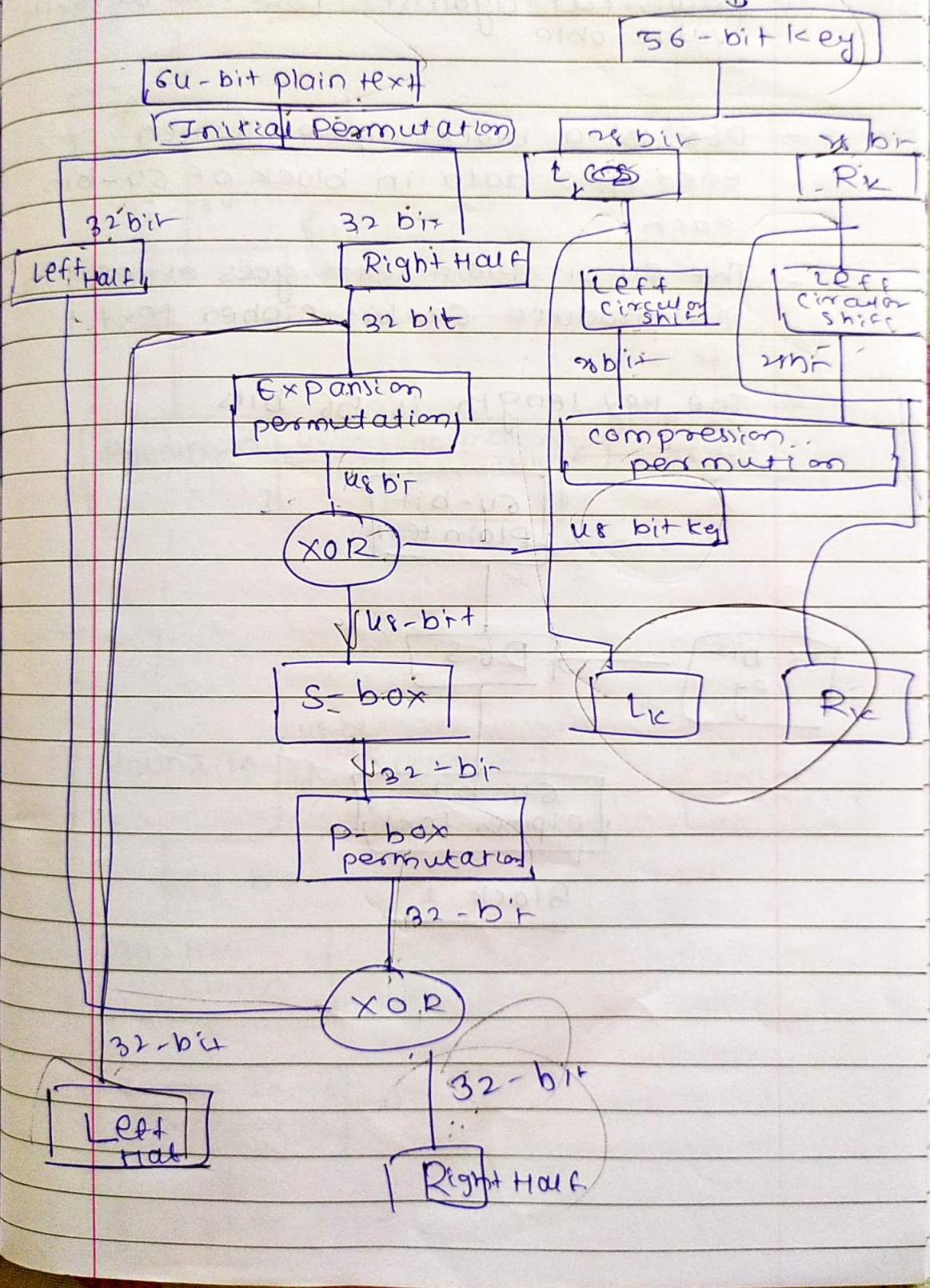
Page No.:
Date:

DES:-

Round Function in DES:-

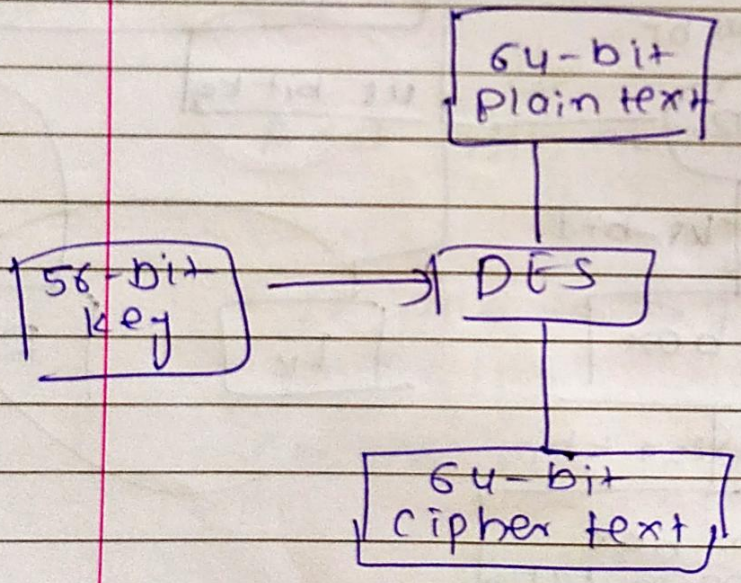


DES:-

- Data Encryption Standard.
- ~~powerful~~ vulnerable against powerful attacks.

- DES is a block cipher which encrypts data in block of 64-bits each.
- The 64-bit Plain text goes as input to DES produce 64-bit cipher text.

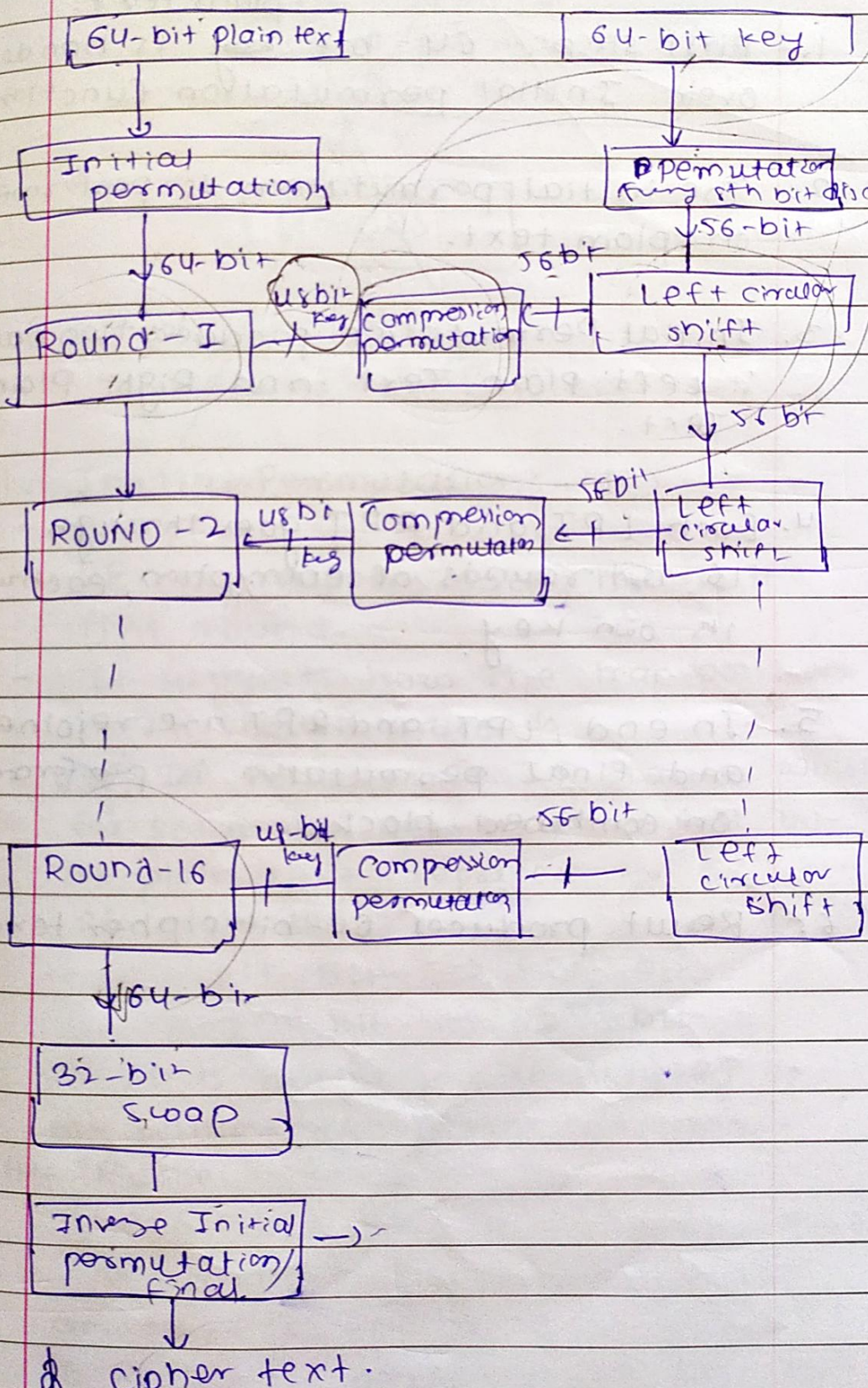
- The key length is 56 bits



Block 1

Page No.:
Date:

Block Diagram of DES:-



Page No.:
Date:

Steps in DES:-

1. First step:- 64-bit ~~key~~ plain text is handed over Initial permutation function.

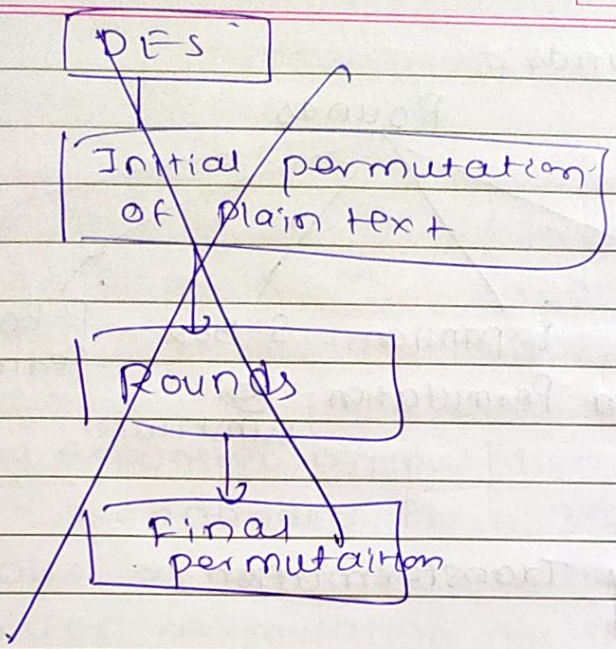
2. The initial permutation is performed on plain text.

3. Initial Permutation produces two halves :- Left Plain Text and Right Plain Text.

4. Each LPT and RPT goes through 16 rounds of encryption, each with its own key.

5. In end, LPT and RPT are rejoined, and Final permutation is performed on combined block.

6. Result produces 64-bit cipher text.



1. Initial Permutation :- (IP)

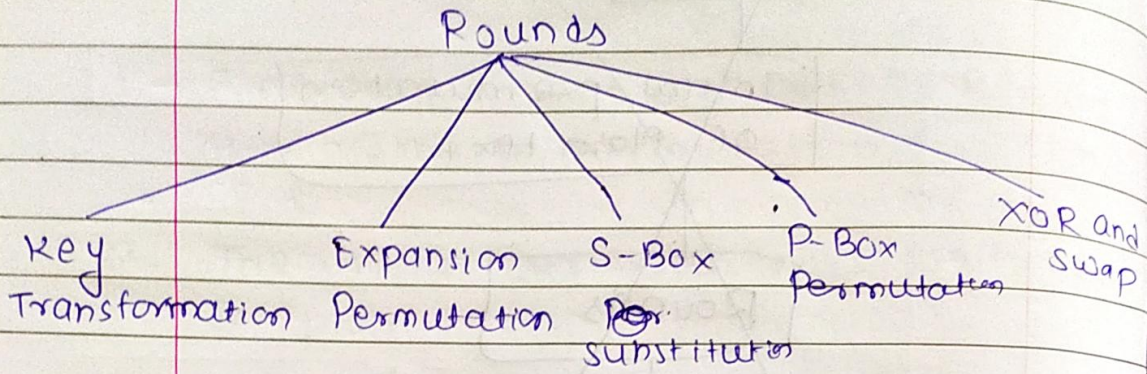
- IP only happens once, before the first round.
- It suggests how the transposition in IP should proceeds
- ~~Eg~~. IP follows the IP table which for example says that 1st bit of plain text replaced by 58th bit of plain text

  1st bit → 58th bit
  2nd bit → 50th bit
- So IP is nothing but juggling of bit positions of plain-text block.

After IP done,
- the 64-bit permuted text block is divided into two half-blocks. Each block consists of 32-bit as LPT and RPT. 16 Rounds are performed on these two blocks.

Page No.:
Date:

2. Rounds :-



1. Key Transformation :-

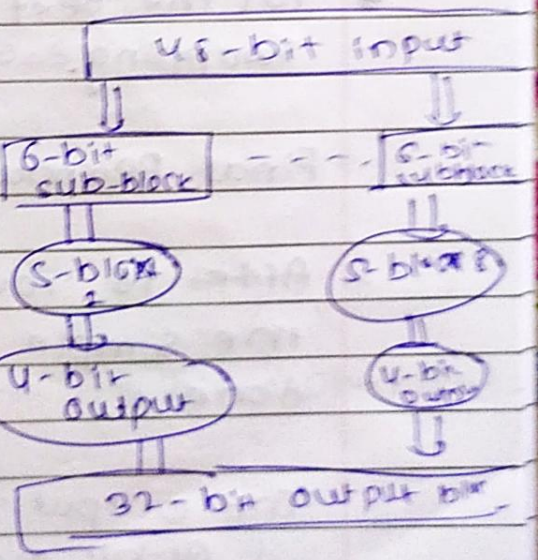
- Initially, the 64-bit key is transformed into 56-bit key by discarding every 8th bit of key.
- From 56-bit key, different 48-bit subkeys is generated during each round. This procesr is called key Transformation.
- This 56-bit key is divided into two halves, each of 28 bit. Each halves is circularly left shift.
- After circular shift, 48 of 56 bits are to be selected. So, this procesr of permutation as well as select of 48-bit key is called compression permutation.

2. Expansion Permutation :-

- After Initial permutation, two 32-bit plain text blocks i.e. Left Plain Text (LPT) and Right Plain Text (RPT).
- During expansion permutation, the RPT is expanded from 32 bits to 48 bits. as well permutated, hence expansion permutation.
- Now the 48-bit RPT is XORed with the 48-bit key that is compressed while the key transformation process, and output is given next step, i.e. S-box substitution.

3. S-box permutation :-

- The 48-bit input is divided into 8 6-bit sub-blocks.
- This sub-blocks given to S-box which gives 4-bit output.
- All 4-bit output combines to gives the 32-bit output block.



4. P-box Permutation:-

- The output of 32-bit S box is given to P-box.
- P-box involves simple permutation i.e. each bit replaces with another bit. This is called p-box permutation.

5. XOR and swap:-

- Now the output 32-bit P-box is XORed with the Left Half Plain text of 32-bit which was untouched so far.
- This result of XOR operation is the new right half of the next round. and right half becomes left half for the next round. This process is swapping.

Final Permutation:-

- After 16 rounds of encryption, the simple final permutation is done.
- The output of final permutation is 64-bit cipher text.

Page No.:
Date:

DES Decryption:-

- The algorithm used for encryption in DES also works for decryption.

- The only diff. betw the encryption and decryption process is reversal of key portion.

- If original key K was divided into K1, K2, K3 .. K16 for 16 encryption rounds, then for decryption, the key used as K16, K15, K14 .. K1.

Block-size → 64-bit Plain Text

No. of. Rounds → 16 Rounds

Key-Size → 64 bit

No. of Sub keys → 16 sub keys

Sub key size → 48 bit sub key

Cipher Text → 64 bit cipher text.

AES:-

- Advanced encryption standard.

Block size → 128 bit plain text (4 words) 16 bytes

No. of Rounds → 10 Rounds

key size → 128 bit (4 words / 16 Bytes)

No. of subkeys → 44 subkeys

Each subkey size - 32 bit / 1 word / 4 Bytes.

Each Round - 4 subkeys (128 bit 4 words) 16 Bytes

Pre Round calculation - 4 subkeys (128 bit / 4 words) 16 Bytes)

cipher Text — 128 bit.

Page No.:
Date:

* RC4:-4

- RC4 - Ronald Rivest.
- A symmetric key encryption algorithm
- Stream cipher.
- used in data communication and networking protocol.
- RC4 generates a pseudorandom stream of bits called keystream. This is combined with the plain text using XOR for encryption.

~~Process~~ :-

1. ~~Initialization~~ of
- It uses an S array of length 256 where S[0] = 0 to S[255] = 255.

Process :-

1. Initialization of S
2. Stream generation.

1. Initialisation of S :-

1. Choose key of length between 1 to 256 bytes.

2. Set values of S array as S[0] = 0 to S[255] = 255.

3. Create another temporary array T. length of T should be equal to S array and all elements of key should be copied in T. The remaining positions should also be filled with values of K again. T should be completely filled.

e.g. If S = [0 1 2 3 4 5 6 7]
K = [1 2 3 6]
then, T = [1 2 3 6 1 2 3 6].

4. Now, the initial permutation happens with key scheduling algorithm. The algorithm is as follows:-

```
j = 0
for i = 0 to 255
    j = (j + S[i] + T[i]) mod 256
    swap (S[i], S[j])
```

1. Stream Generation:-

- For stream generation, it uses key stream generation algorithm. The algorithm is as follows:-

```
i = j = 0
while (true)
    i = (i + 1) mod 256
    j = (j + S[i]) mod 256
    swap ( S[i], S[j] )
    t = (S[i] + S[j]) mod 256
    keystream = S[t];
```

- After this, for encryption, the keystream is XORed with the plain text.

- For decryption, keystream is XORed with the cipher text.

Blowfish :-

- ~~developed by~~
- Symmetric.

- Some properties :-
  1. fast
  2. Compact → executs in less memory
  3. simple → XOR, addⁿ.
  4. Secure → variable length

- Blowfish algorithm encrypts 64-bit block with variable length key [32 - 448 bits]

- Blowfish algorithm :-
  1. Sub key Generation.
  2. Data Encryption.

1. Subkey Generation :-

- In blowfish, variable length keys ranging from 32 bit to 448 bits are used. The key ranges from 1 to 14 words which is stored in array :

  $K_1, K_2, \ldots K_n ; n \leq 14$

- Another P-array consisting of 18 32-bit sub-keys is used.

  $P_1, P_2 \ldots P_{18}$.

- Four S-boxes each containing 256 32-bit entries:

  $S_1 \rightarrow S_0 \ldots S_{255}$

  $S_2 \rightarrow S_0 \ldots S_{255}$

  ⋮

  $S_4 \rightarrow S_0 \ldots S_{255}$.

- Initialize P-array and S-boxes with the fixed string with use of hexadecimal form of Pi (π).

- bitwise XOR of P_1 with k_1, P_2 with k_2, ... until key exhausted then again P_{15} with k_1 ... so on.

  $P_1 = P_1 \text{ XOR } k_1$

  $P_2 = P_2 \text{ XOR } k_2$

  ⋮

  $P_{15} = P_{15} \text{ XOR } k_1$

  ⋮

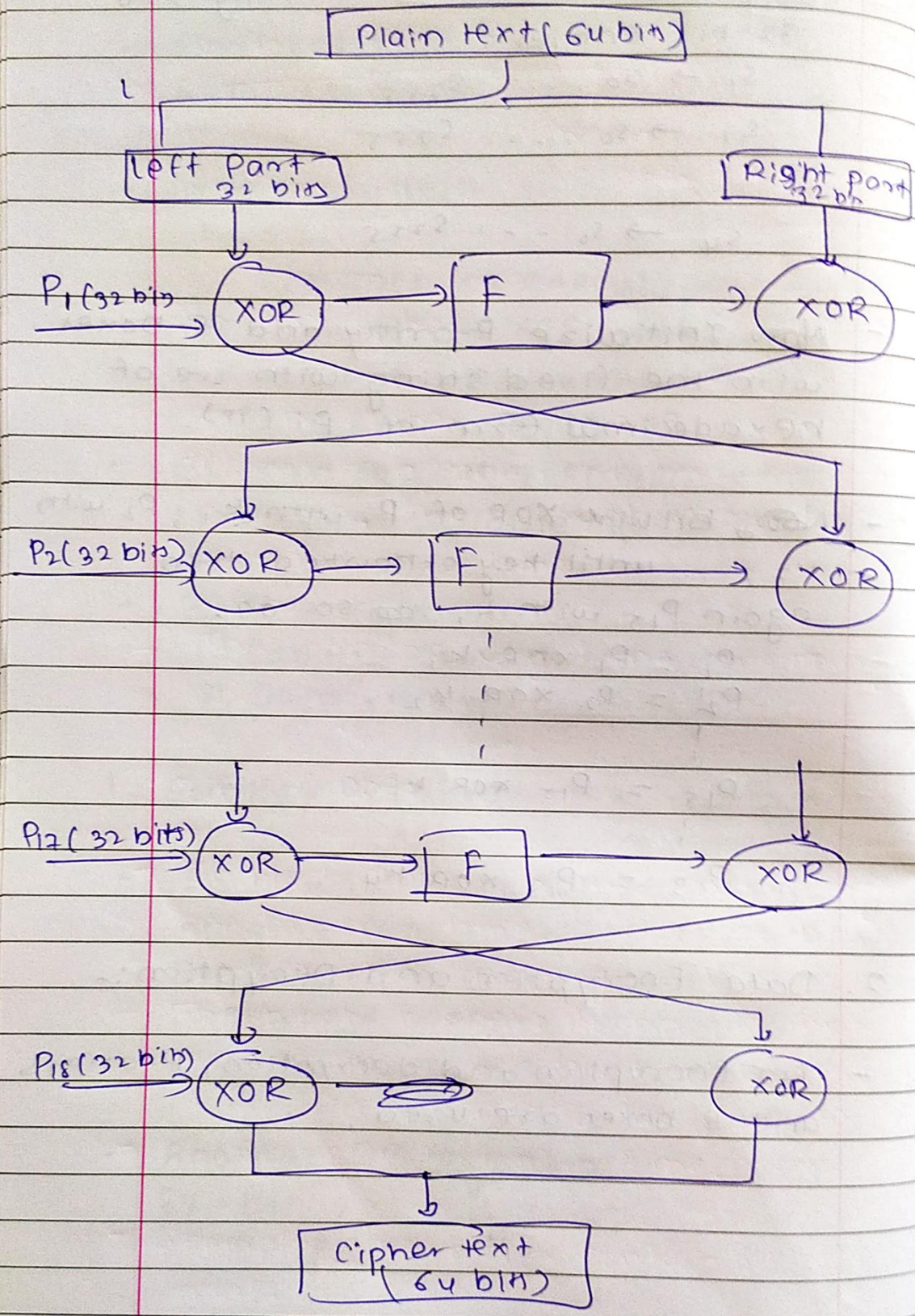
  $P_{18} = P_{18} \text{ XOR } k_4$.

2. Data Encryption and Decryption:-

- For Encryption and decryption, P-arrays and S-boxes are used.

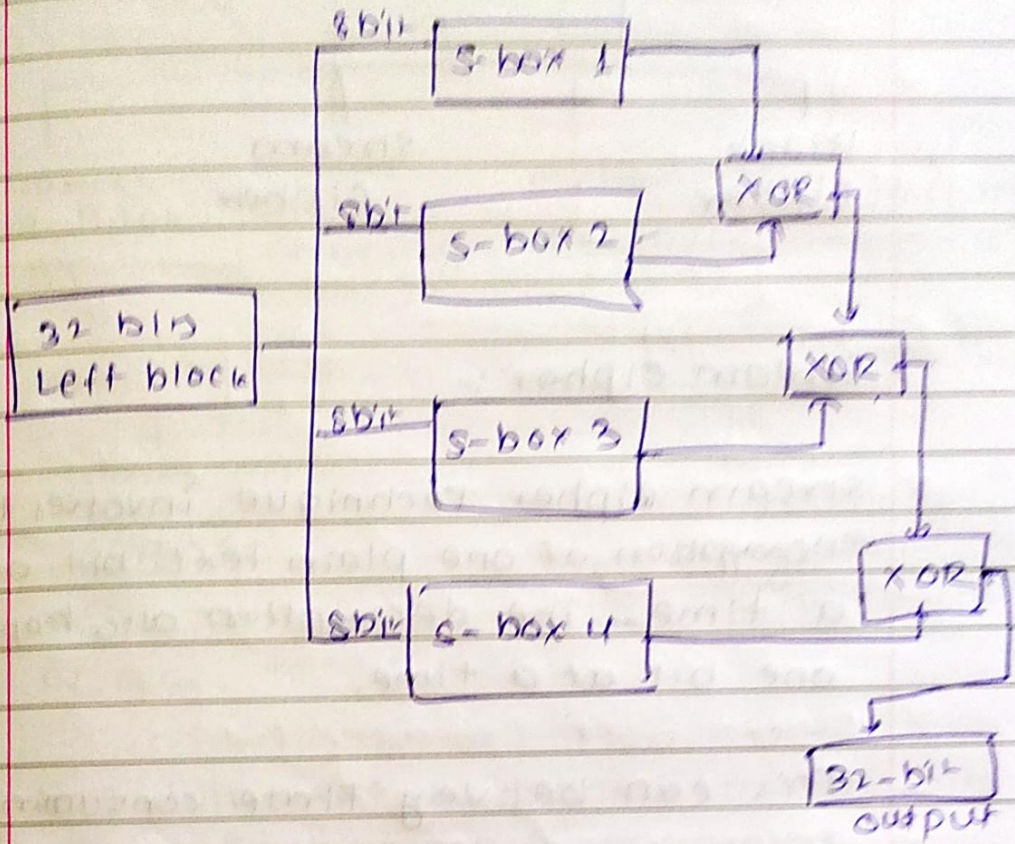
Page No.:
Date:

Block Diagram of Blowfish encryption:



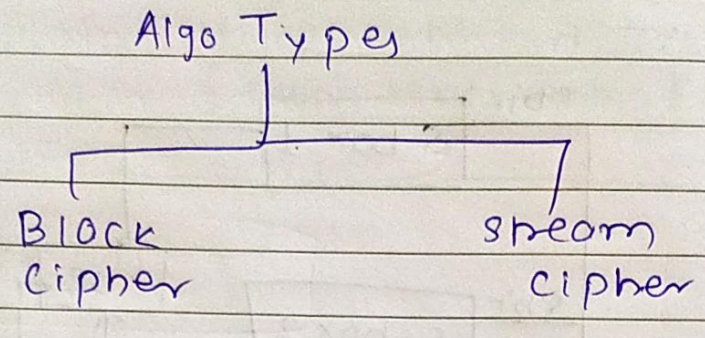
Page No.:
Date:

Now, the function F is shown as follows :-



- For decryption, same P-arrays are used with $P_{17}, P_{16}, \ldots P_1, P_0$ order.

* ~~Block~~



Stream Cipher :-

- Stream cipher Technique involves the encryption of one plain text bit at a time. The decryption also happens one bit at a time.

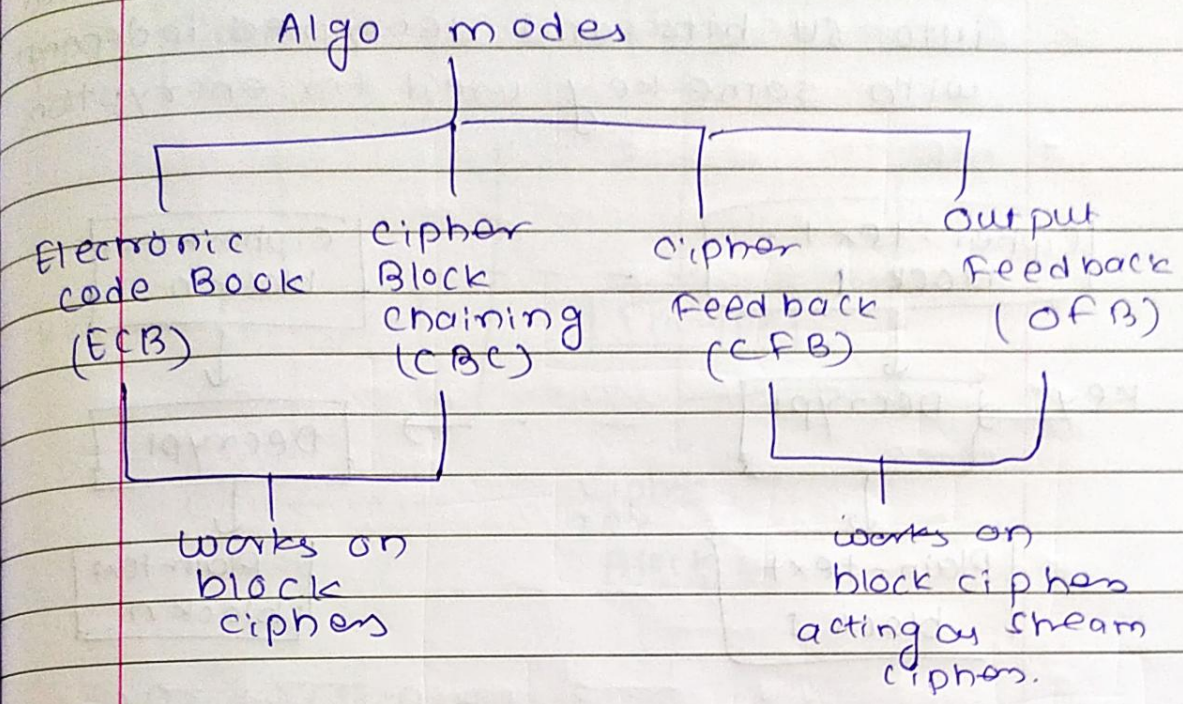
- This can be very time consuming.

Block Cipher :-

- In block ciphers, rather encrypting one bit at a time, a block of bits is encrypted at one go.
- The block-ciphers technique involves encryption of one block of text at a time. Decryption also takes one block of encrypted text at a time.

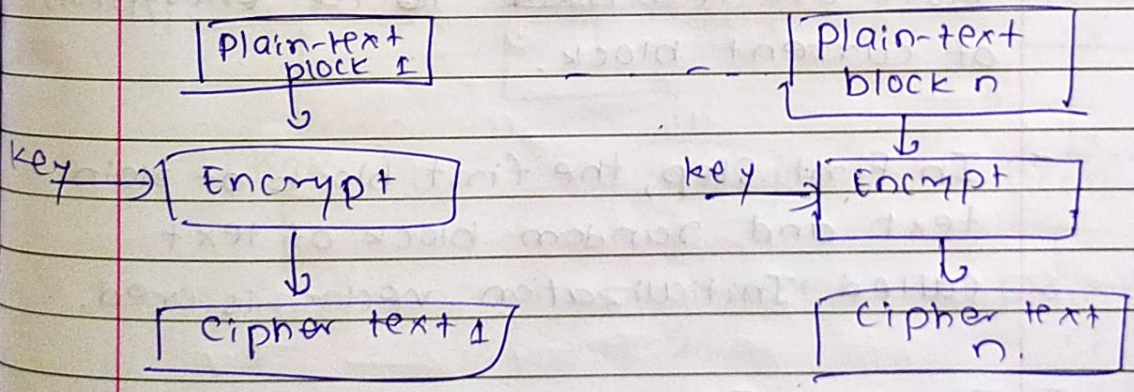
- Generally, the blocks contain 64 bits or more.

Page No.:
Date:

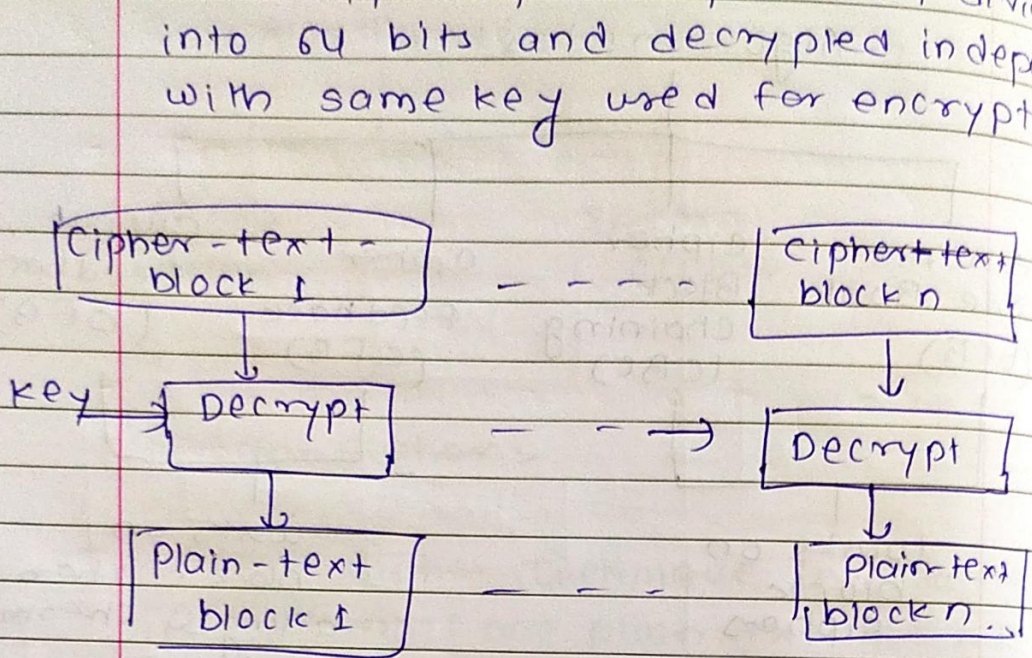


1. ECB:-

- The plain-text is divided into 64 bits each. Each block is encrypted independtly with the same key.

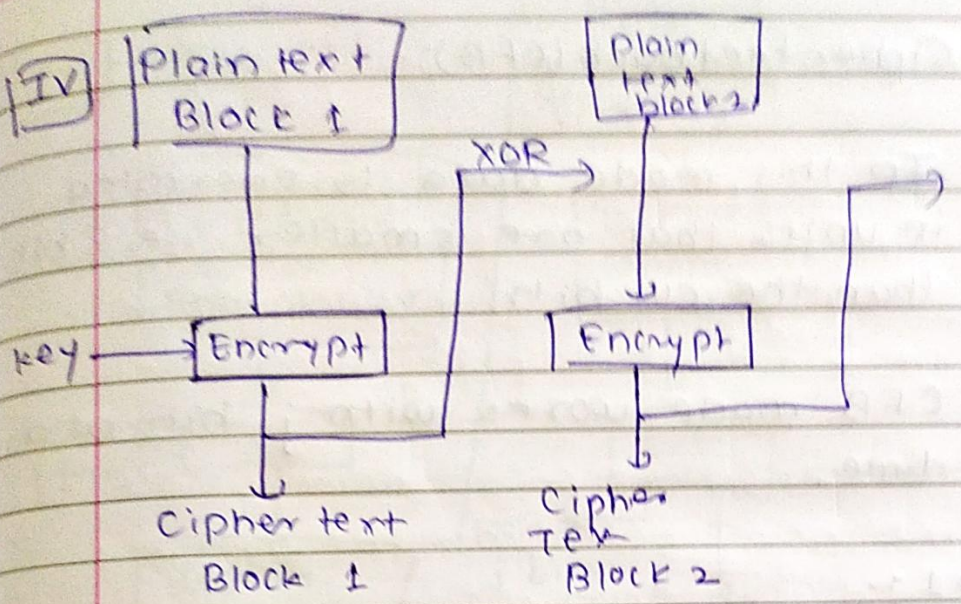


for Decryption, the cipher text divided into 64 bits and decrypted independently with same key used for encryption.

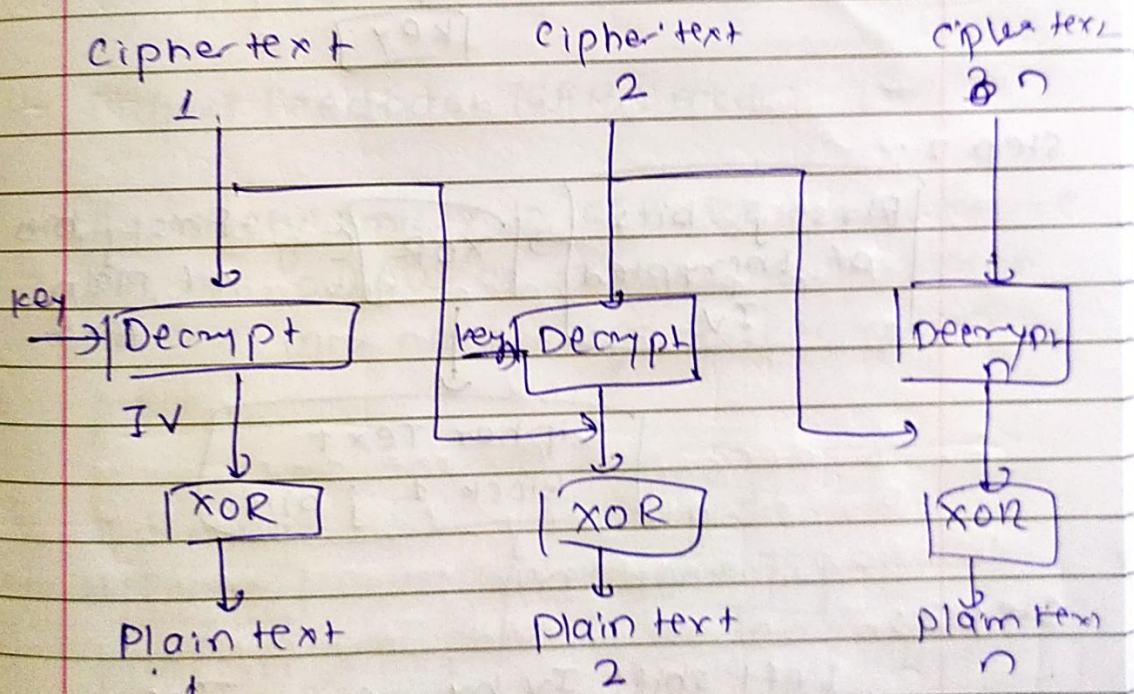


2. Cipher Block Chaining (CBC) :-

- Chaining adds a feedback mechanism to block cipher.
- The result of encryption of previous block are fed ~~back~~ into to the encryption of current block.
- In first step, the first block of plain text and random block of text called Initialization vector is used.
- The value IV is generated randomly.


IV
Plain text Block 1
Plain text block 2
XOR
key
Encrypt
Encrypt
Cipher text Block 1
Cipher Text Block 2

Decryption :-

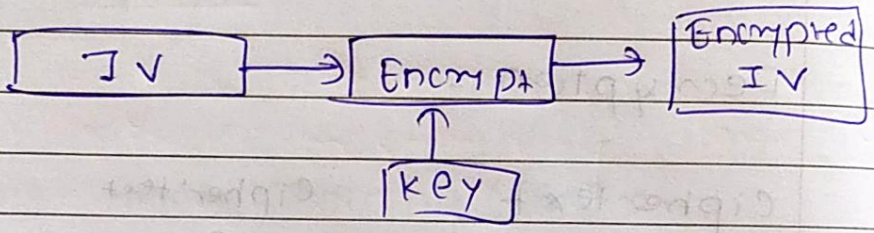

Ciphertext 1
Ciphertext 2
Ciphertext n
key
Decrypt
key
Decrypt
Decrypt
IV
XOR
XOR
XOR
Plain text 1
Plain text 2
Plain text n

3. Cipher feedback (CFB):-

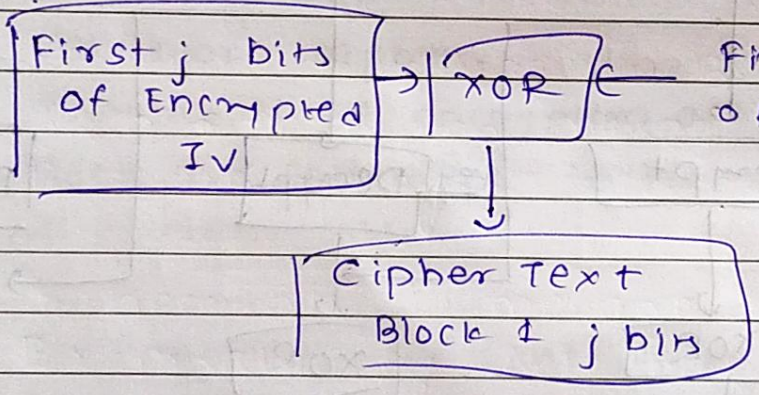
- In this mode data is encrypted in units that are smaller i.e. 8 bits than the 64 bits.

- CFB mode works with j bits at a time.

Step 1:-



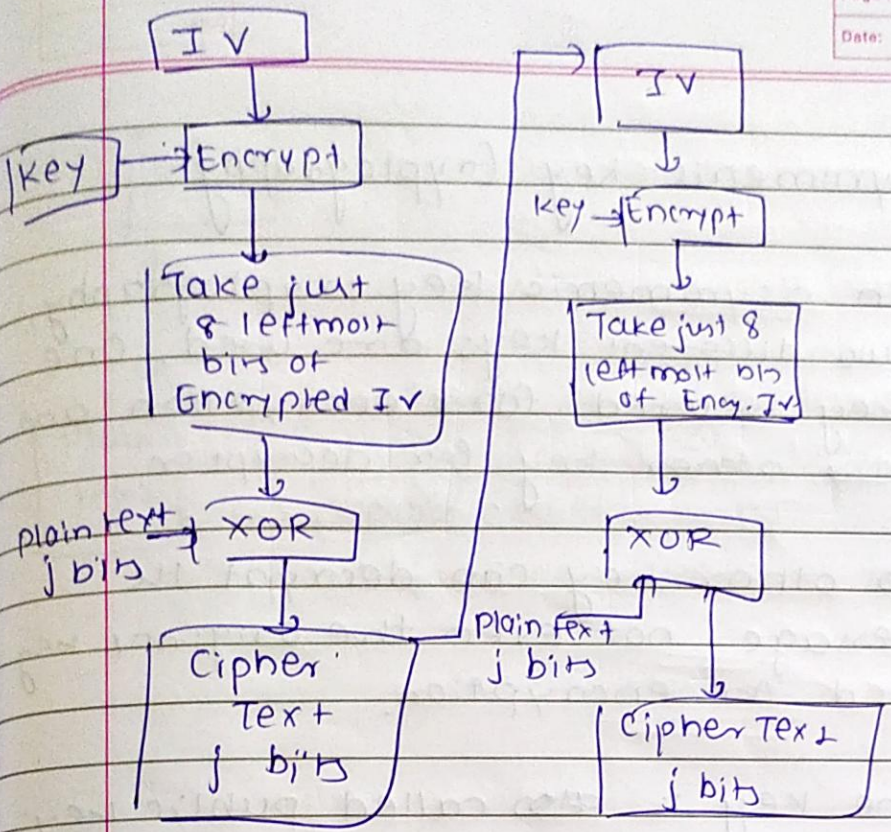
Step 2:-



Step 3:-

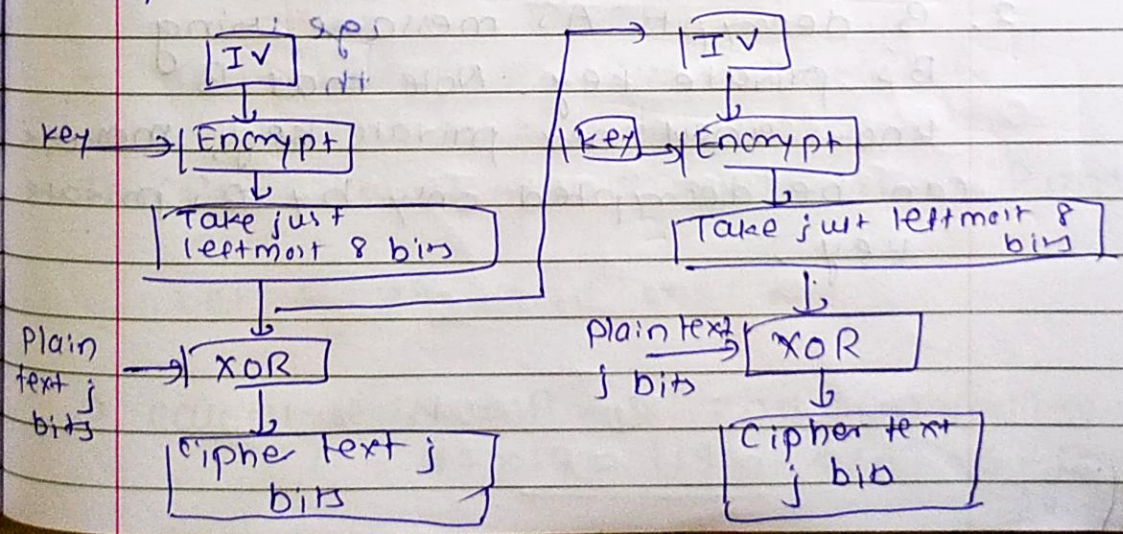
Left shift IV by j positions ← IV

IV ← move j bits of cipher text into the rightmost of IV



4. Output Feedback (OFB) mode:

- Extremely similar to CFB. The only difference is the output of IV encryption process is fed into next stage of encryption process.



Page No.:
Date:

Asymmetric-key Cryptography:

- In asymmetric key cryptography, two different keys are used. One key is used for encryption and other key for decryption.

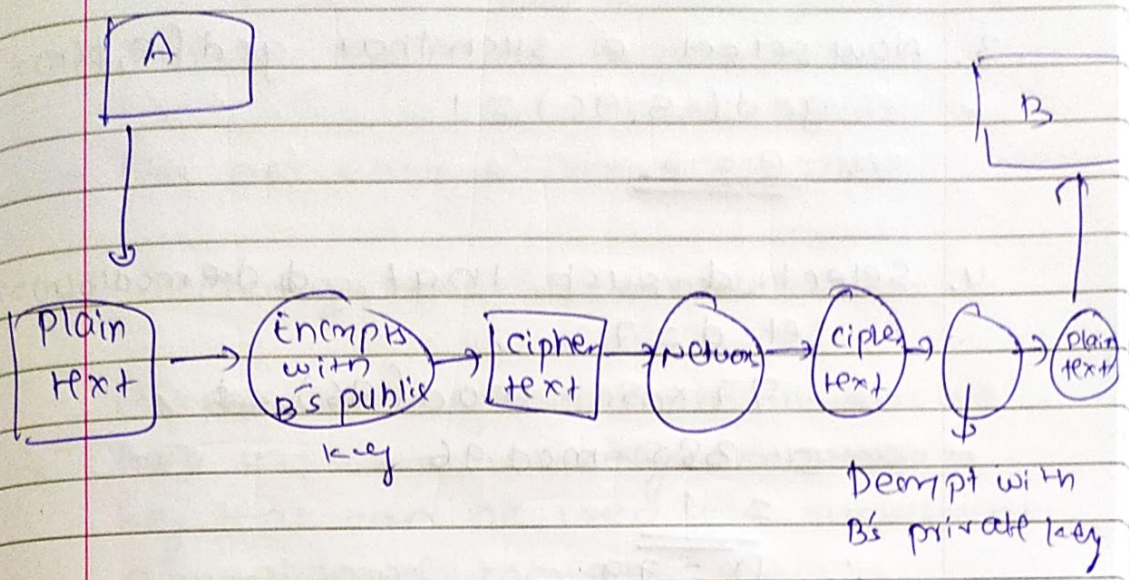
- No other key can decrypt the message not even the original key used for encryption.

- One key is called public key and other is private key.

It works as follows:-

1. A sends a message to B with encrypted message using B's public key.

2. B decrypts A's message using B's private key. Note that B knows about her private key. message can be decrypted only by B's private key.



* RSA Algorithm:-

- The RSA Algorithm is based on large prime number.

- The private and public keys in RSA are based on very large prime numbers.

- The algorithm is as follows:-

1. Choose two large prime numbers, P and Q.
   Let P = 17 and Q = 17.

2. Calculate $N = P \times Q$ and $\phi(n) = (p-1)*(q-1)$
   $N = 17 \times 17 = 119$ $\phi(n) = 6 \times 16 = 96$

3. Now select e such that $gcd(e, \phi(n)) = 1$

$gcd(5, 96) = 1$.

$\therefore e = 5$

4. Select d such that $d \times e \bmod \phi(n) = 1$

let $d = 77$

$= 77 \times 5 \times \bmod(96)$

$= 385 \bmod 96$

$= 1$.

$\therefore D = 77$

5- For encryption calculate Cipher Text C from plain text P as :-

$C = P^e \bmod n$.

let $P = 10$

$C = 10^5 \bmod 119$

$C = 40$

6. Now for decryption, calculate Plain Text from Cipher Text

$P = C^d \bmod n$

$= 40^{77} \bmod 119$

$P = 10$

Page No.
Date:

Key Exchange.

* Diffie-Hellman Algorithm:-

- Not an encryption algorithm
- Exchange secret/symmetric key.
- Purpose of algorithm is to enable two users to securely exchange a key that can be used for subsequent encryption of messages.
- Algorithm is limited to exchang of secret values.

Algorithm:-

Global public elements

q — prime number

α — $\alpha < q$ and α should be primitive root of q

Primitive root:- If α is primitive root of prime no. p, the numbers

$\alpha \bmod p, \alpha^2 \bmod p, \alpha^3 \bmod p \dots \alpha^{p-1} \bmod p$

are distinct and ranging from 1 to $p-1$.

Page No.
Date

User A key Generation

select private X_A $\quad X_A < q$

Calculate public Y_A $\quad Y_A = (\alpha)^{X_A} \bmod q$

User B key Generation

select private X_B $\quad X_B < q$

Calculate public Y_B $\quad \Rightarrow Y_B = (\alpha)^{X_B} \bmod q$

Calculation of Secret key by User A.

$$K = (Y_B)^{X_A} \bmod q.$$

Calculation of Secret key by User B.

$$K = (Y_A)^{X_B} \bmod q.$$

E-mail security

- Email is perhaps the most widely used application on Internet

Using Email, an Internet user can send a message to other Internet users. Therefore, Email security has become an extremely important issue.

- An email message is considered to made up of two portions: it's contents and headers.

- An email message consists of no. of header lines followed by the actual message content.

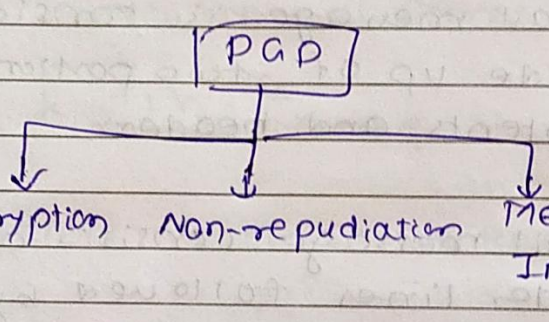
- An header line usually consists of keyword, followed by colon, followed by keywords arguments. Header keywords can be from, To, Subject and Date.

Page No.:
Date:

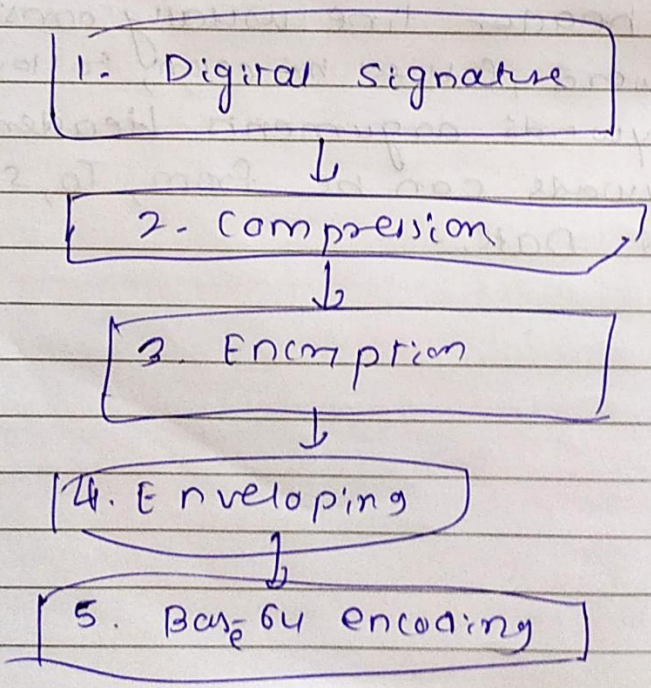
Pretty Good Privacy (PGP) :-

- The aspects of PGP are that it is supports basic requirements of cryptography, is quite simple to use, and is completely free, including it's source code and documentation.

- The email cryptographic offered by PGP :-



- The steps in PGP are :-



- PGP allows ~~for~~ three ~~four~~ following security options:-

1. Signature only.
2. Signature and Base-64 encoding.
3. Signature, Encryption, Enveloping and Base-64 encoding.

Step 1:- Digital signature

- In PGP, it consists of creation of message digest of email message using SHA1 algorithm.
- The resulting message digest is then encrypted with sender's private key. The result is sender's digital signature.

Step 2:- Compression:-

- Additional step in PGP.
- input message and digital signature are compressed together to reduce the size of final message that will be transmitted.
- ZIP program is used.

Step 3:- Encryption

- The compressed output of step-2 are encrypted with symmetric key.
- Generally, IDEA algo. of CFB mode is used.

Step 4:- Digital Enveloping.

- Output of Step 3 is now encrypted with receiver's public key.
- The output of step 3 and step 4 togeter form digital envelope.

Step 5:- Base-64 encoding,

- The output of Step 4 is now encoded with base-64.

Page No.:
Date:

Secure multipurpose Internet Mail Extensions (S/MIME):-

- The traditional email systems using SMTP protocol are text based, which means we can send only text messages but not multimedia files, etc.

- MIME System extends the basic email system by permitting users to send binary files using basic email system.

- A MIME email message contains a normal Internet text message along with some special headers and formatted sections of text.

- In header, the contenttype MIME header shows that the sender has attached a multimedia file to message.

- Header of MIME contain:-

1. MIME version :- contains version number.

2. Content-Type :- Describes data contained in body of message
The content are specified as
Type/subtype

3. Content - Transfer - Encoding :-

- Specifies the type of Transformation that has been used to represent the body of message.

- Five content - encoding - methods :-
  7-bit, 8-bit, Binary, Base-64, Quoted Printable

4. Content ID.
5. Content Description.

- Functionality of S/MIME is quite similar to PGP. It offers functionalities as :-

1. Enveloped data
2. Signed data.
3. clear - signed data
4. Signed and Enveloped data.

- Algorithms used in S/MIME :-

Message Digest	- SHA1
Digital signature	- DSS, RSA.
Enveloping	- Diffie-Hellman, RSA.
Symmetric key Encryption	- RC4, DES 3.

Page No.:
Date:

IP Security :-

- The IP packets contain data in plain text format.

- Anyone watching IP packets can actually change them, read their contents.

- So to secure IP packet we have protocols

Applications of IP sec :-

1. Remote Internet Access :- Using IPsec, we can connect to organization's network in secure fashion from our home or hotel. we can access corporate network facilities or access remote desktop / servers.

2. Secure Branch Office Connectivity :- Organization can set up IPsec-enabled network to securely connect all its branches over Internet.

3. Setup Communication with other Organizations :- Organization can connect the networks of different org. together in secure fashion.

Advantages:

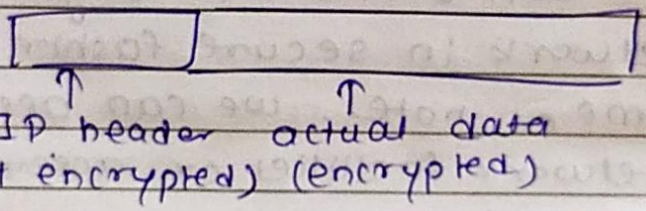
1. IPsec allows interconnectivity between branches/offices in very inexpensive manner.

2. IPsec can allow traveling staff to have secure access to corporate network.

3. IPsec is transparent for end users.

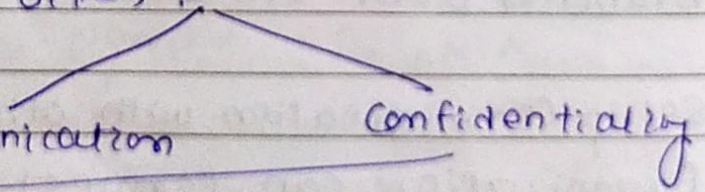
4. IPsec works at network layer. Hence, no changes are needed to upper layers.

- IP packets has: IP header and actual data



- IPsec features are implemented in extension headers which follows standard IP header.

- IPsec offers:



- Each has it's own extension header.

Page No.:
Date:

Protocols

- **Authentication Header**
  - provides authentication and integrity
- **Encapsulating security Payload (ESP)**
  - provides confidentiality

IP Architecture.