1) Explain with a neat diagram working of DES algorithm

→ The Data encryption standard is also called Data Encryption Algorithm : By ISO has been a cryptographic ~~alg~~ algorithm used for over two decades The origin of DES go Back to 1972 When in the US the national Bureau of Standards (NBS) - Nowadays, known as national Institute of standards, and Technology embarked upon a project for protecting the data in Computers and Computer Communication . Towards the end of 1976, the US federal government decided to adopt this algorithm as soon it was ~~se~~ renamed as 'Data Encryption standard'. The other bodies also recognized and adopted DES as cryptographic algorithm.

How the DES Works:

Broad-level steps for DES-

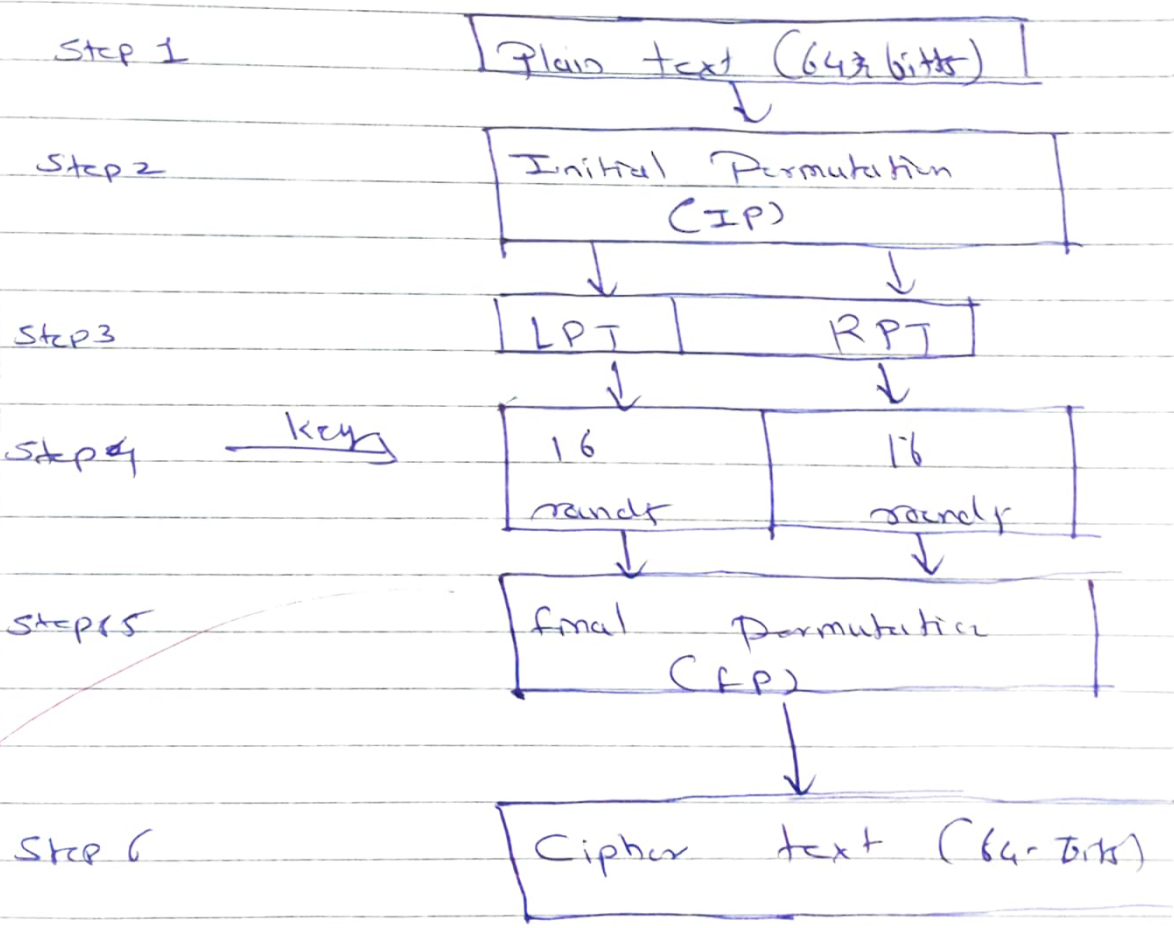
(i) 64-bit plain text block Handed over to Initial Permutation (IP) function.

(ii) After Initial permutation the IP produces two Halves of the permuted block, one : left plain text (LPT) and Right Plain text (RPT)

(iii) Each LPT and RPT go through 16 rounds of encryption process.

(iv) In the end, LPT and RPT are rejoined and a final Permutation (FP) is performed on the Combined block.

(v) The result of this process produces 64-bit Cipher text



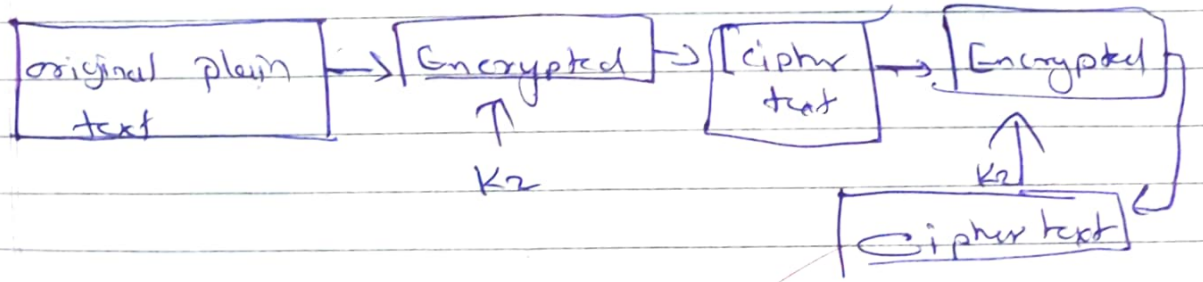
2) Explain two variations of DES

→ In variation of DES, there are two main variation

1) Double DES
2) Triple DES

1) Double DES

Double DES is quite simple to understand essentially. It does twice what DES normally does only once, Double DES uses two keys say K1 and K2. It performs DES on the original plain Text using K1 to get the encrypted Text But this time with the other key that is K2, The final output is the encryption of encrypted text. (that is the original plain text) encrypted twice with two different keys.

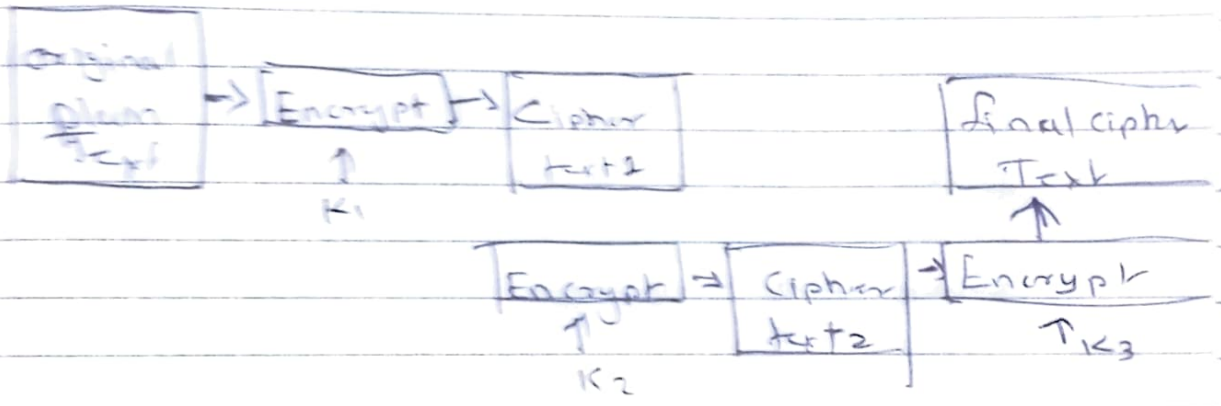


2) Triple DES

Triple DES is DES three times, It comes in two flavours. one that uses three keys and other that uses two keys.

Triple DES with three keys K1

1) Encrypt the plain text with key K1.
2) Decrypt the output of step 1 above with key K2
3) Finally encrypt the output of step 2 again with key K2.



3) What is Asymmetric key cryptography? How does it work

→ In Asymmetric cryptography each party has two keys - public key and private key.

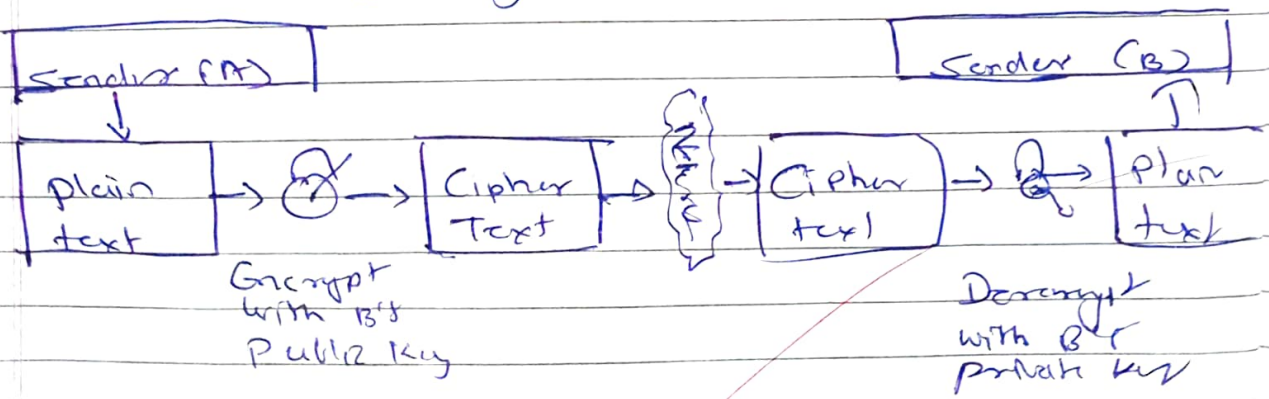
The public key is known to everybody; However the private key must be kept secret. If A is the sender of a message and B is the receiver, A encrypts the message using its own private key.

The Decryption can be done only and only by the private key which is confidential and known only to the receiver. Since, this process involves sending one key openly

it is also called as public key multiply key encryption. This solves the problem of multiple key pair when many parties are communicating. Also, key management is one more of issue.

Example - A bank has a public key and private key. The bank distributes its public key. However it keeps its own private secret key. So, whenever anyone wants to communicate with the bank they can encrypt the message using the bank's public key which can be further decrypted using the bank's private key only.

- Asymmetric key cryptography works as follows.



9(i) Write short note on steganography.

-> Steganography is the technique of Hiding data within an ord within an ordinary non secret file or message to avoid detection. The Hidden data is then extracted at its destination steganography use can be Combined with encryption as an extra step for Hiding or Protecting data.

When steganography is employed aloms it is security by obscurity which might result in the secret message being disclosed steganography can be used to conceal almost any type of digital Content including text image video or audio content.

Techniques

Clear text or plain text signifies the messages that can be understood by the sender, the decrypt and also by anyone else who gets acces to that message:

When a plaintext msg is codified using any suitable scheme, the resulting msg is called cipher text.

There are 2 primary ways to which a plain text msg can be codified to obtain the Corresponding cipher text.

1) Substitution technique
2) Transposition techniques

5) Explain the techniques of Cryptography

-> Clear text or plain text signifies the message that can be understood by the sender, the recipient and also by anyone else who gets access to that message.

When a plaintext msg is codified using any suitable scheme, the resulting msg is called cipher text.

There are 2 primary ways in which a plain text msg can be codified to obtain the corresponding cipher text:

1) Substitution technique
2) Transposition technique

-> Substitution technique

In character of plain text msg are replaced by other character, numbers or symbols

- Caesar cipher

The simplest form of substitution technique is the caesar cipher, where each letter in the plaintext is shifted a certain numbers of places down or up the alphabet.

Defined scheme 3

A	B	C	D	E	F	G	H	I	J
65	66	67	68	69	70	71	72	23	74
K	L	M	N	O	P	Q	R	S	T
75	76	77	78	79	80	81	82	83	84
U	V	W	X	Y	Z				
85	86	87	88	89	90				

* plain text : INDIA IS TAY CONTRY

Cipher text : LQGLD LY PB FRXQWUB

2) Transposition technique :-

Transposition technique is differ from substitution technique in the way that they do not replace one alphabet with another but they perform permutation over plain text.

- Railfence Technique :- It involves writing plain text as a sequence of diagonals and then reading it row to produce cipher text.

plain text : INDIA IS TAY COUNTRY

- Encryption in single row.