.
→ virus.

Types of Threats.

① Worm: Type of virus that Replicate itself and consume host resources.
② logic bomb: programming code that execute after certain condition will be met. Eg delete all files of computer on 25 Dec execution date
③ Trapdoor: method of gaining access to system with password. once user login Trapdoor embeed to system to password
④ Trojan Horse: Trojan's Horse silently embeed embeed to system process and sends. host ccel activity to hacker. Eg Installing fake software
⑤ RAT (Remote Admin Trojan's): Special form of Trojan's that provide remote access of host system. Eg image + embeed (RAT) < send's IP address to hacker

⑥ Malware: Any program harmful for our Computer System.

⑦ Rootkits: Gaining uses System access without user/host knowledge.
very dangerous type of threat.
Gaining the system access in very secret way.

⑧ Virus: perform malicious functions along

Vunlerability

↳ lack of security mechanisms in existing System.
↳ weakness in existing security mechanisms.

Security Mechanisms.

~~① Encrip Encripo~~

① Encipherment ⟶ going to use key + Mathematical formula + algo. to encrypt
② Digital Signatures ⟶ proof the identity for authentication service
③ Access Control ⟶ restrict access based + data integrity service.
some users.
④ Data Integrity ⟶ Same.
⑤ Authentication Exchange ⟶ some pack cookies info sends to connected routers to discover neibours next routers
To ensure that router will get info data packets from nebious router IP only not by hacker.
⑥ Traffic padding ⟶ dummy data send over transmission channel to confuse hacker.
⑦ Routing control ⟶ Controlling Routes

Security Services.

① Authentication
② Integrity (Data)
③ Confidentiality
④ Non-Repudiation

security attacks

① active attacks
② passive attacks

☆ Steganography

① Steganography refers to concealing information in another image or physical object to avoid detection.

② steganography is used to send/transmit any type of digital data over an unsecured transmission medium including text, video, images, audio content.

③ useful text is extracted at the receiver's side.

Steganography Working/How to achieve.

① LSB: this involves embedding secret information in LSB (least significant bit) of media/text.

② Embedding secret information network packets.

Types of steganography.

① Text
② Video
③ Network
④ Image
⑤ Audio.

Cryptography → data encryption

steganography → data hide.

embedding secret information in network Control protocols.

embedding in TCP, UDP, ICMP protocols.

info secrets

~~What is Vulnerable~~

~~① Finical [illegible]~~

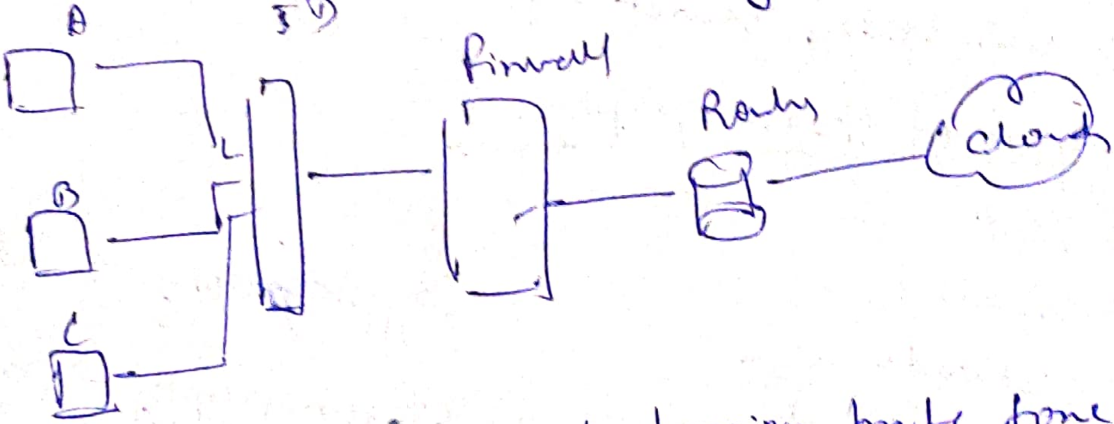
Types Security Attacks.

① Finding a way into network.

② Firewalls → only allow authorized person to access network.

- Good → To filter out what good comes & what goes out.
- bad → Single point failure, confusion

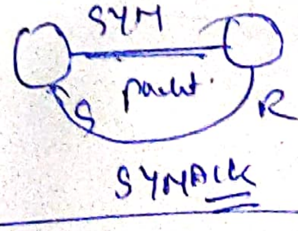
③ Intrusion Detection → monitor the suspicious activity over network.



④ Dictionary attacks → performing brute force attack on system.

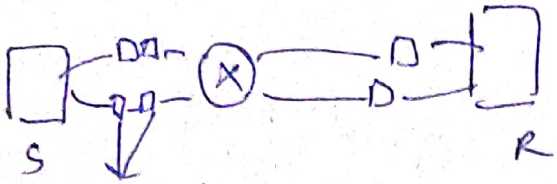
⑤ DOS (Denial of service) → flooding network.

- DDOS → much larger scale, multiple people attack with.
- SYN → solution: SYN cookies. forget everything else.



⑥ → TCP attack

① packet Sniffing



① Packets are read by Hackers silently.

② Hackers get to known about our communication pattern

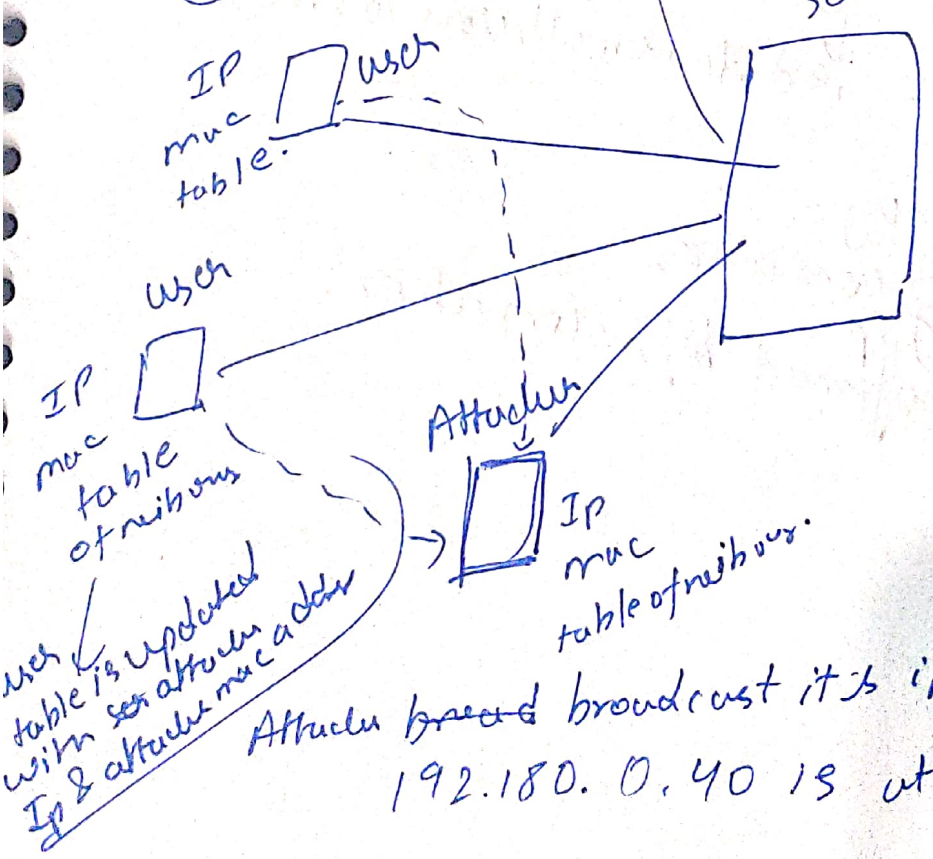
Prevention: ① High Encryption (Use VPN)
② only surf https website

SSL (Service Socket layers)

① packet Sniffing

② TCP attacks

③ ARP Spoofing → address Resolution protocol. Newnode broadcast their IP in network.



Attacker broadcast it's ip on network. /mac.

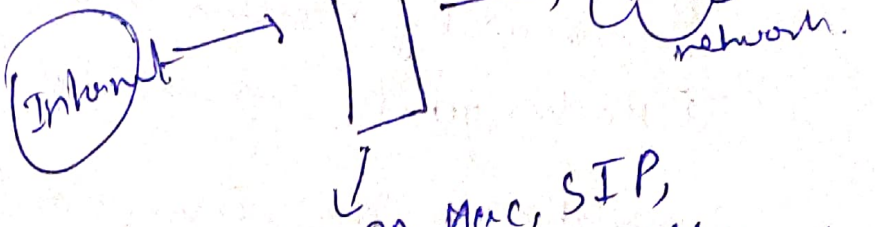
192.180. 0. 40 is at attacker mac address.

TCP/IP Hacking

* Hackers will enter malicious information/data in ~~Network~~, which in TCP stream.

Fire Wall types

① Packet filtering

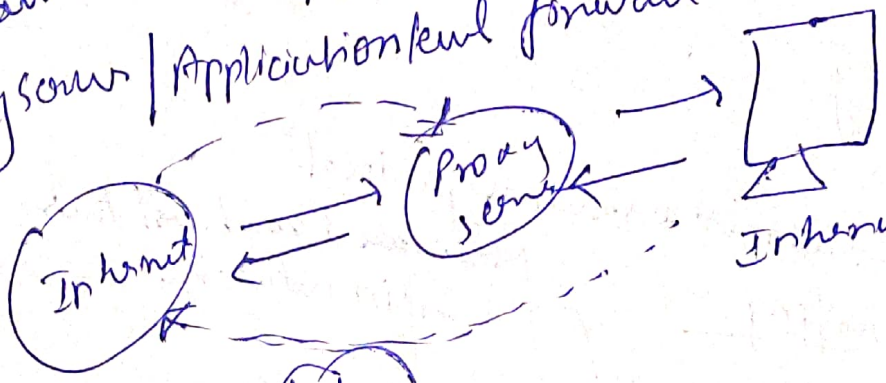


only PA, Mac, SIP, DIP addrss are checked, dat is not checked. less secure.

Disadvantage

Is if data is malicious it came harm to private network.

② proxy server / Application level firewall.



checks headers + data

PA, IP, Mac — is data is malicious or not.

③ Circuit level gateway.

↳ establishes 2 way connection.

↳ security checks performed before connection.

Java Cryptographic package.

1. JCE → Java Cryptography class
2. JSSE → Java Secure Socket extensions.
3. JAAS → Java Authentication And Authorization Service.
4. Java GSS API → Java generic Security Service.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

RSTUVWXYZ

These all are Cryptographic protocols.

1. SSH → uses the remote server to through command. ie SSH → secured shell
   → Is a way through which establish a secured connection to remote server.
2. TLS | SSL → security Socket layer's. used secure data server.
   - encrypt
   - It can used with any network protocols. HTTP, SMTP, FTP.
   - SSL is renamed to TLS

which type of security provided.

1. Integrity.
2. Authication
3. Confidentiality.

sender → ① encrypt. → ② attached SSL header + data

Application layer
SSL layer.
Transport layer.

Receiver
① remove SSL header.
② decrypt