Assignment - 1

1. Explain security services and security mechanisms in cryptography ?

A Security services is a service that is provided by a protocol layer of communicating open systems which ensures that the adequate security of the systems or the data transfers in the data transmission.

→ A processing or communication service that is provided by a system by a system to give a specific kind of protection to the system resources.

→ The security services are classified in to different types they are

* Authentication
* Access control
* data confidentiality
* data integrity.

* Authentication : it gives assurance that the communicating entity is the one which is to be authenticated in two ways.

1. peer-entity authentication
2. Data origin authentication.

1. peer-Entity authentication : This is used in authenticating the users in one to one manner the users with a logical connection to provide confidence in the identity of the entities connected.

2. Data origin authentication : This authentication is used in a connection less transfer it is used in connection less transfer which provides assurance that the source of the received data is asclined.

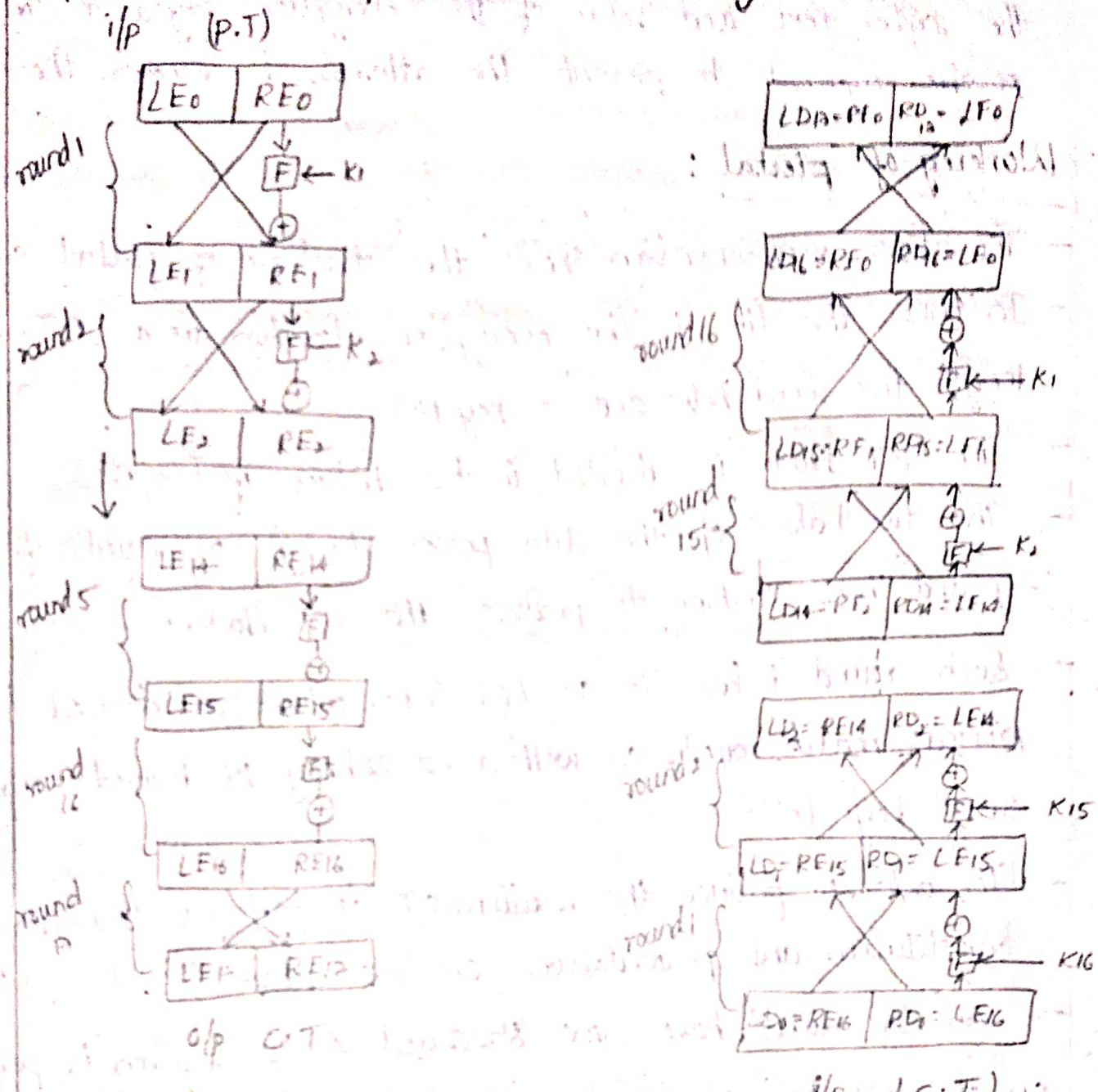
* Access control: The prevention of unauthorised use of a resource that is it controls who can have access to a resource, under what conditions the access can occur and what those accessing the resource, or allow to do
* Data confidentiality: it provides protection to the data from unauthorised access.
→ In connection data confidentiality it provides protection of all the users data on a secure connection.
→ The connection less data confidentiality provides protection of all the users data in a single data block.
→ The selective-field confidentiality provides production of particular selected fields within the userdata on a connection or a single data block.
→ The traffic flow confidentiality provides protection information that might derived from observation of the traffic flows.
* Data integrity: it gives the assurance that the send data received is exactly as send by an authorised entity.

Security Mechanisms:

* Specific Security
* pervasive security.

Specific Security	pervasive Security
• Encipherment	• Trusted functionality
• digital signature	• Security label
• Access control	• Event detection
• Data integrity	• Security audit trail
• Authentication exchange.	• Security recovery.

1. Explain Substitution and transposition techniques?
2. Explain fiestal cipher with block diagram?



→ In cryptography a fiestal cipher is a symmetric structure which is used in the construction of block ciphers.

→ It was proposed by the German IBM cryptographer 'Horst Fiestal' and it is also called as fiestal network.

→ A large set of block cipher use the scheme including data encryption standard. (DES)

→ The main aim of these approach is to develop a block ciphers with a K length K-bits and a block length of n-bits allowing a total of 2^K

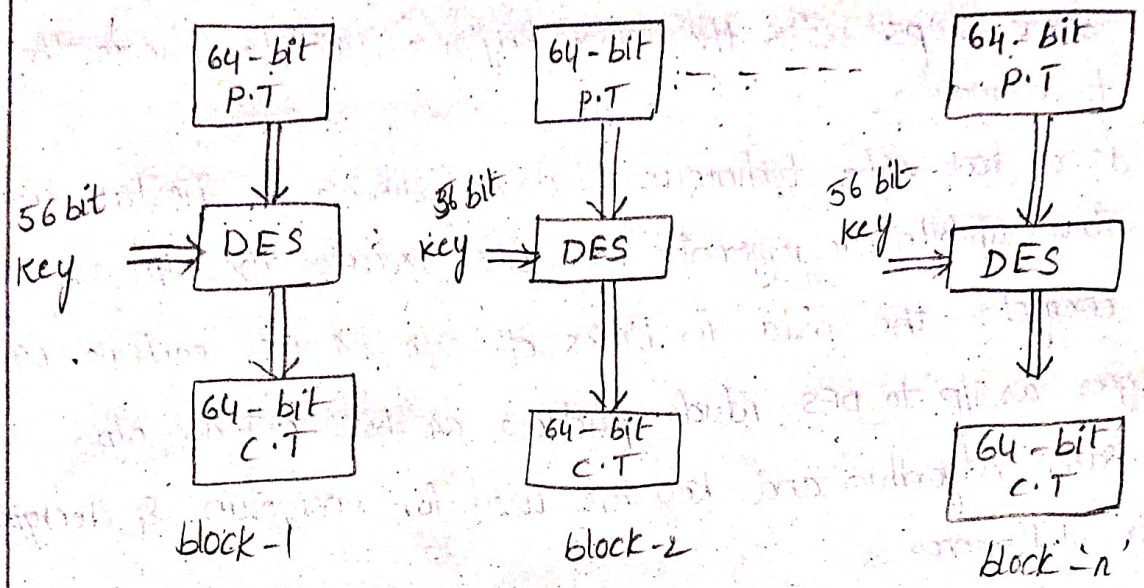
possible transformation rather than $2^n!$ transformation available.

→ Confusion is used to make the relationship b/w the statistics of the cipher text and value of the encryption key as a complex as possible against to prevent the attempts to discover the key.

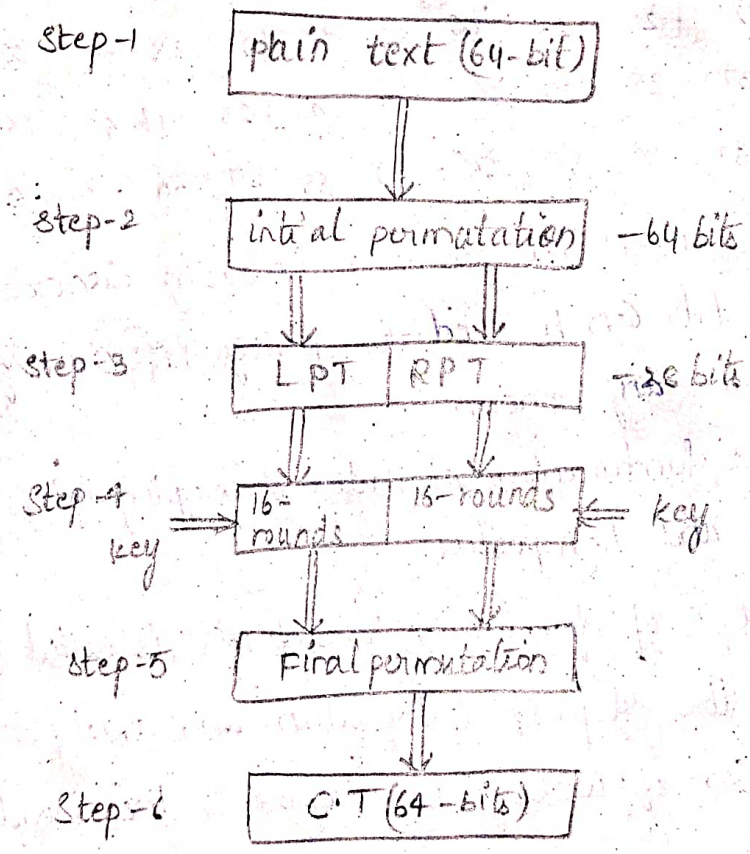
Working of Fiestal:

- The above representation shows the structure of fiestal ciphers
- In this the i/p to the encryption algorithm are a P.T block of length two word bits and a key (K)
- The P.T block is divided in two halves. i.e $[L_0, R_0]$
- The two halves of the data passes through n rounds of processing and then combine to produce the C.T block.
- Each round i has i/p as L_{i-1} & R_{i-1} where are derived from the previous match round, as well as a subkey K_i derived from the overall keys (K)
- In order to produce the resulting C.T it performs 16 rounds of substitution and permutation on the data.
- All the rounds have same structured. A substitution is performed on the left half of the data. This is done by applying a round function (F) to the right half of the data. and then taking the extra pading bits along with XOR operation of the output of that function. and left half of the data
- By following this substitution a permutation is performed which consists of the inter change of the two halves of the data.

3. Explain DES algorithm with neat sketch?



Working of DES:



- DES was the most widely used algorithm until the introduction of AES.
- DES was developed in 1977 by the national bureau of standards, now it is called as National institute of standard & technology
- The algorithm itself is reffered as data encryption algorithm
- In DES the data is encrypted in 64-bits blocks using a 56 bit key.

- it transforms the 64-bit key input in the series of steps into a 64 bit output.
- The same steps with the same key are used to reverse the encryption i.e for decryption.
- DES is a book cipher technique which is similar to fiestal ciphers
- The above architecture represents how DES executes the o/p as ciphertext
- It encrypts the data in blocks of size 64 bits each i.e 64 bits of P.T goes as i/p to DES which produces 64-bit C.T as o/p.
- The same algorithm and key are used for encryption & decryption with minor differences.

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	27	28	29	30	31	~~32~~
33	34	35	36	37	38	39	~~40~~	41	42	43	44	45	46	47	~~48~~
49	50	51	52	53	54	55	~~56~~	57	58	59	60	61	62	63	~~64~~

- This table shows the crossed bit positions indicating discarded bits
- Before discarding these bits can be used for parity bit checking to ensure that the doesn't contain any errors.
- DES is based on two fundamental attributes of cryptography which are called as substitution and transposition.
- DES consits of 6 steps of functioning, Each of bits is called as a round
- Each round performs the steps of substitution and transposition.
- The above block diagram of working DES represents the broadlevel steps which are given below.

Step-1 : 64 bit P.T block is taken as i/p and it is handed over to an intial permutation function.

step-2 : The intial permutation is performed on the P.T where the substitution and transposition are applied on the text

step-3 : The intial permutation generates two halves of the permuted block i.e left P.T (LPT) and right P.T (RPT)

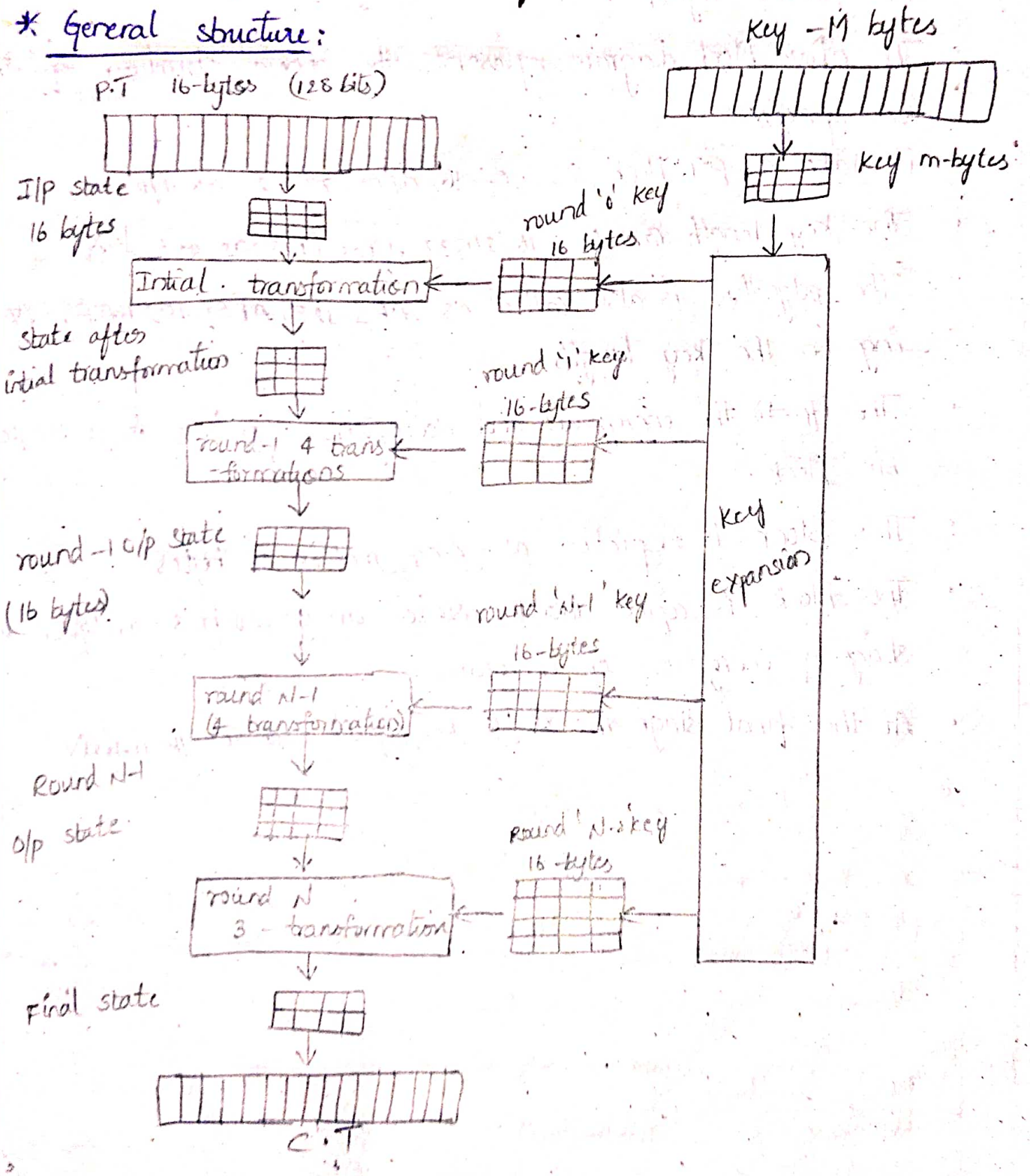
Step-4 : Now, each of LPT and RPT goes through 16 rounds of encrypti-on process.

Step-5 : In the end the LPT and RPT are rejoined and the final permuta-tion is performed on the combined block.

Step-6 : The result of this process generates 64 bit C·T as o/p.

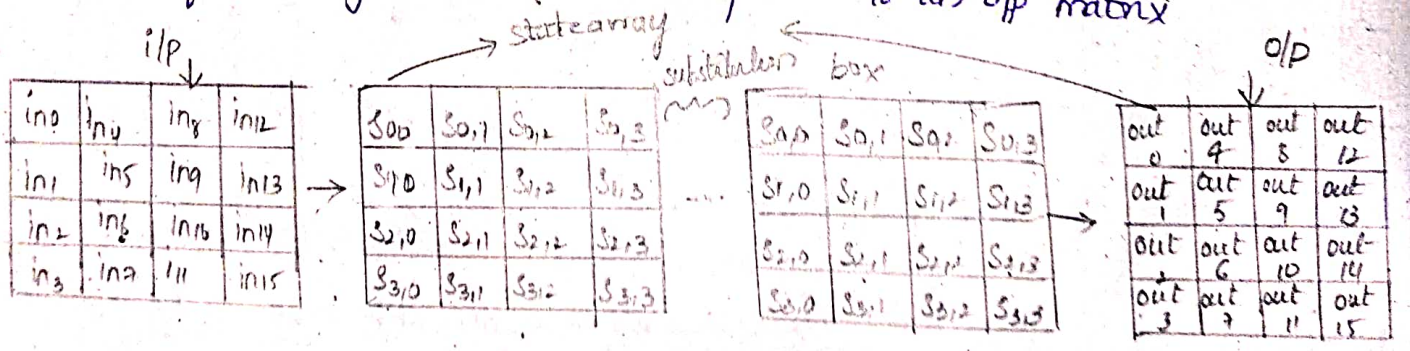
4. Explain the detailed structure of AES?

* General structure:

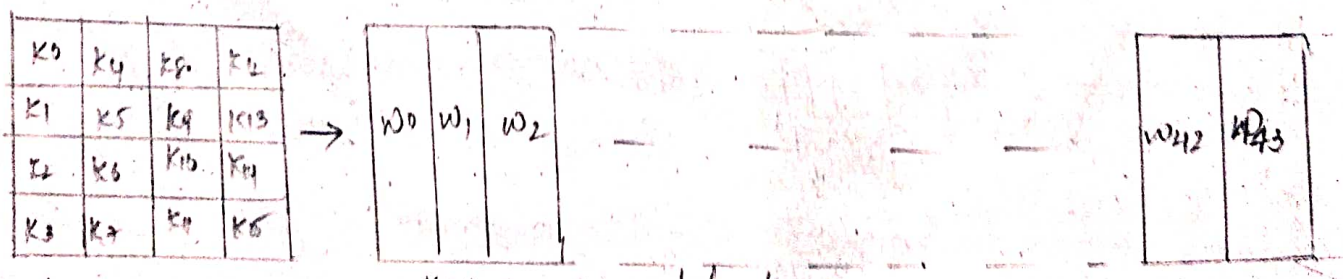


- AES means Advanced Encryption Standard which is the advanced version for DES
- It is classified into two types : 1. General structure
  2. detailed structure.
- AES is a symmetric block cipher encryption algorithm
- This was developed by Belgian cryptographers named as John daemen and vincent rejmen.
- The above block diagram represents the general structure of AES encryption process.
- it takes a PT block size of 16 bytes, 24, 32 as i/p
- The key length can be 16, 24, 32 bytes (128, 192, 256 bits)
- The algorithm is also called as AES-128, AES-192, AES-256, depending on the key length.
- The i/p to the encryption and decryption algorithms is a single 128 bit block.
- This block is depicted as 4x4 matrix of bytes
- This block is copied into the 'state' array which is modified at each stage of encryption or decryption.
- At the final stage the state is copied to an o/p matrix

a)



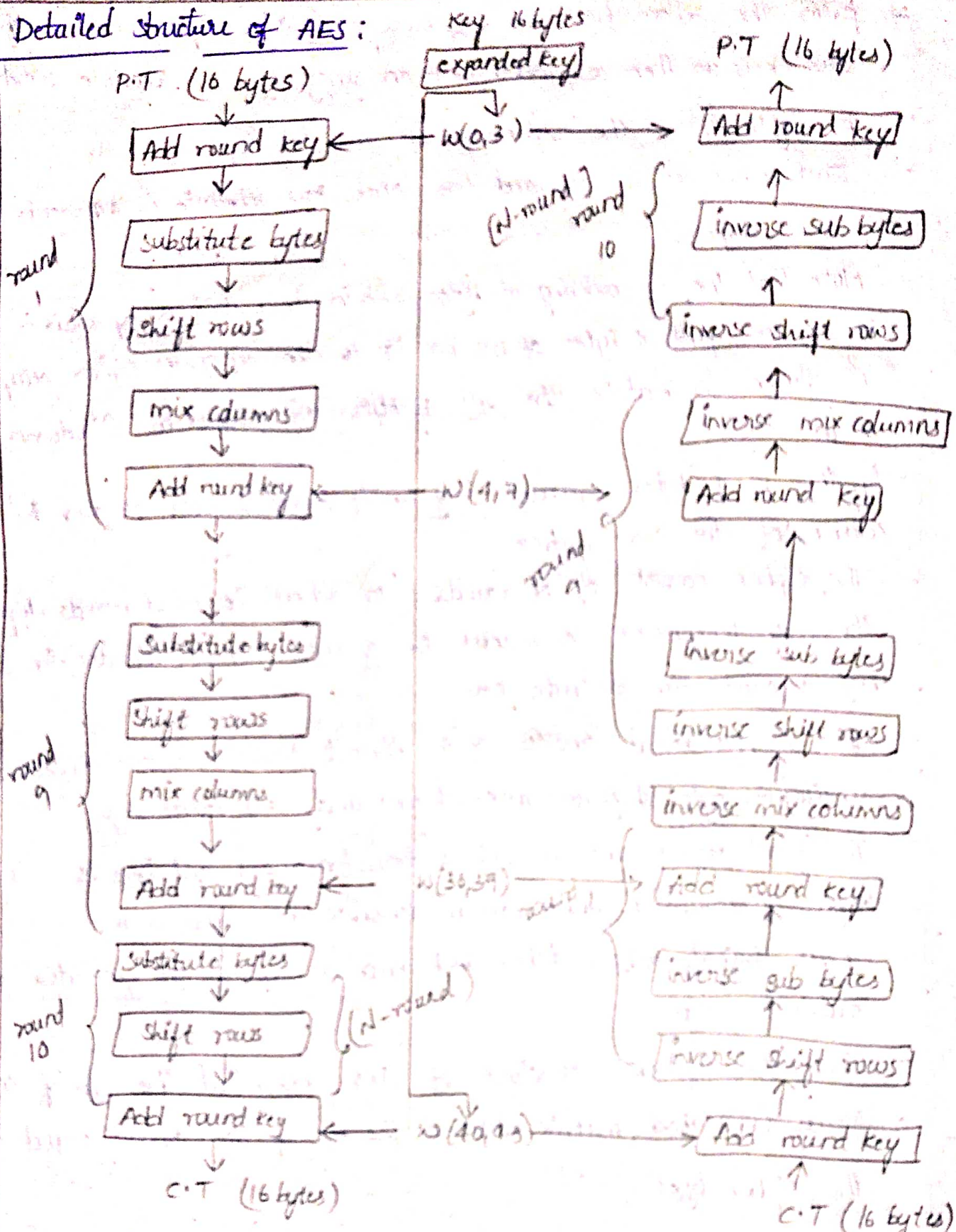
b)



key & Expanded key

- From the above fig(a) the key is depicted as a square matrix of bytes.
- This key is then expanded into an array of key schedule words
- The fig (b) shows the expansion for 128 bit key.
- Each word is 4 bits and the total key schedule is 44 words for the 128 bit key.
- Note that the i/p ordering of bytes with in the matrix is by column proces.
- For ex, the first 4 bytes of 128 bit i/p to the encryption cipher occupies the 1st column in matrix the end 4 bytes are occupied by 2nd column and so on....
- Ly, the 1st 4 bytes expanded key which forms a word occupies the 1st column of the 'w' matrix
- The cipher consist of 'N' rounds = 10 where the no. of rounds depends on the key length i.e 10 rounds for 16 byte key 12 rounds for 24 byte key, 14 rounds for 32 byte key.
- The 1st N-1 round consists of 4 distinct transformations functions i.e Substitution Byte, shift rows, mix columns and add round key.
- The final round contains only 3 transformations and there is a inital single transformation which can be consider as round zero.
- Each transformation takes 4x4 matrices as i/p and generates a 4x4 matrix as o/p
- The above General structure of AES shows that the o/p of each round is a 4x4 matrix, which is the o/p of the final round being the cipher text.

Detailed structure of AES:



- The above diag shows the detailed structure of AES
- In this algorithm it indicates the sequence of a transformation in each round and showing the corresponding decryption function
- In process the entire data block as a single matrix during each round by using substitutions and permutations.

- The key that is provided as ip is expanded into an array of fourty four 32 bit words w[i]
- 4 distinct words serve as a round key for each round!
- In this 4 different stages are used i.e one is permutation and the remaining three are substitutions:

Substitute bytes: It uses an s box to perform a byte-by-byte substitution of block.

Shift rows: it performs a simple permutation operation in the block.

mix columns: In this function a finite field is a set on which the operations of multiplications, additions, subtractions and divisions are defined and satisfies certain basic rules.

Add round key: A simple bitwise XOR operation of the current block is performed with a portion of the expanded key.

5. Explain substitution and transposition techniques?

Encryption techniques are used to produce C.T. they are

1. Substitution
2. transposition

1. Substitution: Replacing data with another data

1. Caesar ciphes
2. homophonic substitution cipher
3. poly-alphabetic ciphes
4. play-fair ciphes.

1. caesar cipher: replaces each letter by 3rd letter on

- This method was proposed by julius caesar

Ex:- meet me

PHHW PH

→ $C = E(p) = (p+k) \bmod (26)$

→ $P = D(C) = (p-k) \bmod (26)$

→ plain text can be lower or upper letters

→ cipher text must be in upper letters.

2. homophonic Substitution ciphers: One alphabet can be replaced with more than one alphabet

Ex: PT → A

CT → replaced by D, H, P, R

PT → B

CT → replaced by E, I, Q, S

3. polyalphabetic substitution cipher:

Keys

PT	a	b	c	d	e	f	g	h	i	j	k	l	m	.....	z
	a	(A)	B	C	D	E	F	G	H	I	J	K	L	M	... Z
	b	B	C	D	E	F	G	H	I	J	K	L	M	N	... A
	c	C	D	E	F	G	H	I	J	K	L	M	N	O	... B
	d	D	E	F	(G)	H	I	J	K	L	M	N	O	P	... C
	e	E	F	G	H	I	J	K	L	M	N	O	P	Q	... D
	f	G	H												
	g	H	I												
	⋮	⋮	⋮												
	z	Z	Z												

Ex: PT – dad

CT – GAG

4. playfair cipher:

→ a 5x5 matrix of letters based on a keyword

→ fill in letters of keyword (sans duplicate)

→ fill rest of matrix with other letters