UNIT-II

Syllabus: Symmetric cipher model, Block and Stream ciphers, Data Encryption Standard (DES), Strength of DES, Block cipher design principles and modes of operation, Triple DES, AES Structure

2.1 Symmetric cipher model

- Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.
- It is also known as conventional encryption.
- Symmetric encryption transforms plaintext into cipher text using a secret key and an encryption algorithm.
- Using the same key and a decryption algorithm, the plaintext is recovered from the cipher text.
- A symmetric encryption scheme has five ingredients

i. Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
ii. Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
iii. Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm.
iv.Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
v.Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

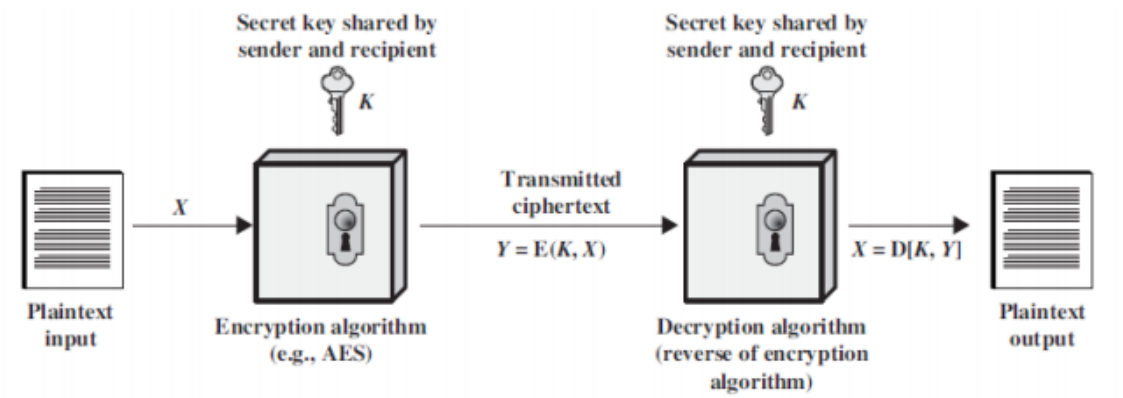
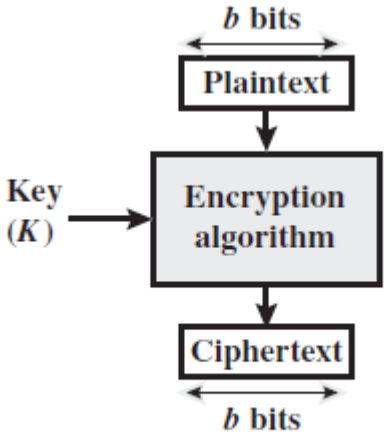


Fig: Simplified Model of Symmetric Encryption

2.2 BLOCK AND STREAM CIPHERS

2.2.1 Block Cipher

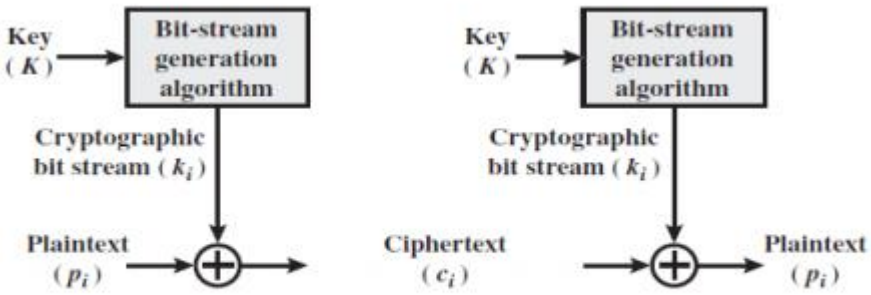
- A block cipher is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Many block ciphers have a Feistel structure.



Block cipher

2.2.2 Stream cipher

- Stream cipher is one that encrypts a digital data stream one bit or one byte at a time.
- Examples of classical stream ciphers are the auto keyed Vigenère cipher and the Vernam cipher.
- If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream.
- The keystream must be provided to both users in advance via some in¬dependent and secure channel
- The bit-stream generator must be implemented as an algorithmic procedure, so that the cryptographic bit stream can be produced by both users.



Stream cipher using algorithmic bit-stream generator

2.2.3 Feistel Cipher

Feistel proposed the use of a cipher that alternates substitutions and permutations, where these terms are defined as follows:

Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

2.2.3.1 Feistel Cipher Structure

- Figure depicts the structure proposed by Feistel. The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K.
- The plaintext block is divided into two halves, L0 and R0.
- The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block. Each round i has as inputs Li-1 and Ri-1, derived from the previous round, as well as a subkey Ki,derived from the overall K.
- All rounds have the same structure. 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 exclusive-OR of the output of that function and the left half of the data. The round function has the same general structure for each round but is parameterized by the round subkey Ki.
- A Feistel network depends on the choice of the following parameters and design features:

i. Block size: Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed for a given algorithm. The greater security is achieved by greater diffusion Traditionally, a block size of 64 bits has been considered a reasonable tradeoff and was nearly universal in block cipher design. However, the new AES uses a 128-bit block size.

ii. Key size: Larger key size means greater security but may decrease encryption/decryption speed. The greater security is achieved by greater resistance to brute-force attacks and greater confusion. Key sizes of 64 bits or less are now widely considered to be inadequate, and 128 bits has become a common size.

iii. Number of rounds: The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.

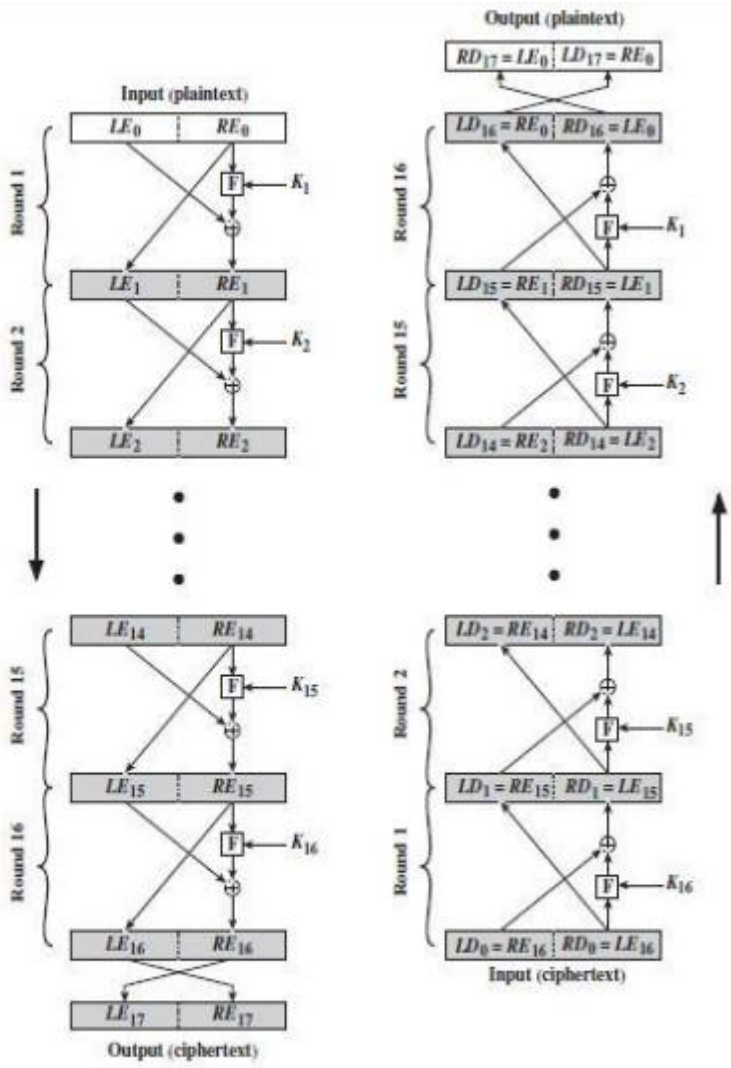
iv. Subkey generation algorithm: Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

v. Round function: Again, greater complexity generally means greater resistance to cryptanalysis.

There are two other considerations in the design of a Feistel cipher

i. Fast software encryption/decryption: In many cases, encryption is embedded in applications or utility functions in such a way as to preclude a hardware implementation. The speed of execution of the algorithm becomes a concern.

ii. Ease of analysis: Although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze.



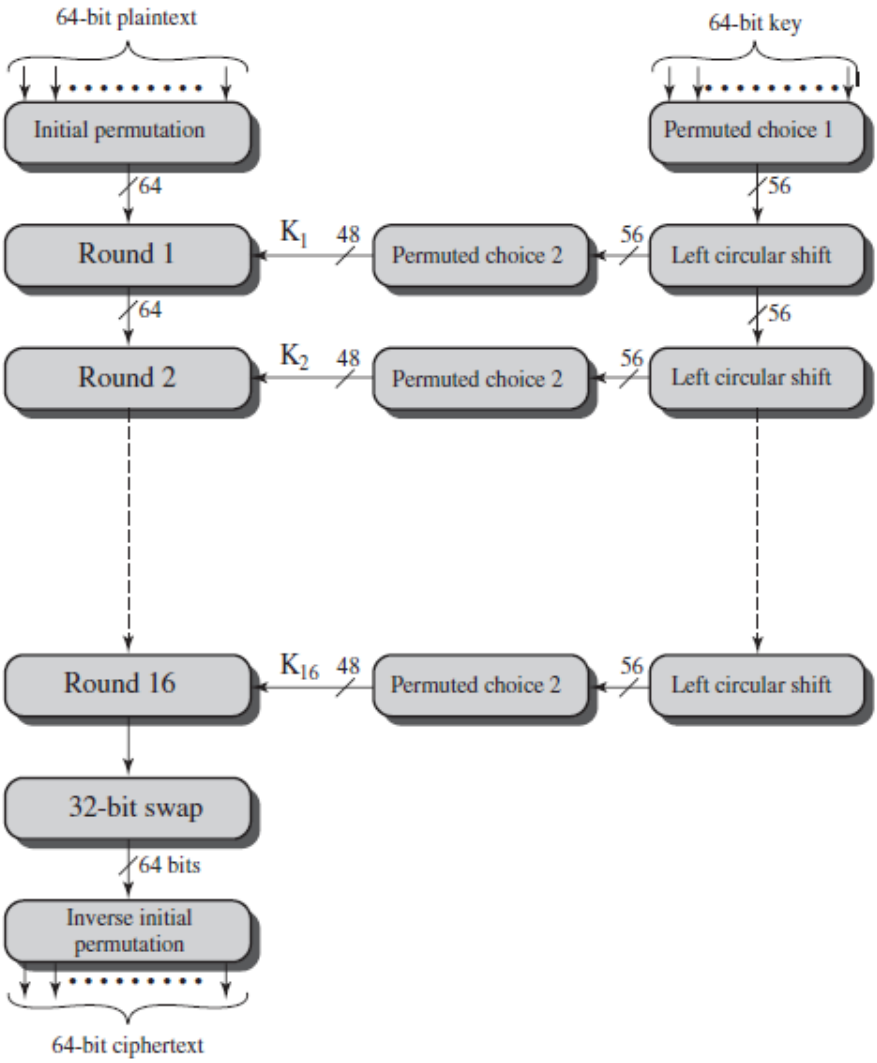
Feistel Encryption and Decryption(16 rounds)

2.3 DATA ENCRYPTION STANDARD (DES)

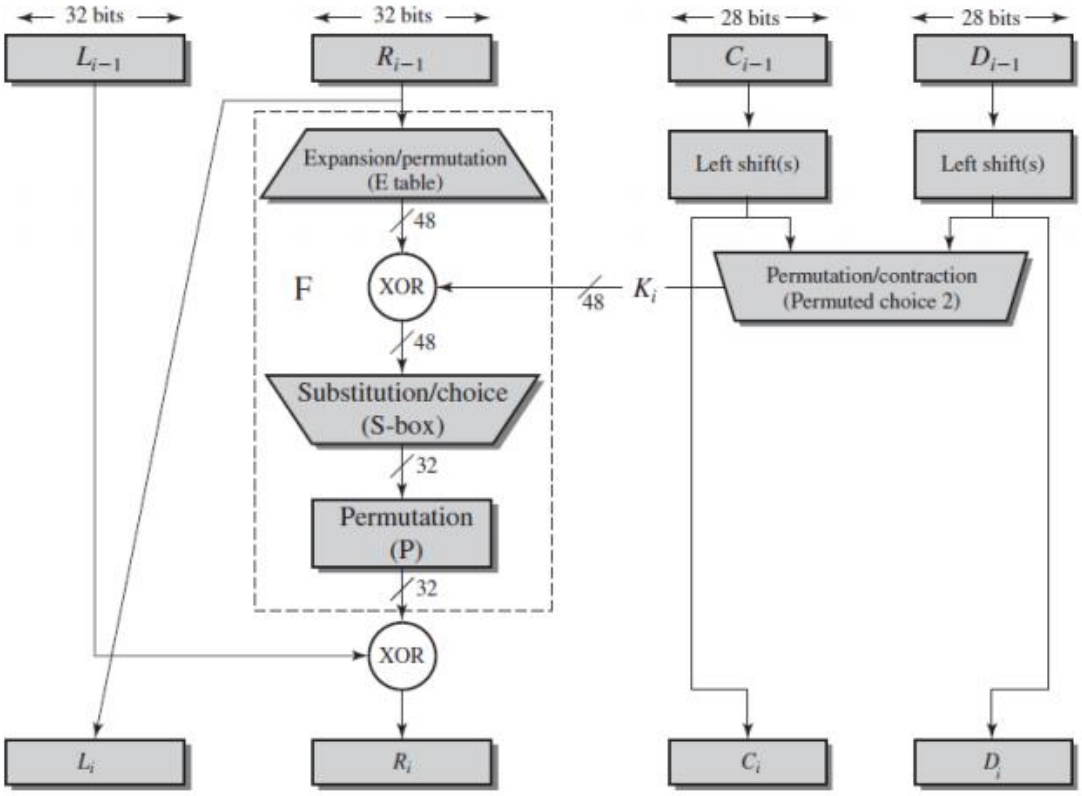
- The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards.
- The algorithm is referred to as the Data Encryption Algorithm (DEA).
- Data are encrypted in 64-bit blocks using a 56-bit key.
- The algorithm transforms 64-bit input in a series of steps into a 64-bit output.
- The same steps, with the same key, are used to reverse the encryption

2.3.1 DES Encryption:

- the plaintext must be 64 bits in length
- the key is 56 bits in length



- Left-hand side of the figure has plaintext proceeded in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. It is followed by a phase consisting of sixteen rounds of the same function. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the pre output.
- Right-hand portion of Figure shows the way in which the 56-bit key is used.Finally, the pre output is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext
- Initially, the key is passed through a permutation function.
- Then, for each of the sixteen rounds, a subkey (Ki) is produced by the combination of a left circular shift and a permutation.
- The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.



2.3.1.1Single Round

- The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right).
- the overall processing at each round can be summarized as:

$$L_i = R_{i-1}$$

$$Ri = L_{i-1} \oplus F(Ri-1, K_i)$$

- The round key K_i is 48 bits. The R input is 32 bits.
- This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits.
- The resulting 48 bits are XORed with K_i.
- This 48-bit result passes through a substitution function that produces a 32- bit output, which is permuted.
- The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.
- These transformations are defined as the first and last bits Si of the input to box form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for S_i.
- The middle four bits select one of the sixteen columns
- The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output.
- The 32-bit output from the eight S-boxes is then permuted, so that on the next round, the output from each S-box immediately affects as many others as possible.

<u>2.3.2 DES Decryption</u>

Decryption uses the same algorithm as encryption, except that the application of the sub-keys is reversed.

2.3.3 The Avalanche Effect

- A small change in either the plaintext or the key should produce a significant change in the cipher text.
- A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text. This is referred to as the avalanche effect.

2.4 STRENGTH OF DES

The level of security provided by DES by the following:

i. The Use of 56-Bit Keys

- With a key length of 56 bits, there are 256 possible keys, which is approximately 7.2*1016 keys.
- A brute-force attack is impractical on DES.
- Half the key space has to be searched, a single machine performing one DES encryption per microsecond would take more than a thousand years to break the cipher.

ii. The Nature of the DES Algorithm

- The focus of concern has been on the eight substitution tables, or S boxes, that are used in each iteration.
- A number of regularities and unexpected behaviors of the S-boxes have been discovered.

iii.Timing Attacks

- A timing attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.
- DES appears to be fairly resistant to a successful timing attack.

2.5 BLOCK CIPHER DESIGN PRINCIPLES

The three critical aspects of block cipher design:

- The number of rounds,
- Design of the function F,
- Key scheduling.

2.5.1The number of rounds

- The greater the number of rounds, the more difficult it is to perform cryptanalysis, even for a relatively weak F.
- In general, the criterion should be that the number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack.

2.5.2 Design of the function F

- Design criteria for F
  - The heart of a DES is the function F which relies on the use of S-boxes.
  - The function F provides the element of confusion.
  - Thus, it must be difficult to “unscramble” the substitution performed by F.

        - The criterion is that F must be nonlinear. The more nonlinear F, the more difficult any type of cryptanalysis will be.
    - S-Box Design
        - A change to the input vector to an S-box should result in random-looking changes to the output.
        - The relationship should be nonlinear and difficult to approximate with linear functions
        - Random: Use some pseudorandom number generation or some table of random digits to generate the entries in the S-boxes.
        - Random with testing: Choose S-box entries randomly, then test the results against various criteria, and throw away those that do not pass.
        - Human-made: This is a more or less manual approach with only simple mathematics to support it.
        - Math-made: Generate S-boxes according to mathematical principles. By using mathematical construction, S-boxes can be constructed that offer proven security against linear and differential cryptanalysis, together with good diffusion

2.5.3 Key scheduling.

- The key is used to generate one subkey for each round.
- In general, we would like to select subkeys to maximize the difficulty of deducing individual subkeys and the difficulty of working back to the main key.
- The key schedule should guarantee key/ciphertext Strict Avalanche Criterion and Bit Independence Criterion

DES Design Criteria: focus is on the design of the S-boxes and on the P function that takes the output of the S-boxes.

- The criteria for the S-boxes are as follows
    1. No output bit of any S-box should be too close a linear function of the input bits.
    2. Each row of an S-box should include all 16 possible output bit combinations.
    3. If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits
    4. If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ in at least two bits.
    5. If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must not be the same.
    6. For any nonzero 6-bit difference between inputs, no more than eight of the 32 pairs of inputs exhibiting that difference may result in the same output difference.
    7. This is a criterion similar to the previous one, but for the case of three S-boxes.
- The criteria for the permutation P are as follows.
    1. The four output bits from each S-box at round are distributed so that two of them affect “middle bits” of round (i + 1) and the other two affect end bits.
    2. The four output bits from each S-box affect six different S-boxes on the next round, and no two affect the same S-box.

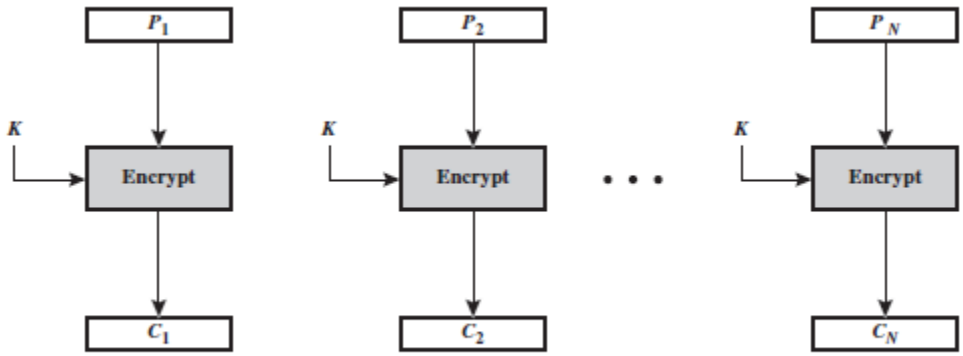
3. For two S-boxes j, k, if an output bit from S_j affects a middle bit of S_k on the next round, then an output bit from S_k cannot affect a middle bit of S_j. This implies that, for j=k, an output bit from S_j must not affect a middle bit of S_j.

2.6 Modes of operation

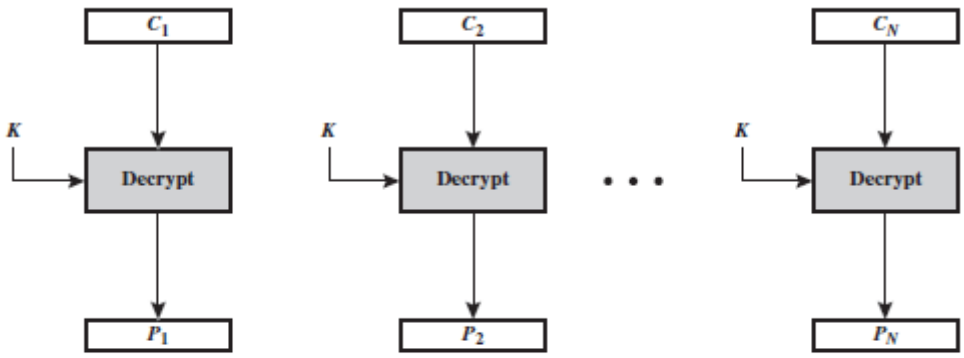
- A block cipher takes a fixed-length block of text of length bits and a key as input and produces a -bit block of ciphertext.
- If the amount of plaintext to be encrypted is greater than b bits, then the block cipher can still be used by breaking the plaintext up into -bit blocks
- To apply a block cipher in a variety of applications, five modes of operation have been defined by NIST
- In essence, a mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream.
- The Block Cipher modes of operations are:
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

2.6.1 Electronic Codebook (ECB)

- Plaintext is handled one block at a time and each block of plaintext is encrypted using the same key.
- The term codebook is used because, for a given key, there is a unique ciphertext for every -bit block of plaintext.
- Message is broken into independent blocks of b-bit size which are encrypted
- Decryption is performed one block at a time, always using the same key.



(a) Encryption

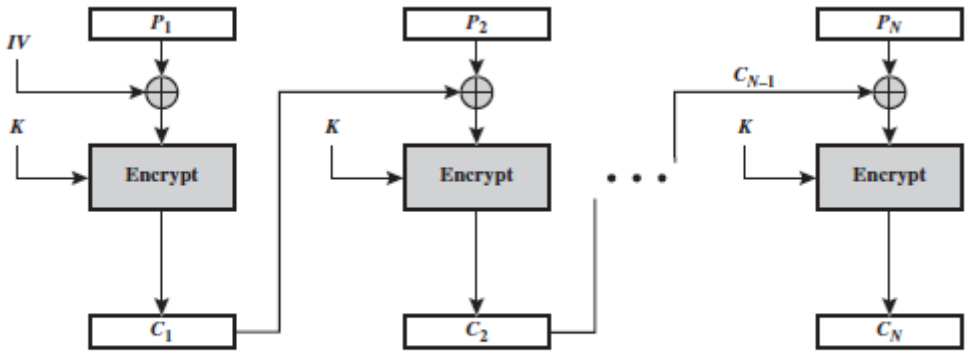


(b) Decryption

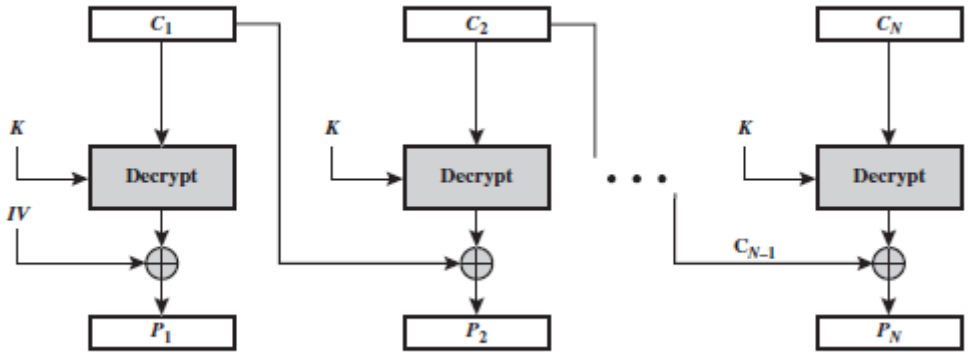
- The plaintext consists of a sequence of b-bit blocks, P_1, P_2…. P_N.
- The corresponding sequence of ciphertext blocks is C_1, C_2 ….. C_N
- ECB mode is defined as:
  - $Cj = E(K, Pj)$ $j = 1, …., N$ (Encryption)
  - $Pj = D(K, Cj)$ $j = 1, ….. , N$ (Decryption)
- The ECB method is ideal for a short amount of data, such as an encryption key
- For lengthy messages, the ECB mode may not be secure
- weakness due to encrypted message blocks being independent

2.6.2 Cipher Block Chaining (CBC)

- the input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block.
- the same key is used for each block
- To produce the first block of ciphertext, an initialization vector (IV) is XORed with the first block of plaintext



(a) Encryption



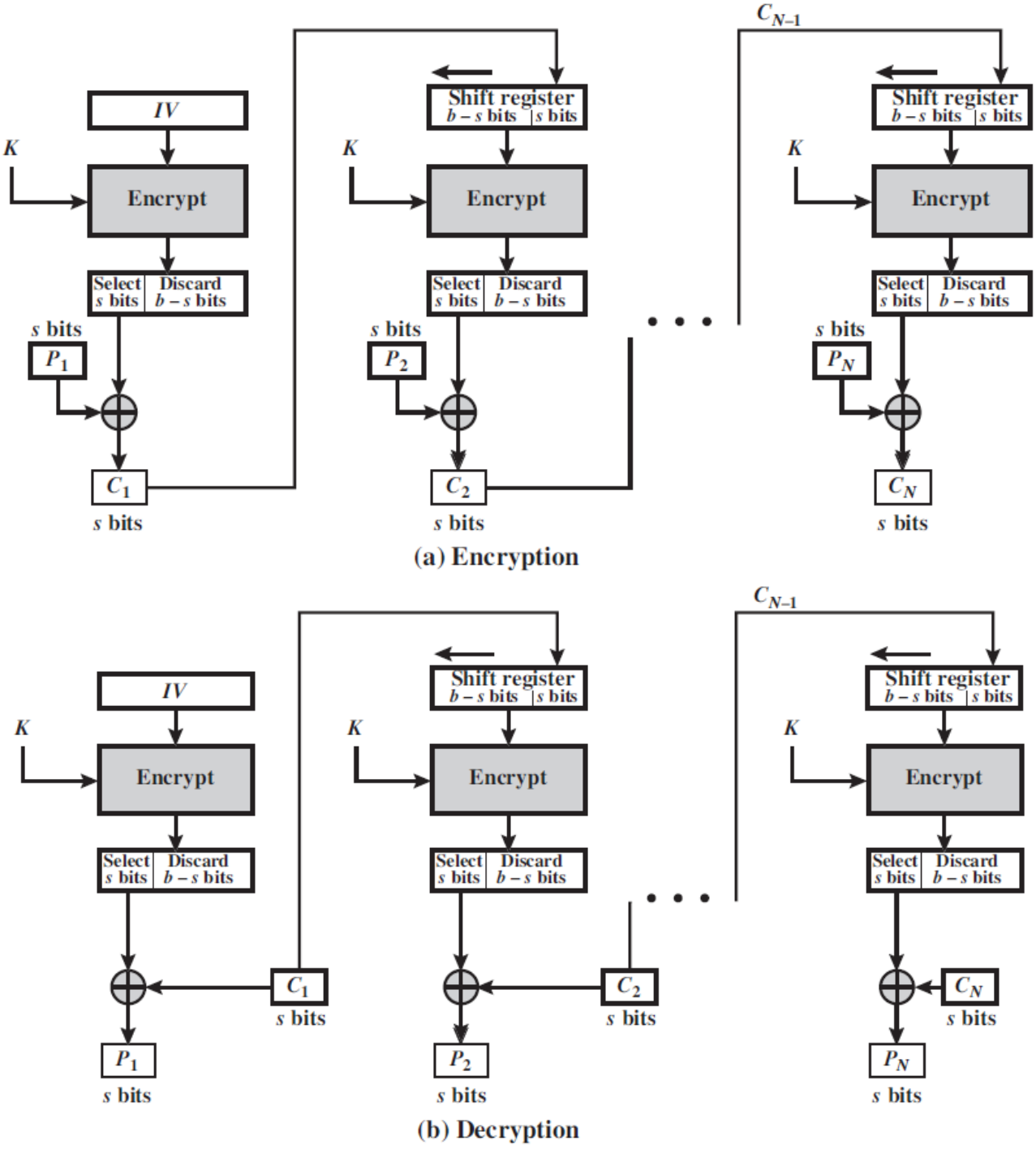
(b) Decryption

- On decryption, the IV is XORed with the output of the decryption algorithm to recover the first block of plaintext.
- The IV is a data block that is that same size as the cipher block.
- The IV must be known to both the sender and receiver but be unpredictable by a third party.
- We can define CBC mode as
  - Encryption
    - $C_1 = E(K, [P_1 \oplus IV])$
    - $C_j = E(K, [P_j \oplus C_{j-1}])$ $j = 2, \ldots N$
  - Decryption
    - $P_1 = D(K, C_1) \oplus IV$
    - $P_j = D(K, C_j) \oplus C_{j-1}$ $j = 2, \ldots N$
- each ciphertext block depends on all message blocks thus a change in the message affects all ciphertext blocks after the change as well as the original block

2.6.3 Cipher Feedback (CFB)

- the plaintext is divided into segments of s bits
- The input to the encryption function is a b-bit shift register that is initially set to some initialization vector (IV).

- The leftmost s bits of the output of the encryption function are XORed with the first segment of plaintext P_1 to produce the first unit of ciphertext C_1.
- The contents of the shift register are shifted left by s bits, and C_1 is placed in the rightmost s bits of the shift register
- Process continues until all plaintext units have been encrypted.
- Encryption $C_1 = P_1 \oplus MSBs[E(K, IV)]$
- Decryption, the same scheme is used, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext.
- Decryption $P_1 = C_1 \oplus MSBs[E(K, IV)]$

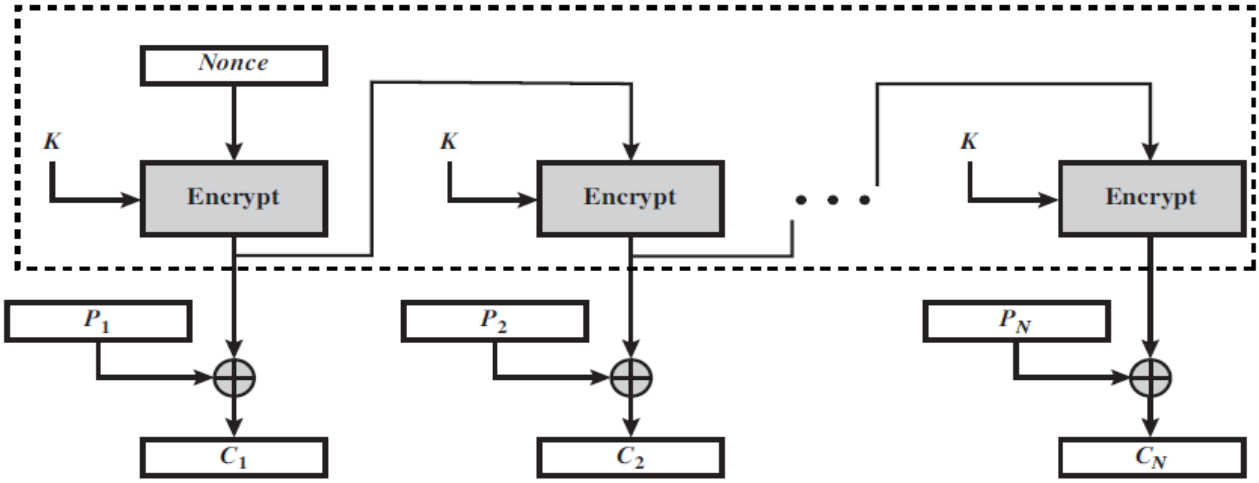


- This is most common stream mode

- The disadvantage is errors propagate for several blocks after the error occurred.

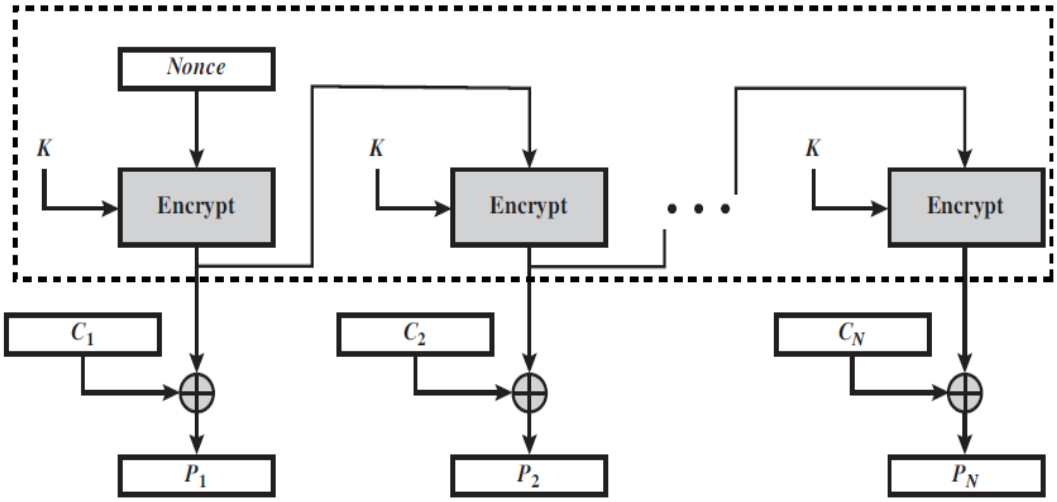
2.6.4 Output Feedback (OFB)

- The output of the encryption function that is fed back to the shift register in OFB.
- message is treated as a stream of bits
- OFB mode operates on full blocks of plaintext and ciphertext



(a) Encryption

- Encryption can be expressed as $C_j = P_j \oplus E(K, [C_{j-I} \oplus P_{j-1}])$



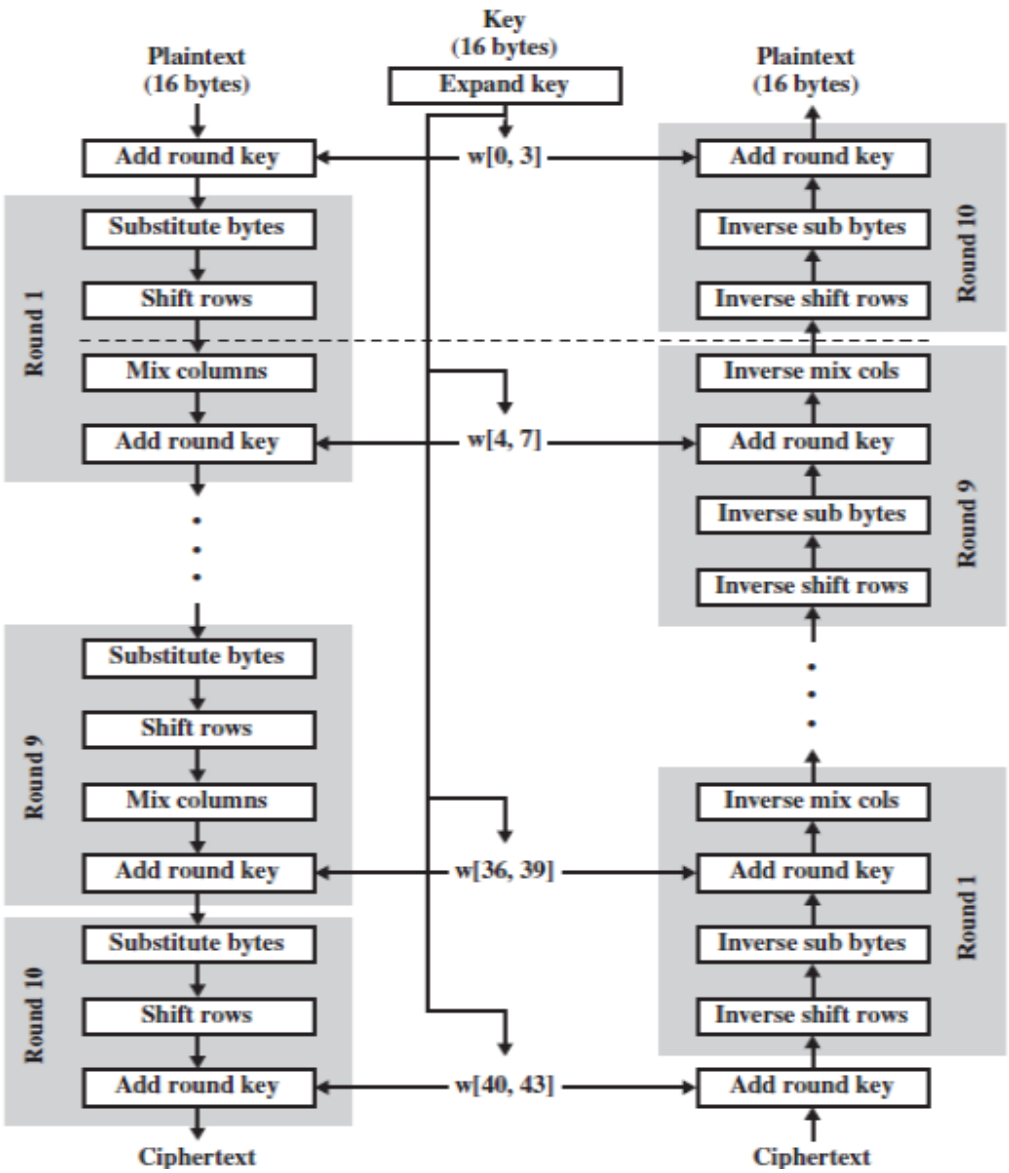
(b) Decryption

- Decryption can be expressed as $P_j = C_j \oplus E(K, [C_{j-1} \oplus P_{j-1}])$

2.7 ADVANCED ENCRYPTION STANDARD (AES)

- Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST).
- AES is a block cipher intended to replace DES for commercial applications.
- It uses a 128-bit block size and a key size of 128, 192, or 256 bits.
- AES does not use a Feistel structure.
- plaintext block is of size 128 bits, or 16 bytes
- The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits)

- The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length.
- The cipher consists of N rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key.
- The first rounds consist of four distinct transformation functions:SubBytes, ShiftRows, MixColumns, and AddRoundKey.
- The final round contains only three transformations, and there is a initial single transformation (AddRoundKey) before the first round, which can be considered Round 0.
  - **Substitute Bytes:** Uses an S-box to perform a byte-by-byte substitution of the block
  - **Shift Rows:** A simple permutation
  - **Mix Columns:** A substitution that makes use of arithmetic over GF(2^8)
  - **Add Round Key:** A simple bitwise XOR of the current block with a portion of the expanded key



- AES defines a 16 X 16 matrix of byte values, called an S-box.
- It contains a permutation of all possible 256 8-bit values

- Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value.
- These row and column values serve as indexes into the S-box to select a unique 8-bit output value.

AES Decryption

AES decryption is not identical to encryption since steps done in reverse o but can define an equivalent inverse cipher with steps as for encryption but using inverses of each step with a different key schedule works since result is unchanged when swap byte substitution & shift rows swap mix column & add (tweaked) round key

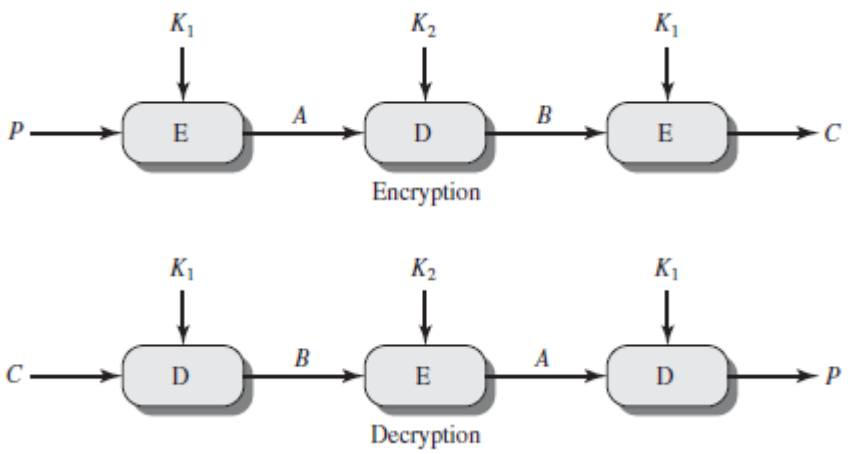
2.8 TRIPLE DES (3DES)

Triple DES makes use of three stages of the DES algorithm, using a total of two or three distinct keys:

- Triple DES with Two Keys
- Triple DES with Three Keys

➢ Triple DES with Two Keys

- A triple encryption method that uses only two keys
- The function follows an encrypt-decrypt-encrypt (EDE) sequence as below



- Encryption is : $C = E(K_1, D(K_2, E(K_1, P)))$
- Decryption is : $P = D(K_1, E(K_2, D(K_1, C)))$
- There is no cryptographic significance to the use of decryption for the second stage.
- Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES

- 3DES with two keys is a relatively popular alternative to DES and has been adopted for use in the key management standards.

- Triple DES with Three Keys
  - Three-key 3DES has an effective key length of 168 bits and is defined as : $C = E(K_3, D(K_2, E(K_1, P)))$
  - Backward compatibility with DES is provided by putting $K_3 = K_2$ or $K_1 = K_2$
  - A number of Internet-based applications have adopted three-key 3DES, including PGP and S/MIME.

ASSIGNMENT-CUM-TUTORIAL QUESTIONS

A. Objective Questions

1. In cryptography, what is cipher? [ ]
a. algorithm for performing encryption and decryption
b. encrypted message
c. both algorithm for performing encryption and decryption and encrypted message
d. decrypted message

2. Which is the principle of the encryption using a key? [ ]
a. The key indicates which function is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
b. The key contains the secret function for encryption including parameters. Only a password can activate the key.
c. All functions are public, only the key is secret. It contains the parameters used for the encryption respectively decryption.
d. The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.

3. Which is the largest disadvantage of the symmetric Encryption? [ ]
a. More complex and therefore more time-consuming calculations.
b. Problem of the secure transmission of the Secret Key.
c. Less secure encryption function
d. Isn't used any more.

4. In cryptography, the order of the letters in a message is rearranged by [ ]
a. transpositional ciphers
b. substitution ciphers
c. both transpositional ciphers and substitution ciphers
d. quadratic ciphers

5. Chosen cipher text attack is based on [ ]
a. Cryptanalysis
b. Cryptography
c. Encryption
d. Decryption

6. Transposition cipher involves: [ ]
a. Replacement of blocks of text with other blocks
b. Replacement of characters of text with other character
c. Strict row to column replacement
d. Some permutation on the input text to produce cipher text

7. Encryption strength is based on: [ ]
a. Strength of algorithm
b. Secrecy of key
c. Length of key
d. **All of the above**

8. Some of the parameters of Feistel cipher are [ ]
(i) Number of rounds
(ii) Block size
(iii) S-Box
(iv) Key size
(v) Sub key Generation algorithm
(vi) Function key

a. all of the above
b. only (i) (ii) (iii) (iv)
c. only (i),(ii),(iv),(v),(vi)
d. only (i),(ii),(iii),(iv),(vi)

9. The input block length in DES is: [ ]
a. 56 bits b. 64 bits c. 112 bits d. 128 bits

10. The sub key length at each round of DES is_____ [ ]
a. 32
b. 56
c. 48
d. 64

11. Identify false statement regarding characteristics of DES [ ]

a. Each bit of the cipher text depends on all bits of the key
b. There is a statistical relationship between plaintext and cipher text
c. Avalanche effect
d. Altering a cipher text bits results in an unpredictable change

12. TDES means: [ ]
a. Triple digital encryption standard
b. Triangular data encryption standard
c. Triple data encryption standard
d. Triangular digital encryption standard

13. Which of the following is not a block cipher operating mode? [ ]
a. ECB b. CBF c. CBC d. OFB

14. In_____ mode, the same plaintext value will always result in the same cipher text value. [ ]
a. Cipher Block Chaining
b. Cipher Feedback
c. Electronic code book
d. Output Feedback

15. Disadvantages of CFB is_____ [ ]

a. if data to be operated on bit or byte oriented level then only stream mode is useful
b. single error leads to errors in several blocks after the error
c. each round must wait until XOR operation finishes its scheme
d. all of the above

16. Identify which of the following is disadvantage of CBC [ ]

a. protection on order of blocks means integrity can be maintained
b. synchronization maintained automatically
c. using initial vector to randomize cipher text
d. serial encryption

17. AES uses a _____ bit block size and a key size of _____ bits. [ ]

a. 128; 128 or 256
b. 64; 128 or 192
c. 256; 128, 192, or 256
d. 128; 128, 192, or 256

18. How many rounds does the AES-192 perform? [ ]

a. 10
b. 12
c. 14
d.16

19. The 4×4 byte matrices in the AES algorithm are called [ ]

a. States
b. Words
c. Transitions
d. Permutations

20. Which of the 4 operations are false for each round in the AES algorithm
i) Substitute Bytes
ii) Shift Columns
iii) Mix Rows
iv) XOR Round Key [ ]

a. i) only
b. **ii) iii) and iv)**
c. ii) and iii)
d. only iv)

B. Descriptive Questions

1. List and explain the essential ingredients of a symmetric cipher.
2. Explain the Fiestel cipher structure with a neat sketch. And also give its significance.
3. Illustrate the single round operation of DES algorithm in detail.
4. Justify the statement that the strength of DES algorithm depends on key and nonlinear S-box design.
5. Inspect various cipher modes of operation in detail.
6. Analyze encryption and decryption process in TDES.
7. Illustrate the encryption and decryption process of AES.
8. Infer the block cipher design principles.
9. List and explain the strengths of DES.