UNIT - 1

Q. ACTIVE VS PASSIVE ATTACKS.

→

ACTIVE ATTACKS	PASSIVE ATTACKS.
* modification in information.	Info is not modified
* dangerous for integrity and availability.	dangerous for confidentiality
* system is always damaged.	No harm done to the system.
* victim is informed about attack	Victim unaware of the attack.
* System resources are altered.	No changes made to resources.
* influences the system services.	System info is acquired.
* difficult to restrict entry from entering 8 systems/network	Easier to prohibit compared to active attacks.

Q. SECURITY ATTACKS ON ENCRYPTION SCHEME :

(1) CRYPTANALYSIS –

- Ciphertext only
- known Plaintext
- ~~known~~ Chosen Plaintext
- Chosen Cipher text
- Chosen Text

} 5 types.

* cryptanalysis attacks rely on nature of the algo and some knowledge of general characteristics of plaintext or some examples of plaintext - ciphertext pairs.
* This attack exploits the characteristics of algorithm to attempt to deduce a specific plaintext or to find the key being used.

(2) BRUTE FORCE ATTACK :–

* attacker tries ~~to~~ every possible key on a piece of cipher text until an intelligible ~~so~~ translation into plaintext is obtained.
* ~~A~~ Half of all possible keys must be tried atleast to achieve success.

Q. SECURITY SERVICES/ MECHANISM OF X.800.

(1) Authentication - assurance that the communicating entity is the one it claims to be.

(a) Peer Entity Authentication - used in association with a logical connection to provide confidence in the identity of entities connected.

(b) Data Origin Authentication - is connectionless transfer. It provides assurance that the source of received data is claimed and trusted.

(2) Access Control - prevention of unauthorized use of a resource.
This service controls who can have access to a resource, under what conditions access can occur, & what they are allowed to do.

(3) Data Confidentiality - protection of data from unauthorized disclosure

(a) Connection Confidentiality : protect user data on a connection.
(b) Connectionless Confidentiality: protect user data in a single data block.
(c) Selective Field — " — : protect selected fields within user data
(d) Traffic-Flow — " — : protect info that might be derived from observation of traffic flows.

(4) Data Integrity - assurance that data received is same as the data sent.

(a) Connection Integrity with Recovery
(b) Connection Integrity without Recovery
(c) Selective Field Connection Integrity
(d) Selective Field Connectionless Integrity.
(e) Connectionless Integrity.

(5) Non Repudiation - provides protection against denial of service by one of the entities involved in communication of having participated in all or part of the commn.

(a) Non-repudiation Origin.

(b) Non-repudiation Destination.

Q. COMPONENTS OF SYMMETRIC ENCRYPTION:

(1) Plaintext - original intelligible message/ data. fed into the algorithm as input.

(2) Ciphertext - scrambled message produced as output. Depends on plaintext and secret key used for encryption. Different secret keys produce produce different ciphertexts.

(3) Secret Key - It is also input in the encryption algo. The key is a value independent of plaintext & algo. The encryption output of algo depend on the secret key

(4) Encryption Algo. - performs various substitutions and transformations on the plaintext.

(5) Decryption Algo. - basically the encryption algo run in reverse. It is used to obtain the intelligible plaintext from the ciphertext with the help of secret key.

Q. REQUIREMENTS OF SECURE ENCRYPTION:

(1) Strong Encryption Algo - the opponent should not be able to decrypt ciphertext / discover key used to cipher.

(2) Sender & receiver must have obtained copies of the secret key in a secure manner & must keep the key secure...

Q. SUBSTITUTION TECHNIQUES.

* A substitution technique → the letters of plaintext are replaced by other letters or by numbers/symbols.
* If plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bits with ciphertext bits pattern.
* Caesar Cipher –

Encryption.

$$C = E(k, p) = (p+k) \bmod 26.$$

Cipher text bit is equal to keyword k (numeric/alphabet) alphabets after the plaintext p bit.

Decryption:

$$P = D(k, c) = (c-K) \bmod 26.$$

→ Allows brute force attack:

(i) encryption & decryption algo are known

(ii) only 25 keys to try

(iii) language of plaintext is known & easily recognizable

* Monoalphabetic Cipher

Randomly assigning any plain text alphabet a cipher alphabet.

It can be broken easily based on the freq. of letters.

* Play Fair Cipher

⇒ Best known multiple-letter encryption cipher

keyword → (keyword + rest alphabets in a 5x5 matrix).

* Hill Cipher

$$C = P * K \bmod 26$$

$$P = C \cdot K^{-1} \bmod 26.$$

* Polyalphabetic Cipher:
keyword added to plaintext to obtain ciphertext.

~~Q. CRYPTOGRAPHY vs STEGANOGRAPHY~~

Q. BLOCK CIPHER DESIGN PRINCIPLES –

(1) Number Of Rounds – It is regularly considered in design criteria; it reflects the no. of rounds to be suitable for an algo to make it more complex.

DES – 16 rounds   AES – 10 rounds.

(2) Design of Function f – The core part of Feistel Cipher is the round function. The complexity of cryptanalysis can be derived from Round func^n^, i.e., ↑ level of complexity for round func^n^ increases complexity Avalanche effect is further included to increase complexity.

(3) Key Schedule Algo – In Feistel Cipher, each round generates a sub-key for increasing the complexity of cryptanalysis. Decryption must be done very carefully to get the actual output due to presence of avalanche effect.

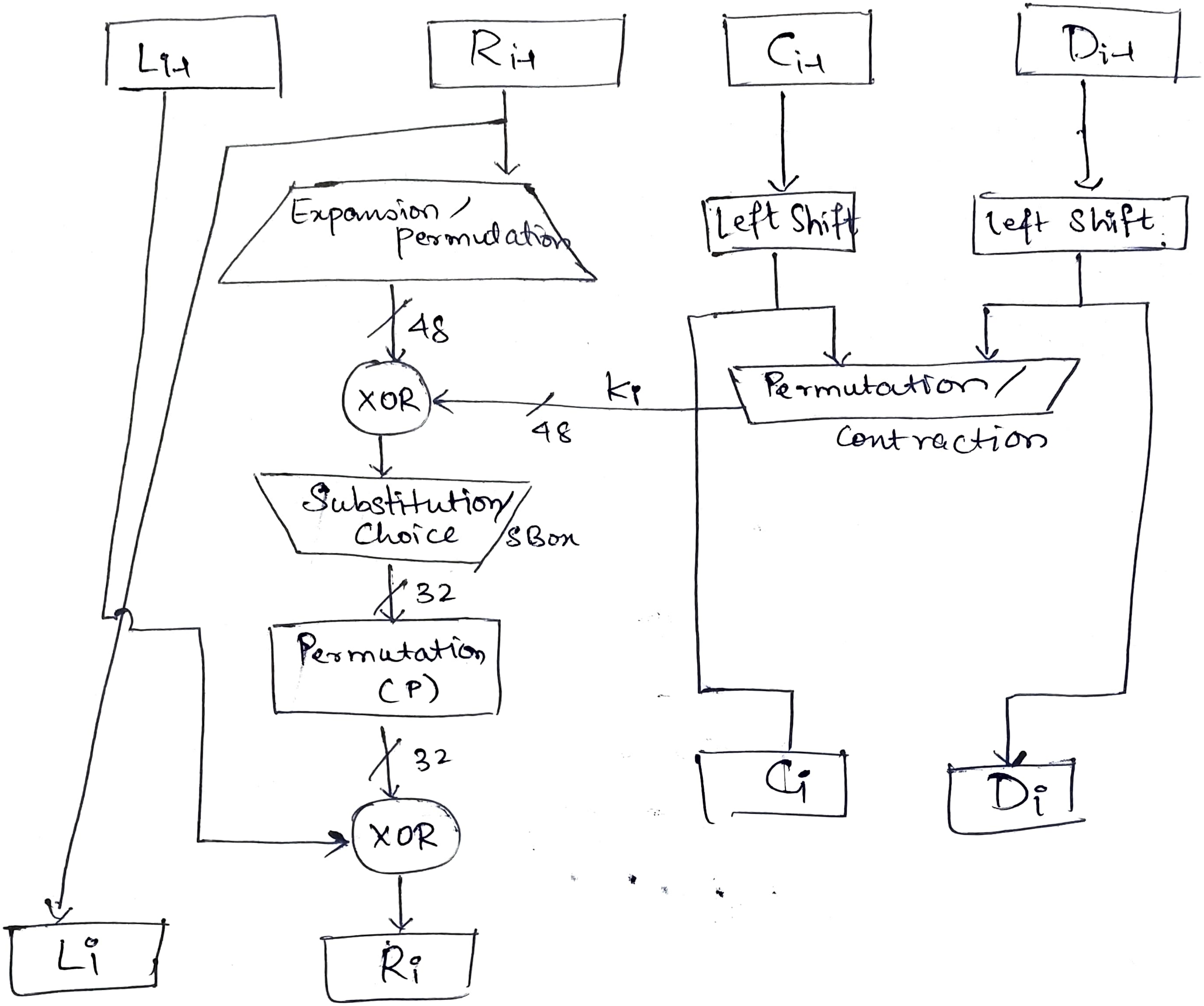
Q. Single-DES · Algo.

* The 64 bit intermediate result is treated as separate 32-bit quantities left (L) & right (R). $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus F(R_{i-1} + K_{i-1})$

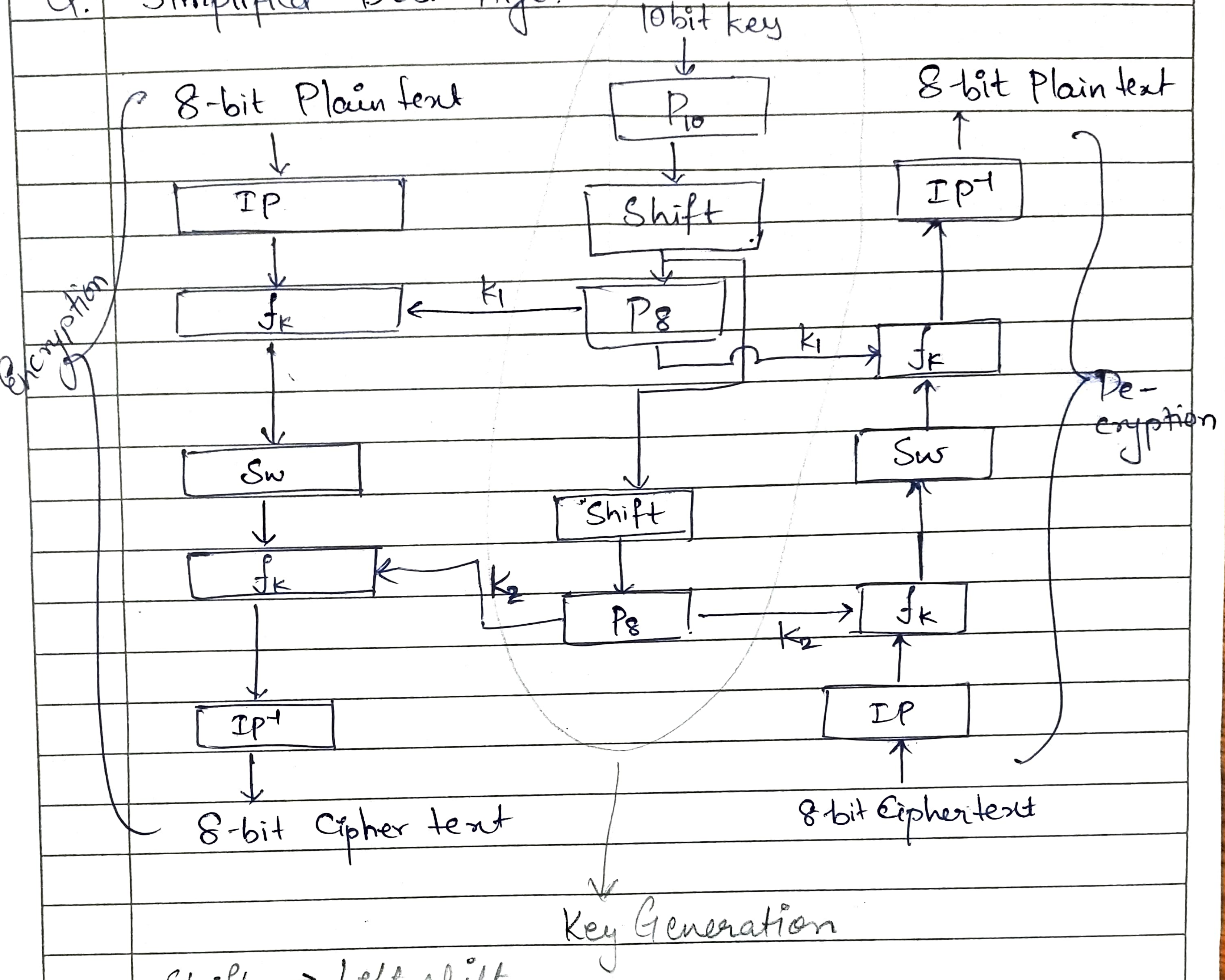
* key K_i is 48 bits

* Input R is 32 bits which is expanded to 48 bits.

* The S-Box performs function f; input 48 bits, o/p 32 bits


Li-1
Ri-1
Ci-1
Di-1
Expansion / permutation
Left Shift
left Shift
48
Permutation / Contraction
Ki
48
XOR
Substitution/ Choice
SBox
32
Permutation (P)
32
XOR
Ci
Di
Li
Ri

Q. Simplified DES. Algo.



Shift → Left shift

Q. DIFFERENTIAL VS. LINEAR CRYPTANALYSIS.

LINEAR	DIFFERENTIAL
* known as plaintext attack in which attacker studies linear relations known as linear approximations b/w parity bits of the plain text, the cipher text and the secret key.	* general form of cryptanalysis that is primarily applicable to block ciphers, cryptographic has func's.
* focuses on statistical analysis against one round of decrypted cipher text.	focuses on statiscal analyis of two inputs and 2 outputs of a cryptographic algorithm.
* The attacker identifies the linear relation b/w P.T, C.T and key.	Attacker analyzes changes in P.T and the difference in the outputs from encrypting each P.T.

CONFUSION	DIFFUSION
Obscure the relationship b/w P.T & C.T	Spread the P.T statistics through C.T.
possible through substitution algo.	possible through transposition algo.
used in both block & stream cipher	used only in block cipher.
hides relation b/w ciphertext & key	hides relation b/w C.T and P.T.
results in increased vagueness	results in increased redundancy