Day:- Monday

Date:- 21-09-2020

Assignment-1

INS UNIT-1

N.V.S.k.kalyani
174N1A0584
4-1 sem (C-sec)

Short Answers

1. Explain Modes of operations.

Ans There are 5 Modes of operations. Those are:

1) Electronic code Book (ECB):

This mode is a most straightforward way of processing a series of sequentially listed message blocks.

2) cipher Block chaining (CBC):-

CBC mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

3) cipher Feedback mode (CFB):

In this mode, each ciphertext block gets 'fed back' into the encryption process in order to encrypt the next plaintext block.

4) Output Feedback (OFB) Mode:

This mode makes a block cipher into Synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.

5) Counter mode:

This mode is a simple counter based block cipher implementation. Every time a counter initiated value is encrypted & given as input to XOR with plaintext which results in ciphertext block

Scanned by CamScanner

3. what is meant by stegnography.

Ans Stegnography is data hidden within data. It is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

4. what is Cryptography?

Ans cryptography systems are generally classified along 3 independent dimensions:

- Types of operations used for transforming plain text to cipher text.
- The number of keys used.
- The way in which the plain text is processed.

→ cryptography is a study of encryption principles / methods.

5. what is Symmetric key encryption technique?

Ans Symmetric encryption is a type of encryption where only one key (secret key) is used to both encryption and decrypt electronic information. The entities communicating via Symmetric encryption must exchange the key so that it can be used in the decryption process.

2. Discuss block cipher techniques?

Ans A Block cipher takes a fixed-length block of text of length b bits and a key as input and produces a b-bit block of ciphertext

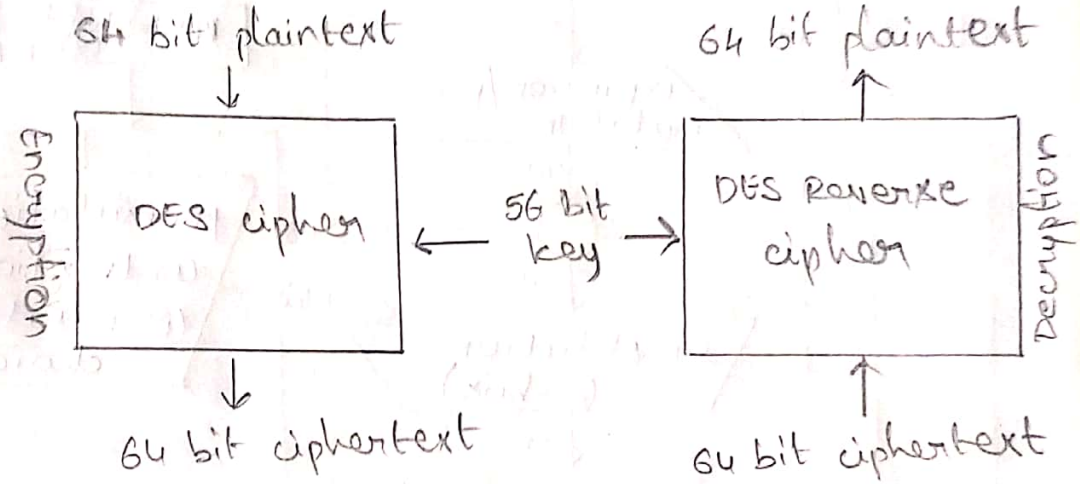
Scanned by CamScanner

Long Answers :-

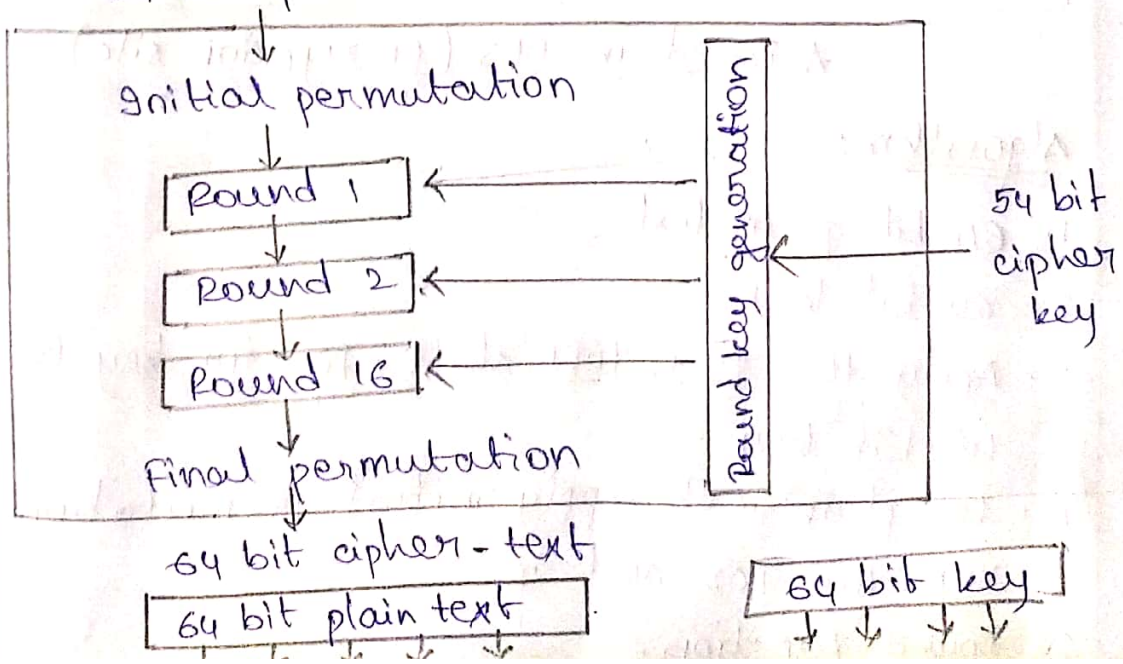
1. Explain concept of DES Algorithm access the strength and boawbacles ?

Ans The Data Encryption standard (DES) is a Symmetric key block either published by the National institution of standard & Technologies

→ DES is a Block cipher

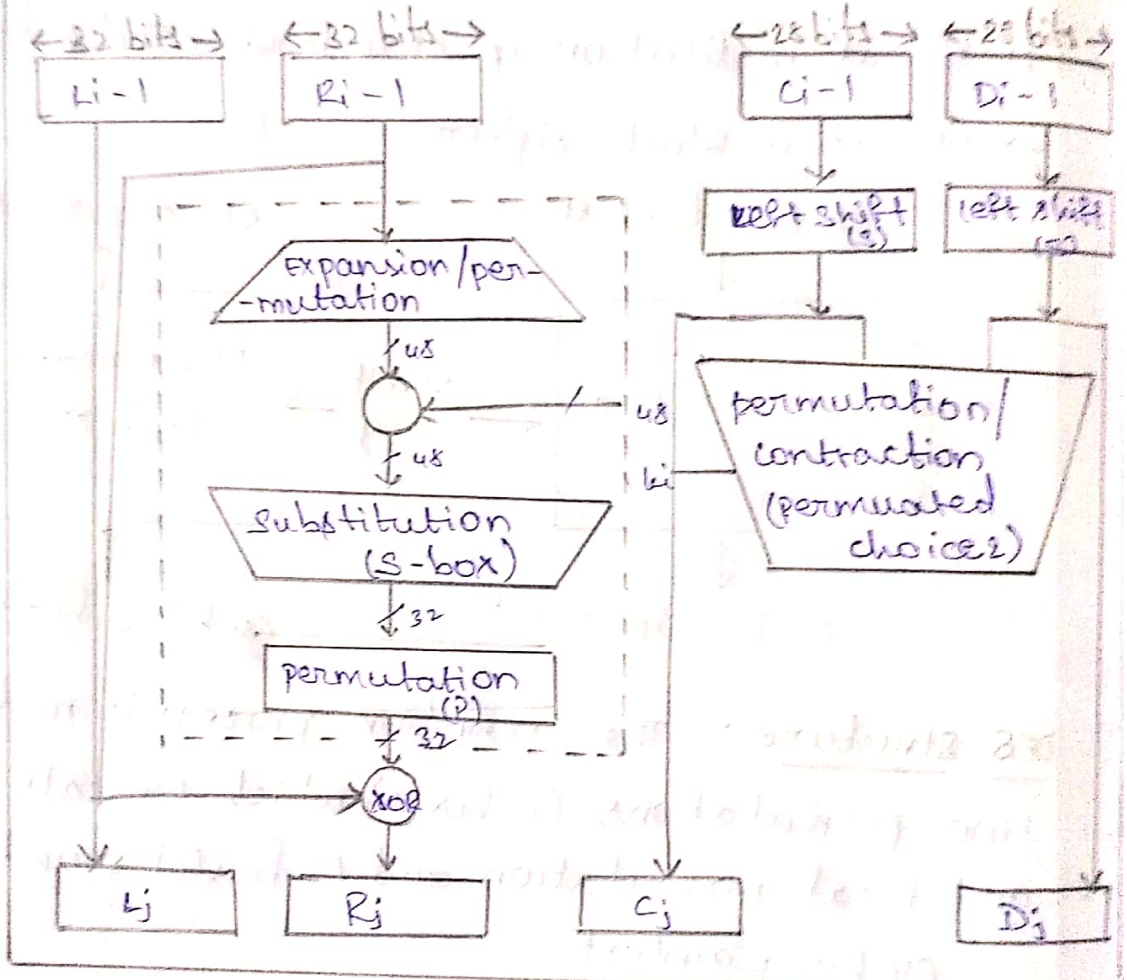


DES structure :- The Encryption process is made of two permutations (P-boxes) which we call initia and final permutation and 16 Feistel rounds



Scanned by CamScanner

* The initial & final permutation are straigh... P-boxes that are inverse of each other
* They have no cryptography significance in DES. Rounds: DES uses 16 rounds each round of DES is feistel cipher



A Round in DES (Encryption site)

Algorithm:-

1. 64 bit plain text
2. 64 bit key
3. Apply the PC1, left shift, PC_2 for key to obtain 48-bit key
4. For plain text apply initial permutation
5. XOR the PC2 and ip
6. Round Function.

Scanned by CamScanner

Eg: IP: 8 5 4 6 7 3 2 1

FP: 1 4 3 2

key: 1010000010

PC1: 9 8 7 5 3 2 1 4

PC2: 7 4 3 1 5 6 8

	0	1	2	3
0	1	2	3	0
1	0	1	2	3
2	1	0	2	3
3	3	2	1	0

permutation after expansion box

4 3 2 1

1. plaintext: 0 1 1 1 0 0 1 0
   1 2 3 4 5 6 7 8

2. key: 1 0 1 0 0 0 0 0 1 0
   1 2 3 4 5 6 7 8 9 10

3. PC1: 9 8 7 5 3 2 1 4 ⇒ 9 8 7 5 / 3 2 1 4
   left shift 0 0 0 1 0 1 0 1 → 1 0 0 0 / 1 0 1 0
   1 2 3 4 5 6 7 8

   PC2: 7 4 2 3 1 5 6 8
   0 1 0 0 0 0 1 1 → key 2
   1 2 3 4 5 6 7 8

4. IP: 8 5 4 6 7 3 2 1
   0 0 1 0 1 1 1 0

5. XOR: for PC2 & IP
   1001 0010

6. Round function:

   Expansion base: 1001 / 0010

   S-Box

	0	1	2	3
0	1	2	3	0
1	0	1	2	3
2	1	0	2	3
3	3	2	1	0

Scanned by CamScanner

Strengths:-

1. The use of 56-bits key
2. The nature of algorithm.

Drawbacks:- has been found in the design of the cipher

a) Two choosen i/p to an s-box can create same o/p.
b) The purpose of initial & final permutatio is not clear.

Scanned by CamScanner

17UNIA0584

2. Discuss briefly about stream cipher algorithm

Ans It is used in data communication & Networ protocols. It generates a key stream consequ of bit used as a keys.

Encryption is a accomplished by combining the key stream with the plain text usually wit bandwith operation.

```
  11001100   plain text
  01101100   key stream
 ----------
  10100000   ciphertext
```

RCA consists of 2 parts

→ key scheduling Algorithm

→ Pseudo Random generation Algorithm (PRGA)

* Because the only operation on S is a swap The only effect is a permutation S till contai all the numbers from 0 through 256.

Pseudo: Random Generation Algorithm:-

* once S is initilized, the input key is no longer used

```
i, j = 0;
plen = length [Plain text]
while (P1 > 0)
{  i = (i+1) mod 256;
   j = (j + s[i] mod 256;
   swap (s[i], s[j])
   k = s[(s[i], s[j] mod 256];
   output k;
   plen = plen - 1;
}  end while
```

Scanned by CamScanner

3. Breifly explain AES Algorithm.

- AES is a block cipher with a block length of 128 bits.
- AES allows for 3 different key lengths: 128, 192, (or) 256 bits. most of our discussion will assume that the key length is 128 bits.
- Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.
- Except for the last round in each case, all other rounds are identical.
- Each round of processing includes one single byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.
- To appreciate the processing steps used in a single round, it is best to think of a 128-bit block as consisting of a 4x4 matrix of bytes arranged as follows:

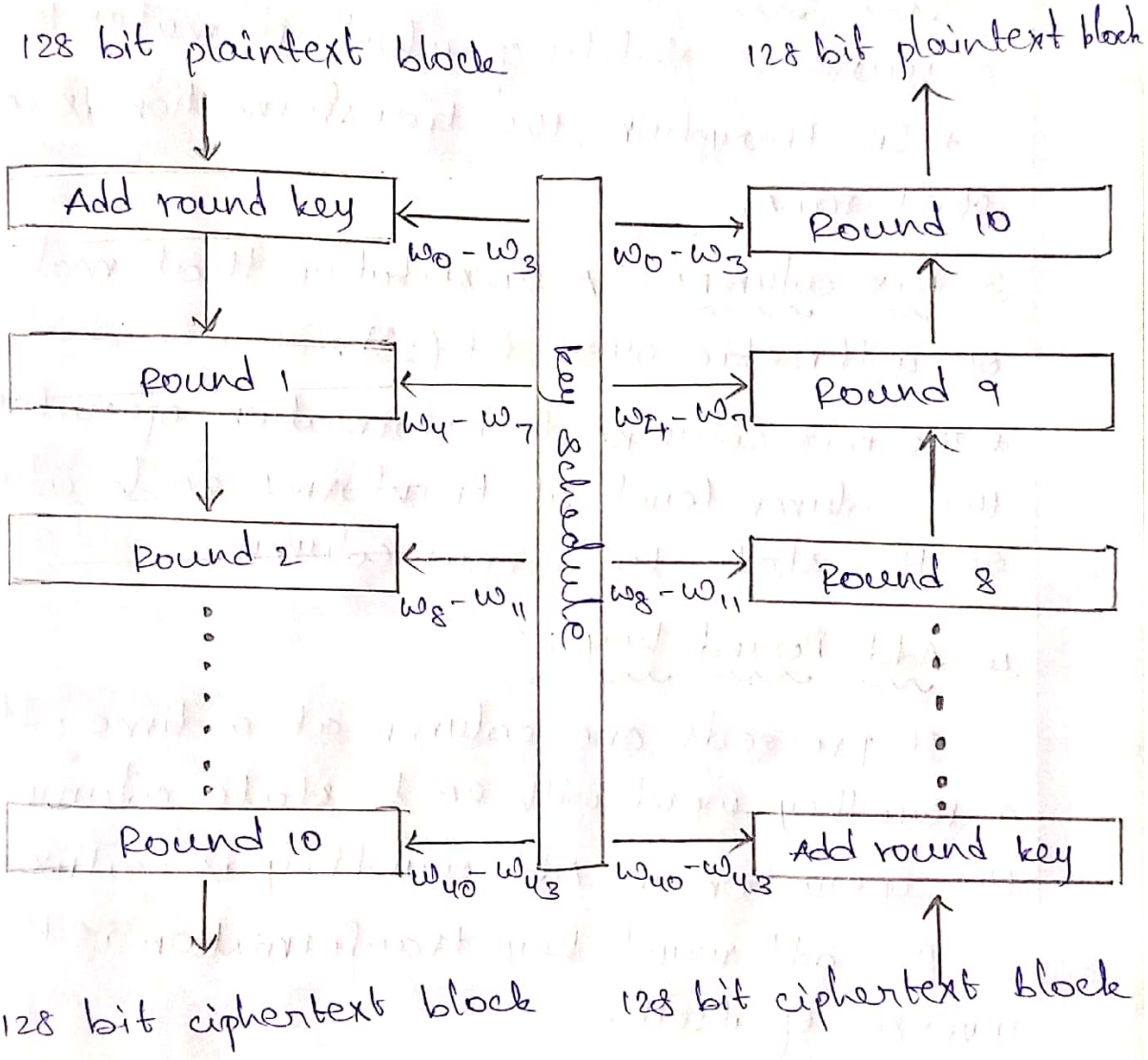
$$\begin{bmatrix} byte_0 & byte_4 & byte_8 & byte_{12} \\ byte_1 & byte_5 & byte_9 & byte_{13} \\ byte_2 & byte_6 & byte_{10} & byte_{14} \\ byte_3 & byte_7 & byte_{11} & byte_{15} \end{bmatrix}$$

Therefore, the first four bytes of a 128-bit input block occupy the first column in the 4x4 matrix

Scanned by CamScanner

of bytes. The next four bytes occupy the 2nd column, and so on.

The 4x4 matrix of bytes shown above is referred to as the state array in AES.



AES Encryption AES Decryption

→ The algorithm begins with an Add round key stage followed by 9 rounds of 4 stages and a 10th round of 3 stages.

• This applies for both encryption & decryption with the exception that each stage of round the decryption algorithm is the inverse of its counterpart in the encryption algorithm.

Scanned by CamScanner

• The 4 stages are as follows:

1, Substitute byte :- use an S-box to perform a byte-to-byte substitution of the block.

2, Shift rows :- Another transformation found in a round is shifting which permutes the byte

* In Encryption, the transformation is called shift rows.

3, Mix columns :- A substitution that makes us of arithmetic over GF(2^8).

* The mix columns transformation operates at the column level, it tranforms each columns of the state to a new column.

4, Add Round key :-

It proceeds one column at a time. It add a roundkey word with each state column matr the operation in Add roundkey is matrix additi

Scanned by CamScanner