Deffine - Hellman key - Exchange / Agreement algorithm

- whitefield Diffine and martin Hellman devised solution to the problem of key no agreement or key exchange, in 1976
- this solution is called the Diffie-Hellman key exchange / agreement algorithm
- The two parties, who want to communicate securly, can agree on a symmetric ~~on~~ key using this Techniques
- used only for key agreement but not for encryption or decryption of messages.

* Alice and bob want to agree upon a key to be used.

1] firstly, Alice and bob agree on two large prime Number, n & g these two integers need not be kept secreate. Alice & bob use an insecure

* man in the middle attack

* Eliptic curve cryptography

- this is asymmetric public crypto system
- it provides equal security with small key size as compared with other non Ecc Algorithm
- it makes use of eliptic curve

eqn: $y^2 = x^3 + ax + b$

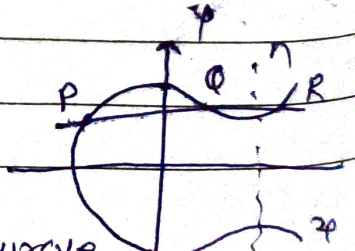


fig Eliptic curve

* properties

Eliptic curve is symmetric to x-axis

- Trapdoor function

Eq (a, b) [∵ a, b, q elements of eliptic curve

Q = K X P

- key generation at alice

select private key n_A [∵ $n_A < n$

- calculate public key P_n

$P_A = n_A \times G_1$ → generator point on EC

key generation at bob

- select private key n_B [∵ $n_B < n$

calculate public key

$P_B = n_B \times G_1$

secreate key : $K = n_B \times P_A$

secreat key , $K = n_A \times P_B$

* encryption :- M → Message

$cm \rightarrow \{ KG,\ Pm + K \cdot P_B$

↑ public key of bo

* decryption :- $KG + n_B$

$Pm + K \cdot P_B - KG \times n_B$

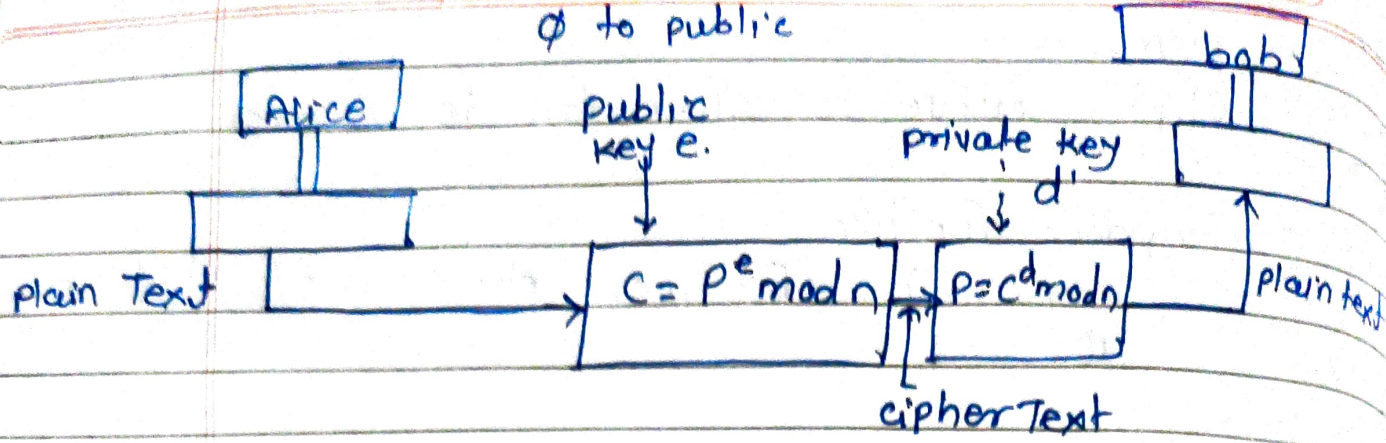
$Pm + KP_B - KP_B = P_B$

$= Pm$

* RSA algorithm (R-Rivent, S-shamir, A-Addel man)

- most comman public key algorithm
- it is uses two number e & d

public key & private key



* selection of keys

1) bob chooses two very large prime number P & q
2) bob multiplies two prime number (P*q) to find n (n = P*q)
3) bob calculate another no. which is ϕ
   ϕ = (P-1)*(q-1)
4) bob chooses random integer 'e' ~~hidden~~ he then calculates d (d x e) mod ϕ = 1
   bob Annoucess e & n to the public & keeps

P = 3 , q = 11

n = 3 x 11
  = 33

ϕ = (P-1) * (q-1)
  = (3-1) * (11-1)
ϕ = 20

1 < e < ϕ e = 3 [e & ϕ does not have any common factor]

P = 5 plain text

C = P^e mod n
  = 5^3 mod 33
C = 26

d = 7

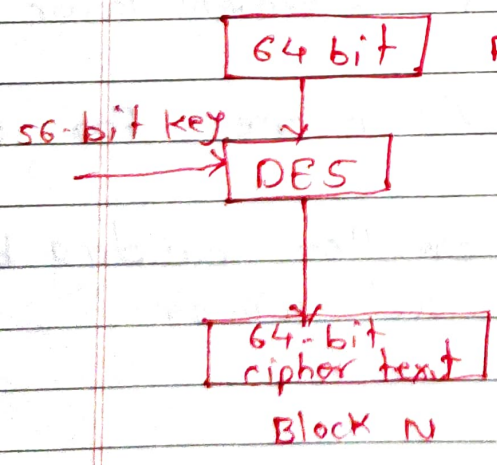
* Data encryption standard. (DES)

- Most widely used block cipher in world
- adopted in 1977 by NBS (Now NIST)
  - as FIPS 46
- encrypt 64-bit data using 56-bit key
- has widespreade use
- has been considerable controversy over its security

- IBM developed Lucifer cipher
- by team led by Feisted in late 60's
- used 64-bit data blocks with 128-bit key

18-04-22

- DSE is a block cipher.
- The algorithom and key are used for enc
  with minor difference.
- The key length is 56 bit



- bit positions is, 8, 16, 24, 32, 40, 48 → those bit discarded
- check parity of every bit thery will be not contains any error.

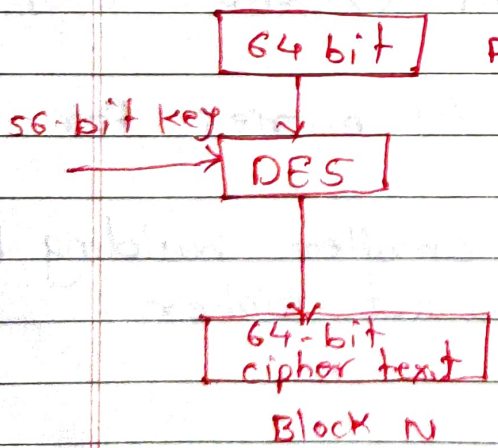
Data encryption standard. (DES)

- Most widely used block cipher in world
- adopted in 1977 by NBS (Now NIST)
  - as FIPS 46
- encrypt 64-bit data using 56-bit key
- has widespreade use
- has been considerable controversy over its security

- IBM developed Lucifer cipher
- by team ~~by~~ led by Feisted in late 60's
- used 64-bit data blocks with 128-bit key

18-04-22

- DSE is a block cipher.
- The algorithom and key are used for enc with minor difference.
- The key length is 56 bit



- bit positions is, 8, 16, 24, 32, 40, 48 ↑ 56 & 64 → these bat discarded
- check parity of every bit thery will be not contains any error.

* Initial permutation (IP)

- first step of the data computation.
- IP records the i/p data bit.
- even no bits in LH & odd bits in RH

step 1: Key Transformation

- from the 56-bit key, a different 48 bit subkey is generated during each round using a process called key Transformation
- The 56-key is divided into two halves, each of 28 bit
- These halves are circularly shifted left by one or two bit position.

25-04-22

step 2] expansion permutation

- RPT (Right plain text) is expanded from 32 bit to 48 bit
- Besides increasing the bit size from 32 to 48 bit are permuted as well, hence the name expansion permutation.

① - the RPT is divided into 8 bit

② - Next, each 4-bit block of the above step is then expanded to corresponding 6-bit block.

unit - III

algorithm types

stream cipher

block cipher.

1) Draw DSE flowgraph to process a plain text block of 64 bit.

- The data encryption standard is also called as data encryption algorithm by ANSI

* Basic principles.
  - DES is a block cipher
  - it encrypts data in blockes of 64 bit each
  - 64 input and 56 are output.

* Basic workflow of DES algorithm

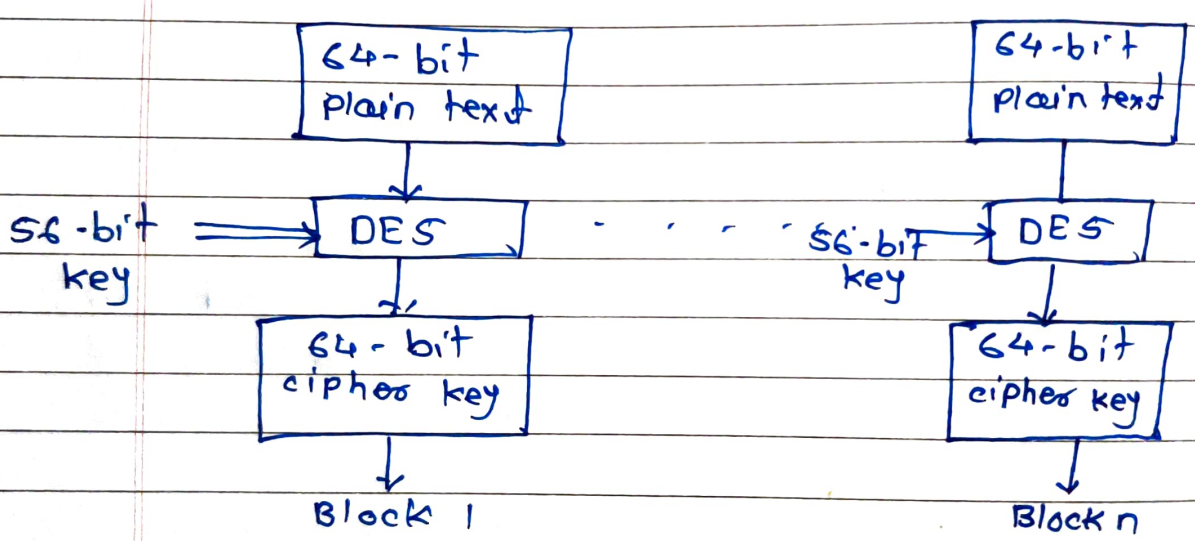
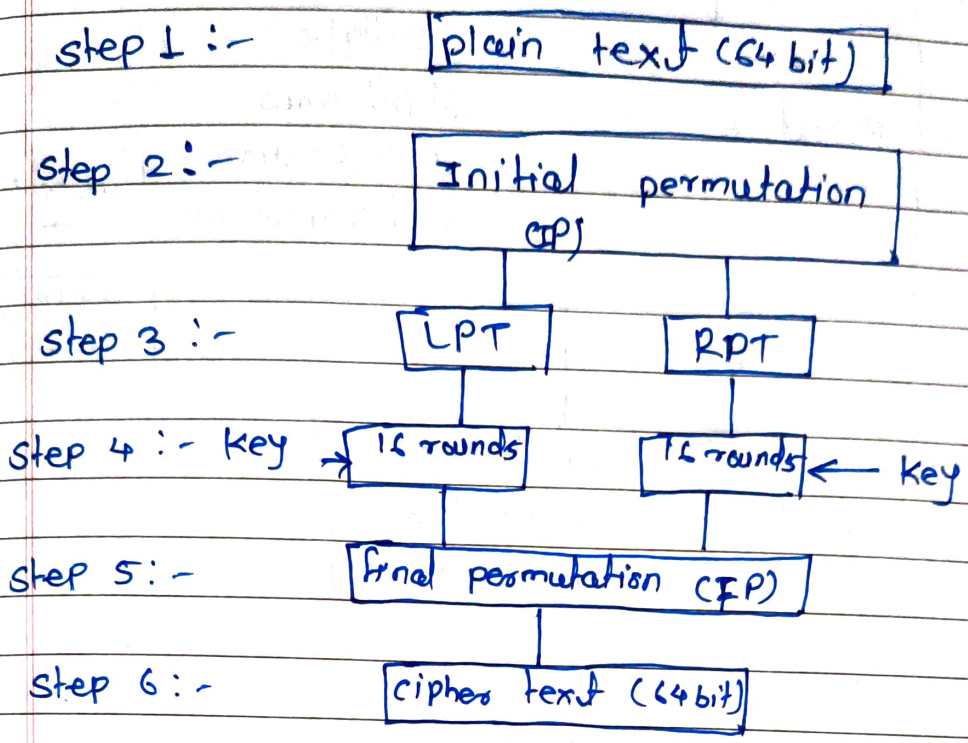


fig. conceptual working of DES

- 8, 16, 24, 32, 40, 48, 56, 64 discarded key
- before discarding, these bits can be used for parity cheaking to ensure that the key dose not contain any errors.

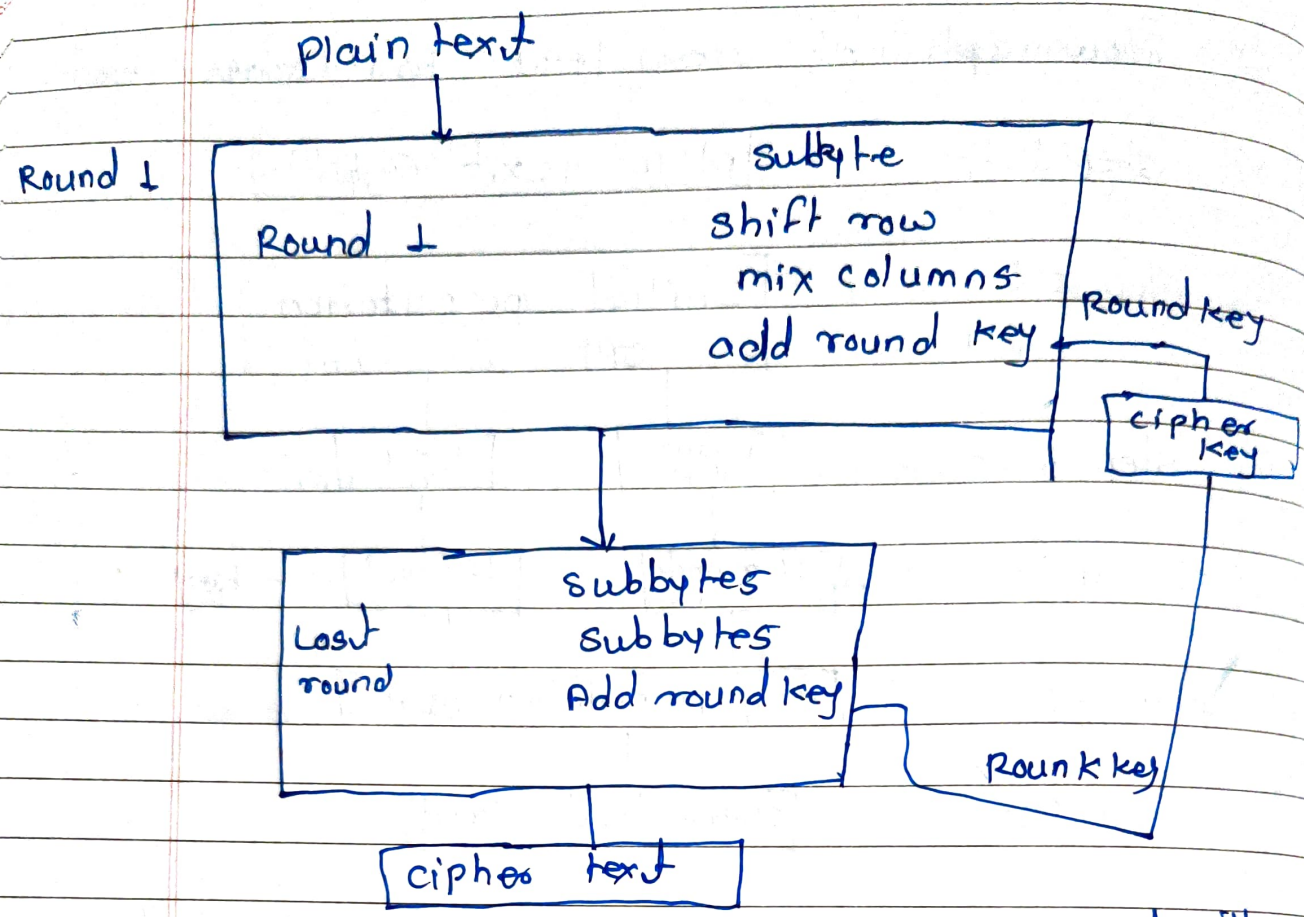
- substitution & transposition.

* flowgraph of plain text to cipher text.



Q] AES [Advance encryption standerd.]

- AES is specification for the encryption of electronic data estabilished by the U.S (NIST) in 2001
- stronger than triple des.
-
- AES is block cipher.
- the key size can be 128 | 192 | 256 bit
- encrypts data in blocks of 128 bits each
- i/p 128 bits & output cipher text 128 bits.
- No of rounds depend on key length
  128 key → 10 rounds.
  192 key → 12 rounds
  256 key → 14 rounds



hashing algorithm.

Message	MD5	SHA → secure				
→	128	160	160	256	384	512.
	2^{64}	2^{64}	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$	

Q.1 compare DES with AES algorithm.

Sr. No	AES	DES
1.	Advance encryption standard	Data encryption standard
2.	byte oriented key length can be 128, 192, 256 bits	The key length is 56 bit DES
3.	AES can encrypt 128 bit of plain text	DES can encrypt 64 bit of plaintext
4.	more sucure than triple DES	less secure than AES
5.	structure based on a substitution NW	the structure based on a feistel NW
6.	No. of rounds depends on key length eg. 10 rounds (128bit)	DES involes 16 rounds.

* advantages of ~~bbbb~~ blowfish algorithm

1. it is faster and much better than DES encryption.

2. it uses only primitive operations such as addition, xOR and table look-up, making its design and implementation simple.

3. The blowfish algorithm also has a lesser amount of operations to complete compared to other encryption algorithm.

4. Blowfish is fast block cipher except when changing key.

* disadvantages.

1. blowfish uses a 64-bit block size which makes vulnerable to attacks.

2. A reduced round variant of blowfish is known to be suseeptible to known plain text.

* Application.

1. Bulk encryption
2. Packet encryption (ATM Packet)
3. password hashing

* advantages of ~~bbor~~ blowfish algorithm

1. it is faster and much better than DES encryption.
2. it uses only primitive operations such as addition, XOR and table look-up, making its design and implementation simple.
3. The blowfish algorithm also has a lesser amount of operations to complete compared to other encryption algorithm.
4. Blowfish is fast block cipher except when changing key.

* disadvantages.

1. blowfish uses a 64-bit block size which makes vulnerable to attacks.
2. A reduced round variant of blowfish is known to be susceptible to known plain text.

* Application.

1. Bulk encryption
2. Packet encryption (ATM Packet)
3. password hashing

* RSA algorithm (Rivest Shamir adleman)

- RSA algorithm is asymmetric cryptography algorithm

- Asymmetric actually means that two different keys ie. public key and private key

RSA encryption algorithm.
- choose any 2 (large) prime number
- compute $n = p * q$
- compute $\phi(n) = (p-1) * (q-1)$
- choose e such that $1 < e < \phi(n)$ and $\phi(n)$ are coprime.
- compute a value for d such that $(d * e) \% \phi(n) = 1$
- public key is (e, n)
- private key is (d, n)
- the encryption of message m is $c = m^e \% n$
- the decryption of cipher text c is $m = c^d \% n$

example.

choose $p = 3$ & $q = 11$

compute $n = p * q = 33$

compute $\phi(n) = (p-1) * (q-1) = (3-1)*(11-1) = 20$

$e = 7$

$(d * e) \% \phi(n) = 1$ [$d = 3$ [$3 * 7$) $\% 20 = 1$

public key is $(e, n) = (7, 33)$

privat key is $(d, n) = (3, 33)$

the encryption of $m = 2$ is $c = 2^7 \% 33 = 29$

$c = 29$ is $m = 29^3 \% 33 = 2$.

Q. Compare public key encryption with conventional encryption.

Sr. No.	conventional. public key en	Public ~~conventional~~ key encryption.
1.	it is type of crypto-graphic system which uses a single key both encrypt the Message and decrypt it	it is a type of encryption scheme which instead of a single key, uses a pair of keys to encrypt the Messag and decrypt it
2.	The some secreate key is shared by the sender and the Recipend and must be kept secreate at all times.	The public can shared freely to anyone while the private key kept secreate & is known only the Recipient
	- Faster	- Slower.
3.	it is ~~more~~ less secure	it is more secure.

public key KU_b
private key KR_b

unit -III

Page No.
Date

* principle of public key crypto systems :-

- Public key cryptography is cryptographic technique that involes 'two distinct key' for encryption and decryption.
- thats why it is also known as asymetric key cryptography
- it is totally based on mathematic function.

* There are two basic principles of any cryptosystem.
  1) confidentiality
  2) authenticity

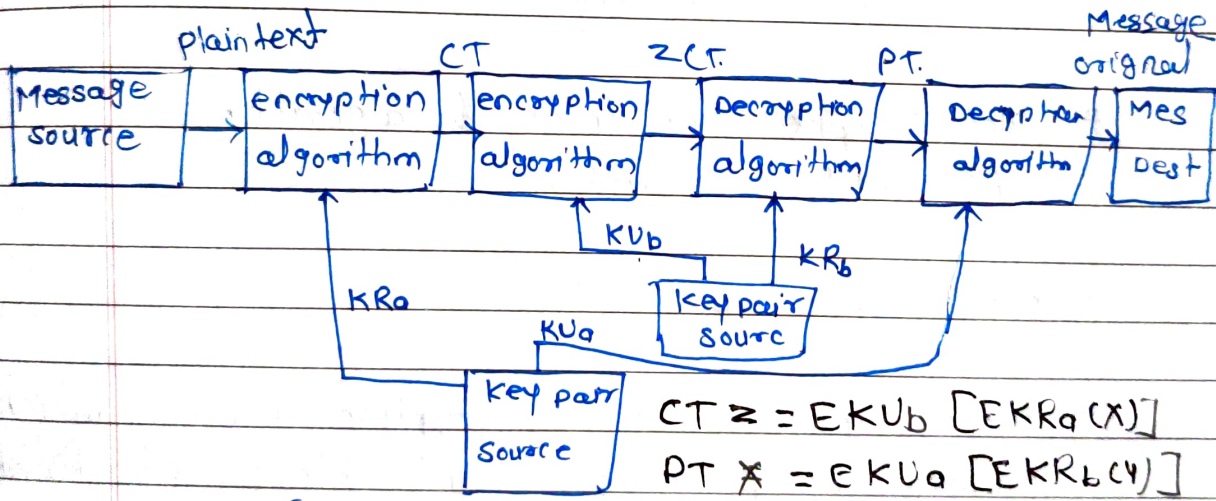


fig public key crypto system.

explanation points:
1. plaintext
2. encryption algorithm.
3. public and private keys.
4. cipher text
5. Decryption algorithm.

* Requirements of public key cryptosystem

- it is computationally easy for the Sender A knowing the public key and message to be encrypted M, to generate the corresponding ciphertext $C = E_{KU_b}(M)$
- it is computationally easy for Receiver B to decrypt the resulting ciphertext using the private key to Receives the original Message $M = D_{KR_b}(C) = D_{KR_b}[E_{KU_b}(M)]$

* public key cryptanalysis.
public key encryption scheme is vulnerable to a brute force attack. The counter measure is to use large keys.

* Block cipher principles & algorithm (DES, AES, Blowfish)

* Block cipher principles.

- Block cipher is an encryption method which divides the plain text into blocks of fixed size block has an equal number bits.
- at a time block cipher operates only one block of plain text and applies key on it to produce the corresponding block of ciphertext.
eg. Data encryption standard.

* Block cipher principles.

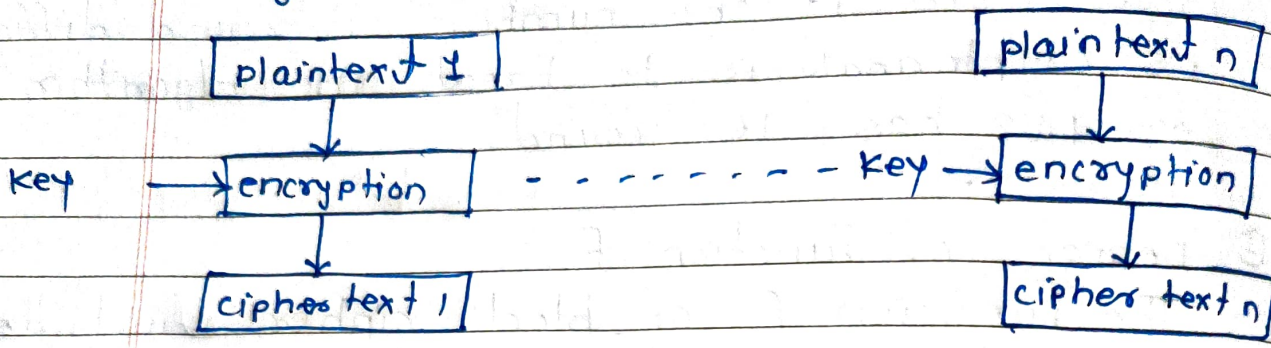
① Number of rounds :-
The number of rounds judges the strength of block cipher algorithm. it considered the that more it the number of round difficult is cryptoanalysis to break the algorithm eg. DES has 16 rounds.

② Design of function F
- The function F of block cipher must be designed such that it must be impossible for cryptanalysis to uncramble the substitution.
- The criterion that strengthens the fun F is it non-linearity
- more the function F is nonliner, more it would be difficult to crack it.
- while desiging the function F it should be conformed that it has good avalanche property which states that a change in one bit of input must reflect the change in one bits inputs reflect the change in many bits of output.

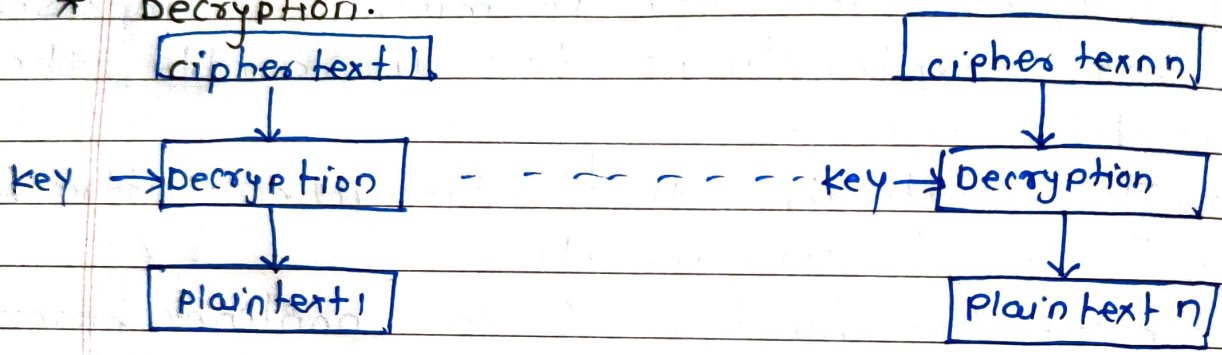
③ key schedule algorithm
- the fiestel block cipher structure, each round would generate a sub-key for increasing the complexity of cryptoanalysis
- the avalanche effect makes more complex in driving sub-key.

* Block cipher modes of operation.

1) electronic code book (ECB) :-
encryption.



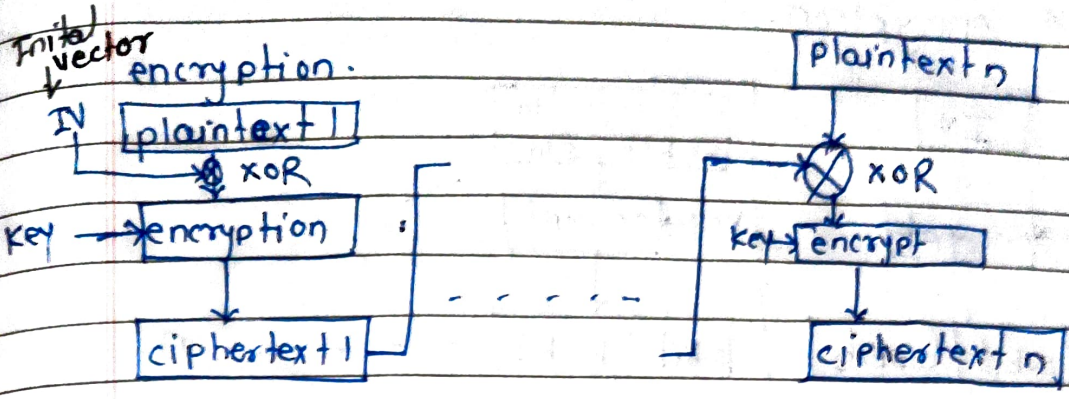
* Decryption.



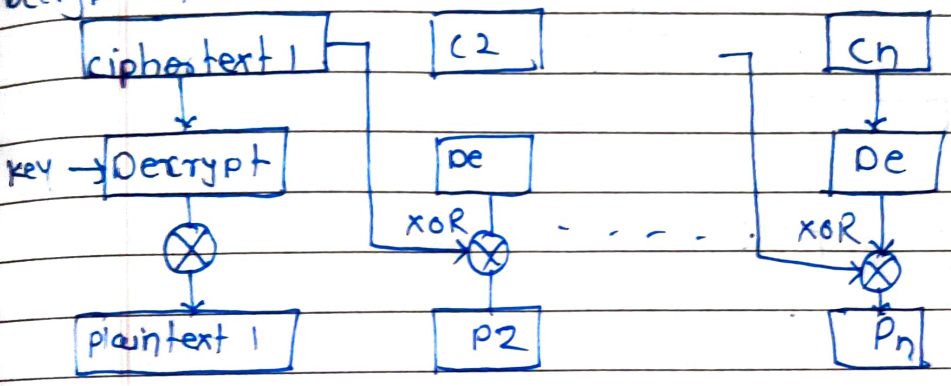
* Advantages of ECB
- Parallel encryption of blocks of bits is possible thus the faster way of encryption.
- Simple way of the block ciphers.

* Disadvantages of ECB
- prone to cryptanalysis since there is a direct relationship between plaintext & ciphertext.

② Cipher Block chaining



* Decryption



* Advantages of CBC :-

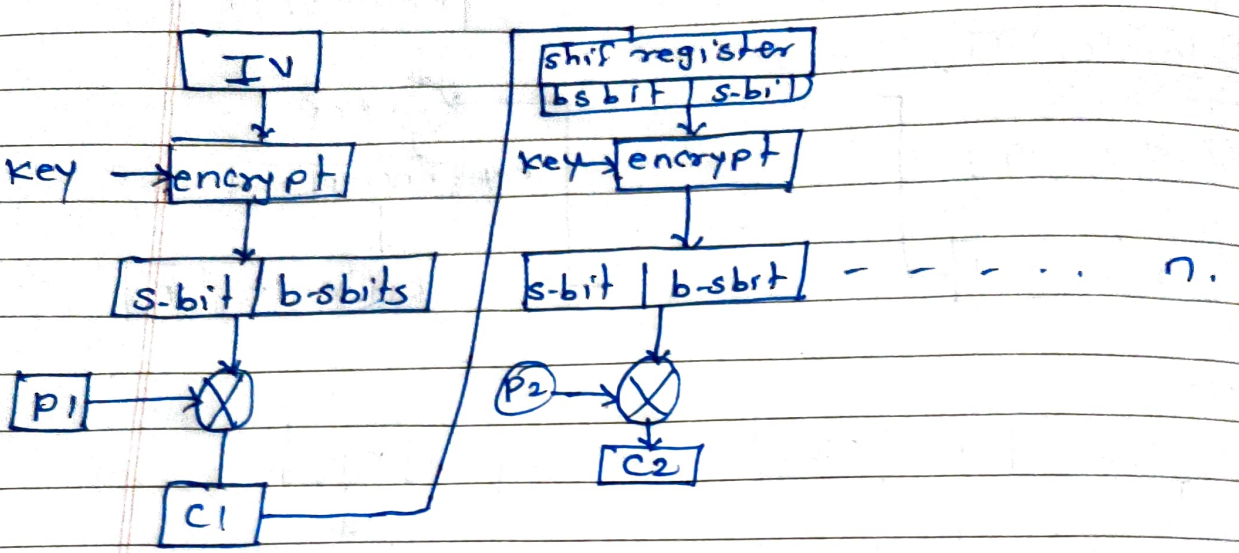
- CBC is a good authentication mechanism
- better cryptoanalysis than ECB
- CBC works well for input greater than b bits

* Disadvantages.

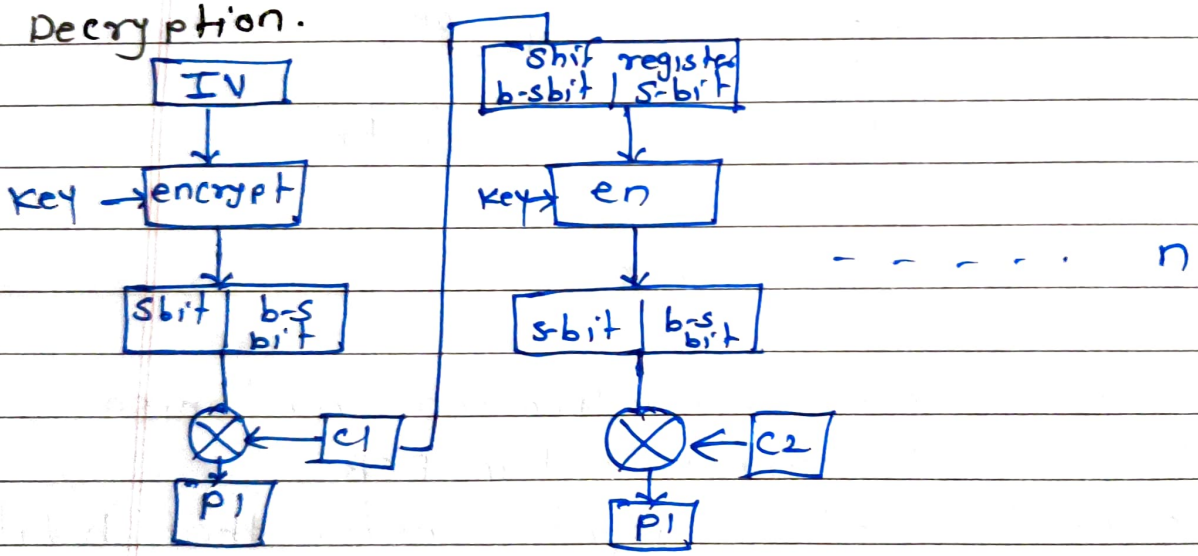
- parallel encryption is not possible since every encryption requires a previous cipher.

③ cipher feedback mode.

* encryption.



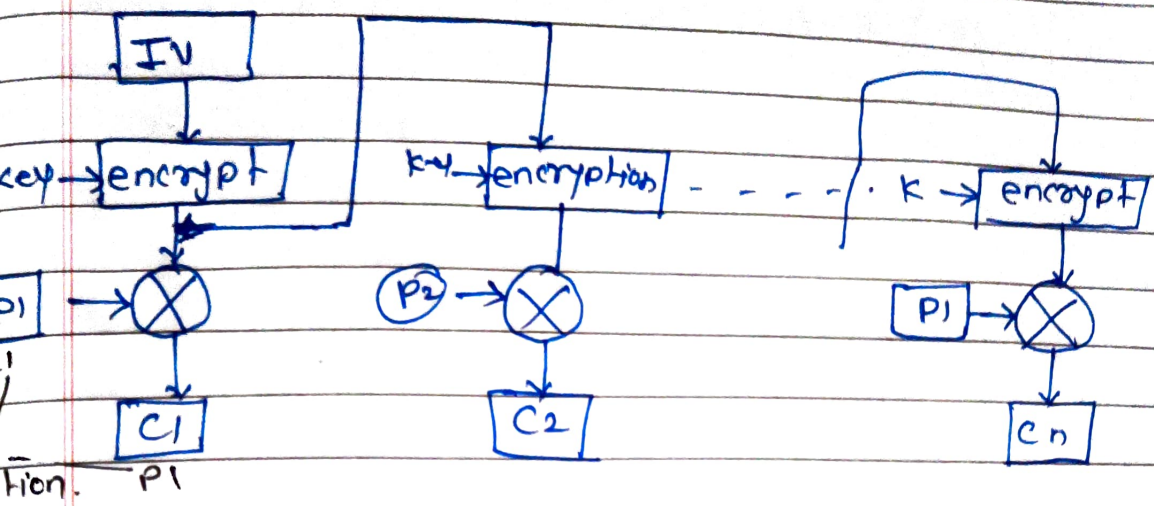
Decryption.



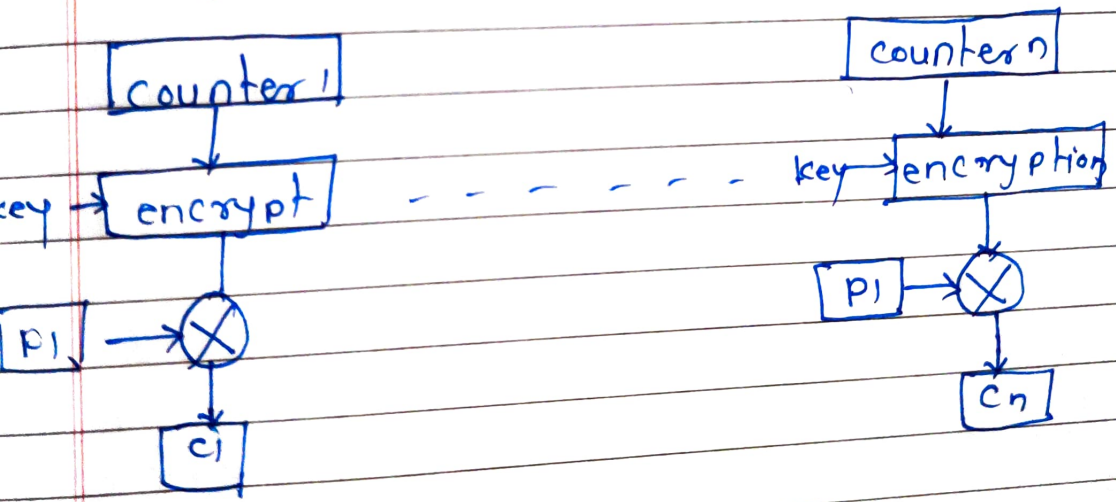
* Advantages-

- Since, there is some data loss due to the use of shift register, thus it is difficult for applying cryptonalysis.

④ output feedback mode.
encryption and decryption.



⑤ counter mode :-
encryption and ecryption.



Advantages:
1) plaintext can be map different ciphertext.