Unit – III

Objectives:

- To introduce the symmetric cipher model
- To know different encryption algorithms and modes of operations.

Syllabus: Basics of Cryptography

Symmetric cipher model, Block and Stream Ciphers, Data Encryption Standard (DES), Strength of DES, Block Cipher Design Principles and Modes of operation.

Outcomes:

Students will be able to

- know symmetric encryption technique
- distinguish block and stream ciphers
- implement symmetric encryption algorithms

Basics of Cryptography

3.1 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
  - Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
  - Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
  - 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.
  - 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.
  - • Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

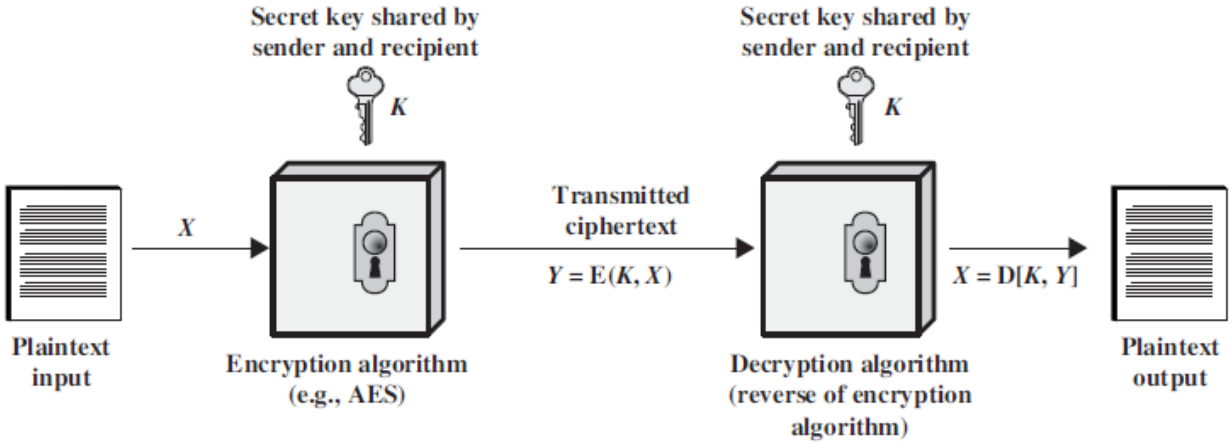
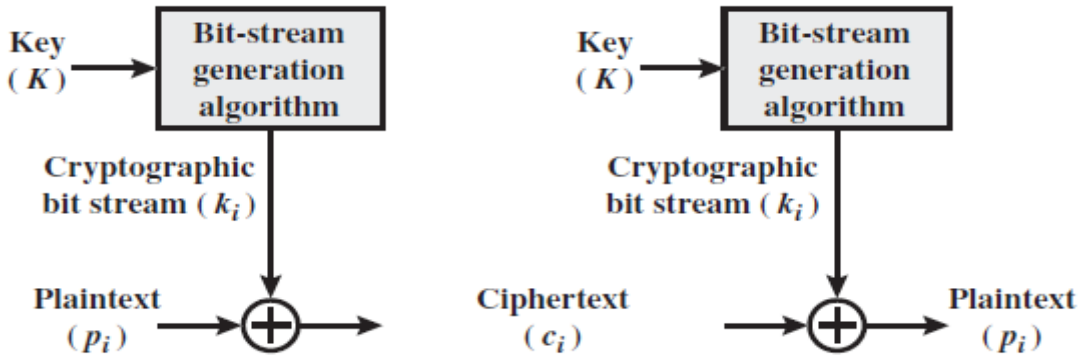


Fig: Simplified Model of Symmetric Encryption

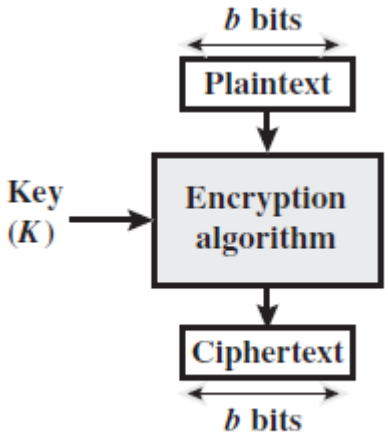
3.2 Block and Stream Ciphers

- **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 autokeyed 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.
- However, the keystream must be provided to both users in advance via some independent 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.



(a) Stream cipher using algorithmic bit-stream generator

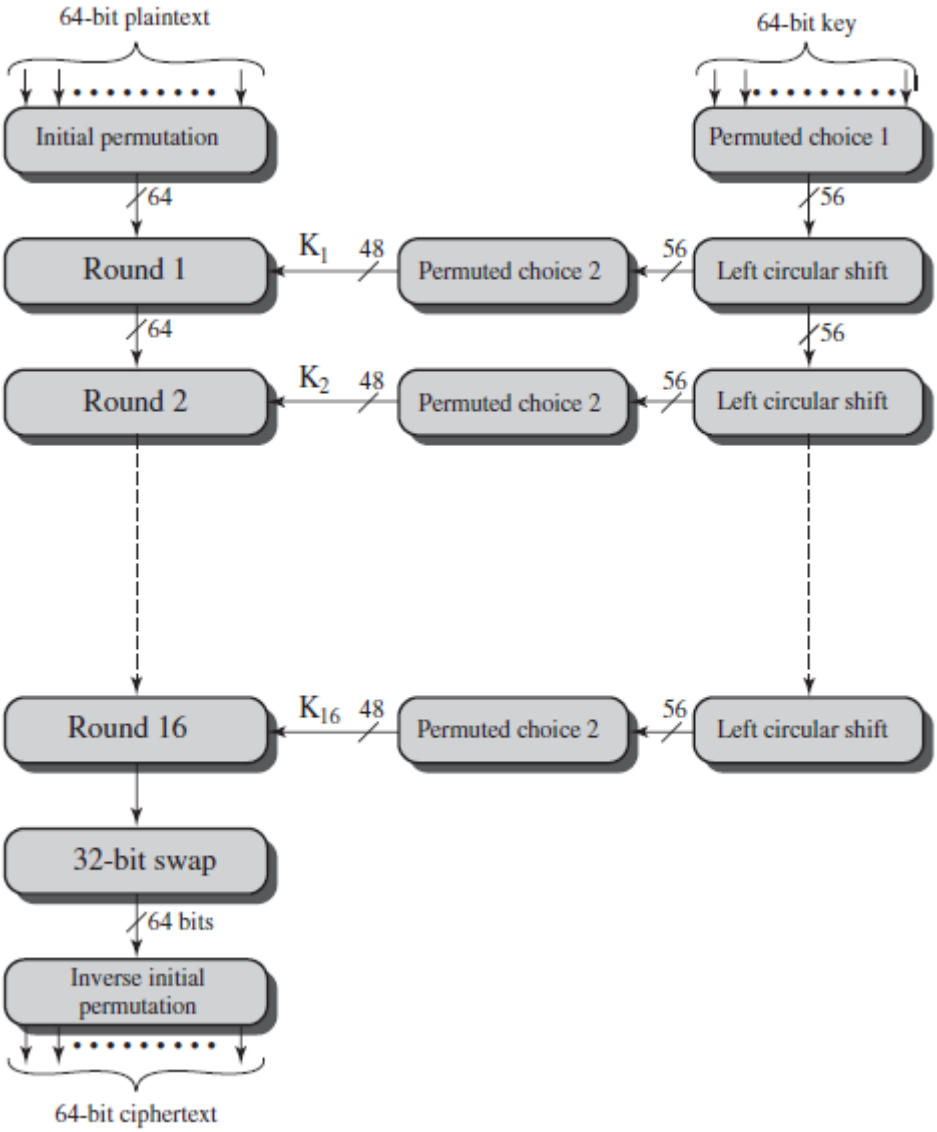
- A block cipher is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Many block ciphers have a Feistel structure.



(b) Block cipher

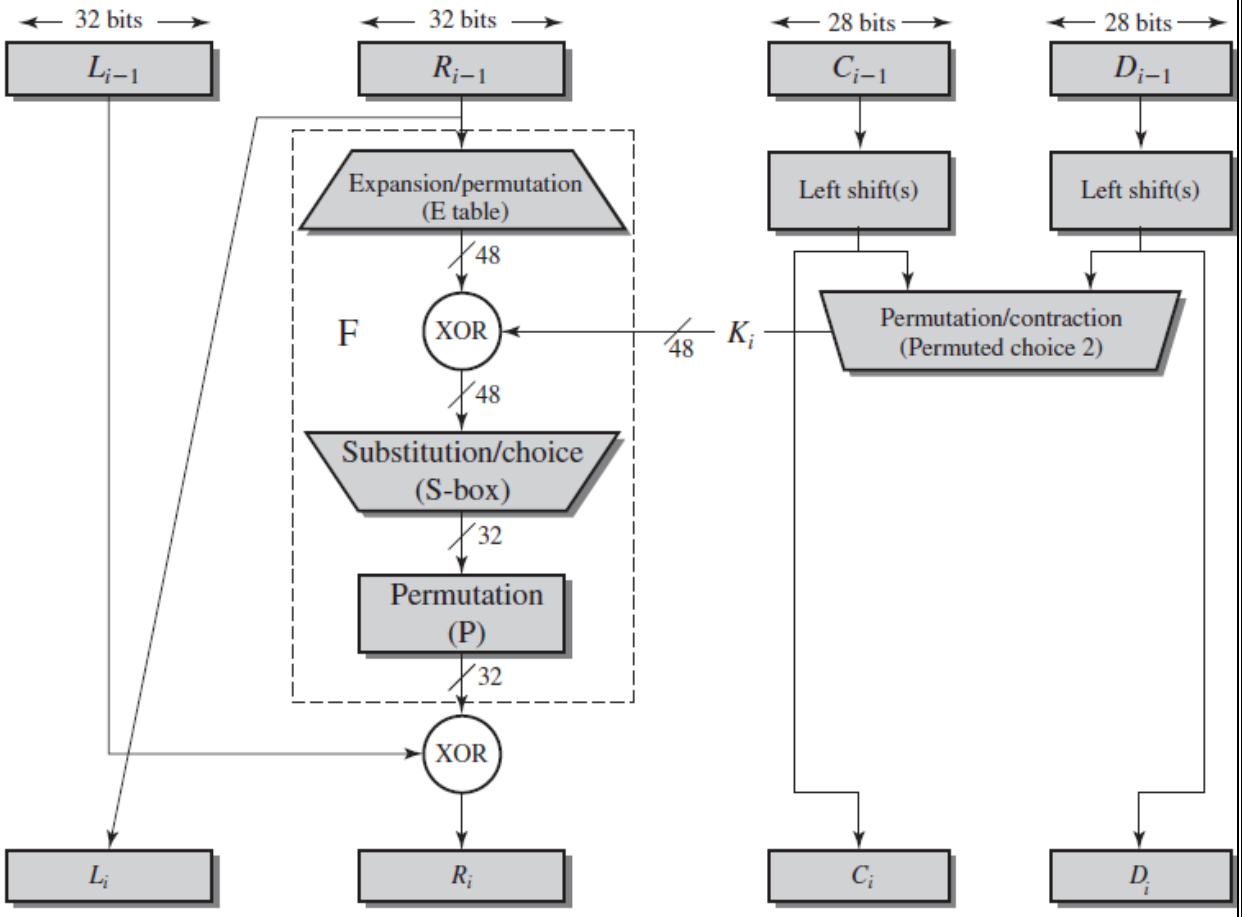
3.3 Data Encryption Standard (DES)

- 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
- **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 preoutput.
  - Finally, the preoutput is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext

- Right-hand portion of Figure shows the way in which the 56-bit key is used.
  - Initially, the key is passed through a permutation function.
  - Then, for each of the sixteen rounds, a subkey (K_i) 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.



- Details of Single 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:
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
  - 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 S_i 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.

- **DES Decryption**
  - Decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed.
- The Avalanche Effect
  - A small change in either the plaintext or the key should produce a significant change in the cipher text.
  - In particular, 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.

3.4 Strength of DES

The level of security provided by DES fall into two areas: key size and the nature of the algorithm.

- The Use of 56-Bit Keys
  - With a key length of 56 bits, there are 2^{56} possible keys, which is approximately $7.2*10^{16}$ keys.
  - A brute-force attack is impractical on DES.
  - On average, 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.
- 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. Despite this, no one has so far succeeded in discovering the supposed fatal weaknesses in the S-boxes.
- 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.

3.5 Block Cipher Design Principles

The three critical aspects of block cipher design:

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

- The 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.
  -
- 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

- 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.

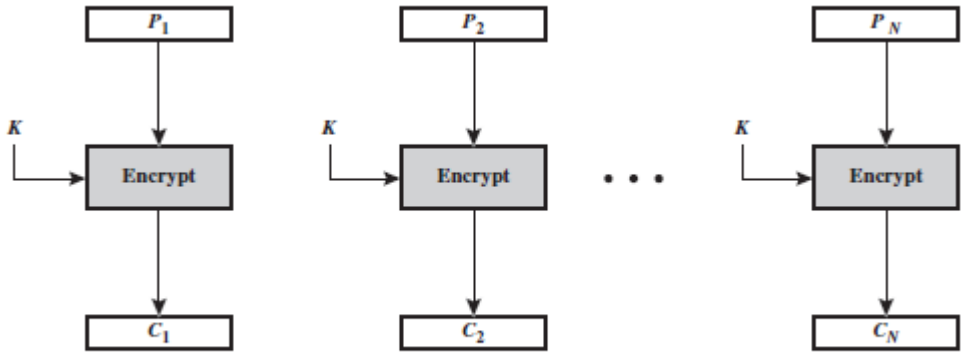
- The criteria for the permutation P are as follows.
  1. The four output bits from each S-box at round are distributed so that two of them affect "middle bits" of round $(i + 1)$ and the other two affect end bits.
  2. The four output bits from each S-box affect six different S-boxes on the next round, 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.

3.6 Modes of operation

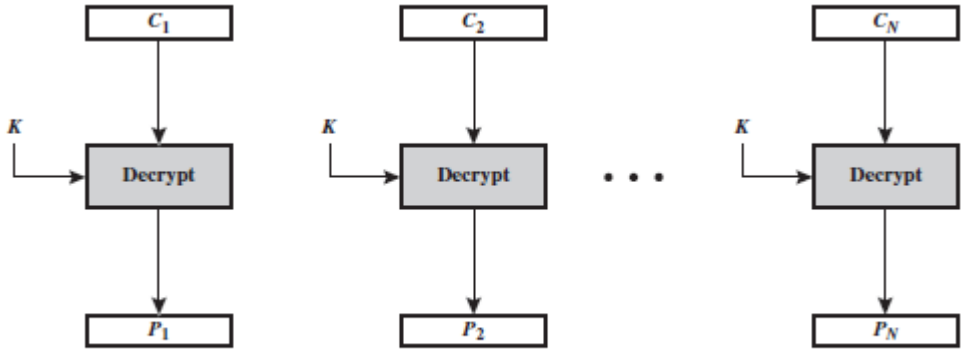
- A block cipher takes a fixed-length block of text of length bits and a key as input and produces a -bit block of ciphertext.
- If the amount of plaintext to be encrypted is greater than b bits, then the block cipher can still be used by breaking the plaintext up into -bit blocks
- To apply a block 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)

3.6.1 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

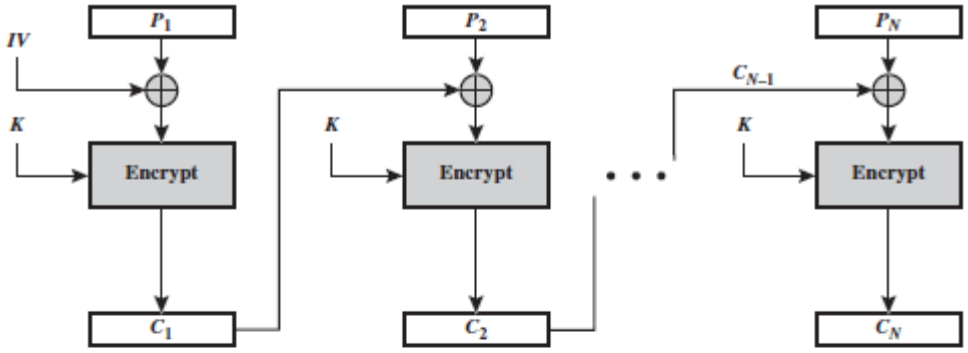


(b) Decryption

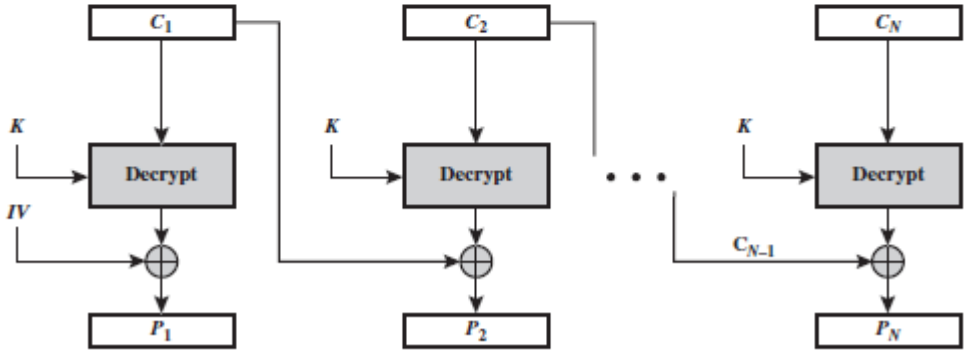
- The plaintext consists of a sequence of b-bit blocks, P_1, P_2.... P_N.
- The corresponding sequence of ciphertext blocks is C_1, C_2 ..... C_N
- ECB mode is defined as:
  - $Cj = E(K, Pj)$ $j = 1, ..., N$ (Encryption)
  - $Pj = D(K, Cj)$ $j = 1, ... , N$ (Decryption)
- The ECB method is ideal for 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

3.6.2 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

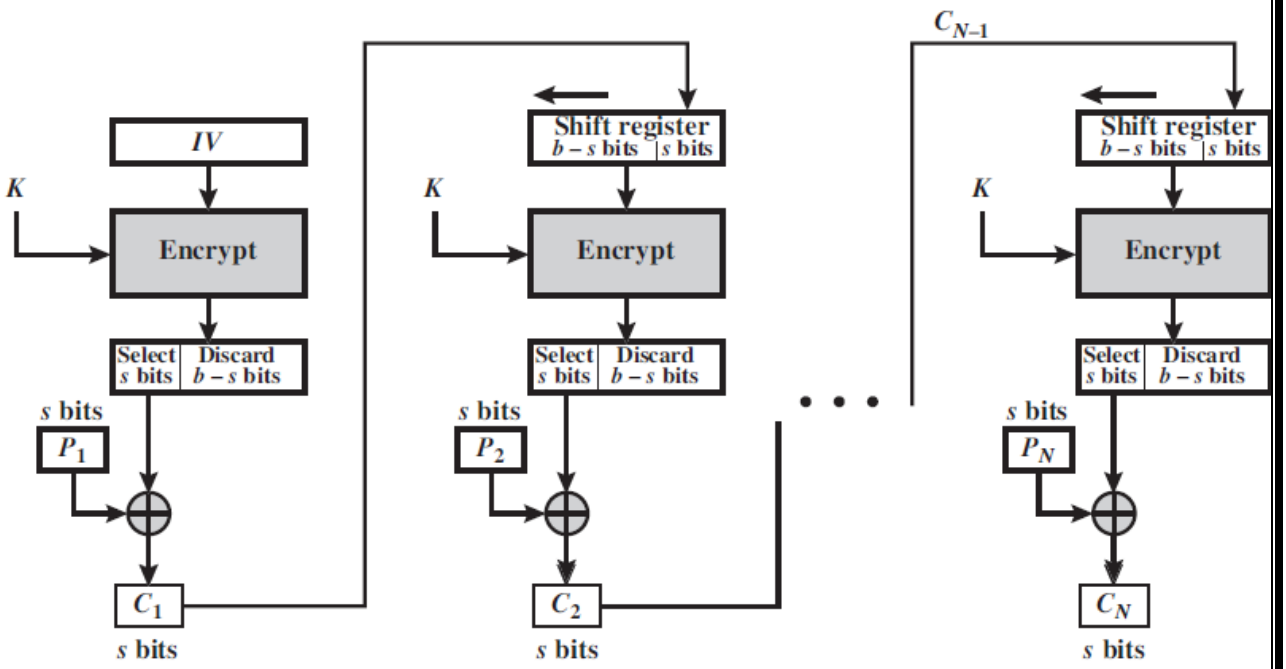
- On decryption, the IV is XORed with the output of the decryption algorithm to recover the first block of plaintext.
- The IV is a data block that is that same size as the cipher block.
- The IV must be known to both the sender and receiver but be unpredictable by a third party.
- We can define CBC 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
    - $P_1 = D(K, C_1) \oplus IV$

- $P_j = D(K, C_j) \oplus C_{j-1}$ $j = 2, \ldots N$

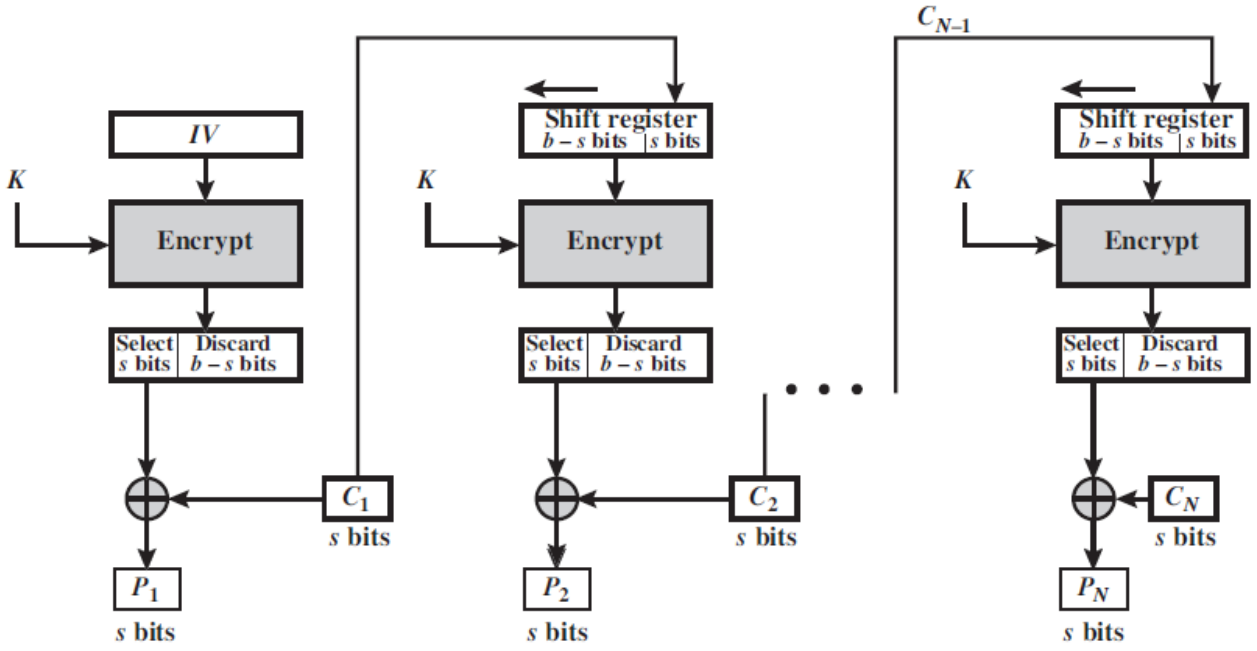
➢ each ciphertext block depends on all message blocks thus a change in the message affects all ciphertext blocks after the change as well as the original block

3.6.3 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)]



(a) Encryption

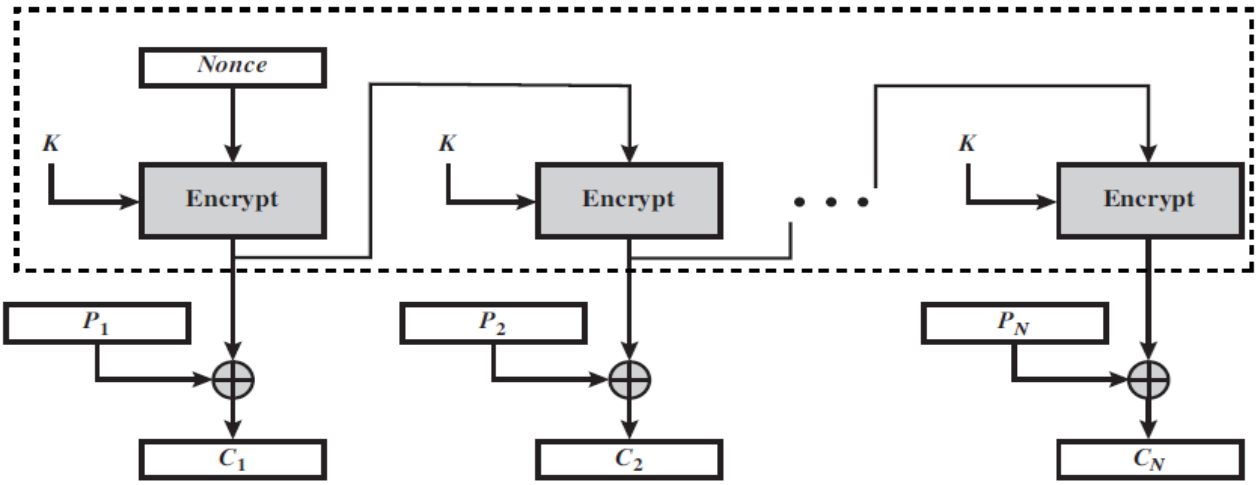


(b) Decryption

- This is most common stream mode
- The disadvantage is errors propagate for several blocks after the error occurred.

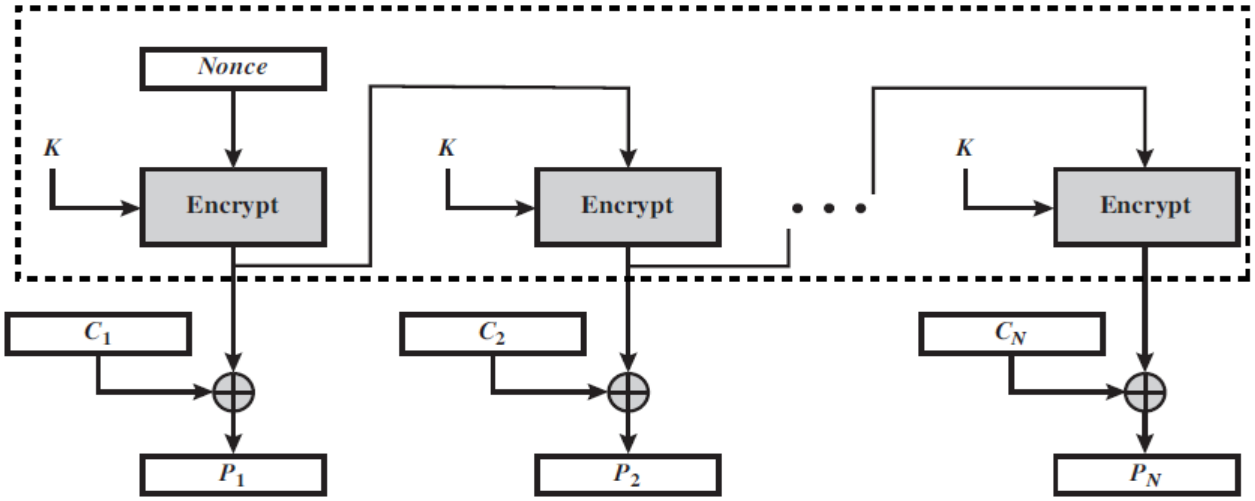
3.6.4 Output Feedback (OFB)

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

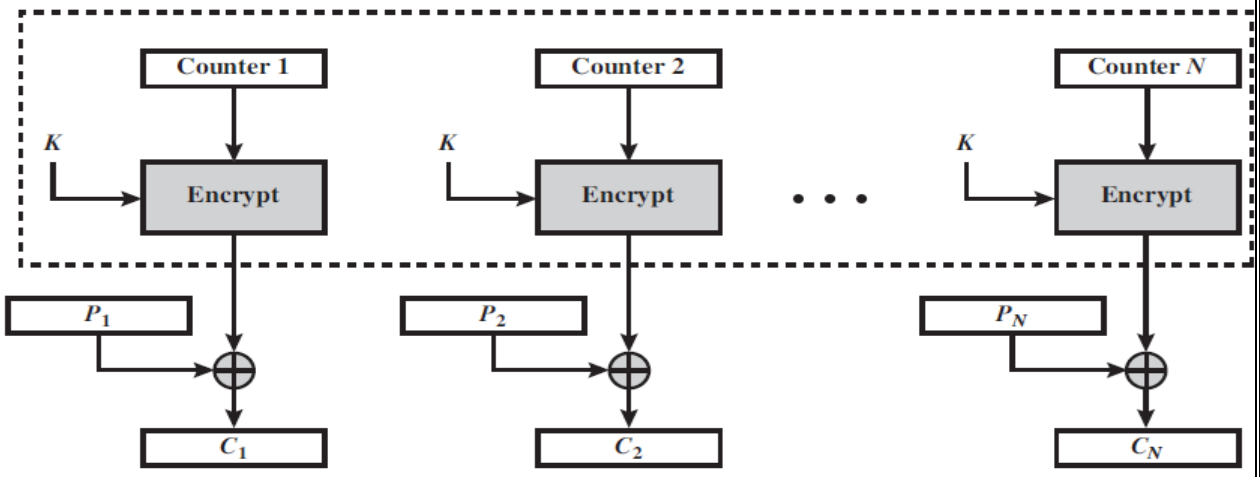


(b) Decryption

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

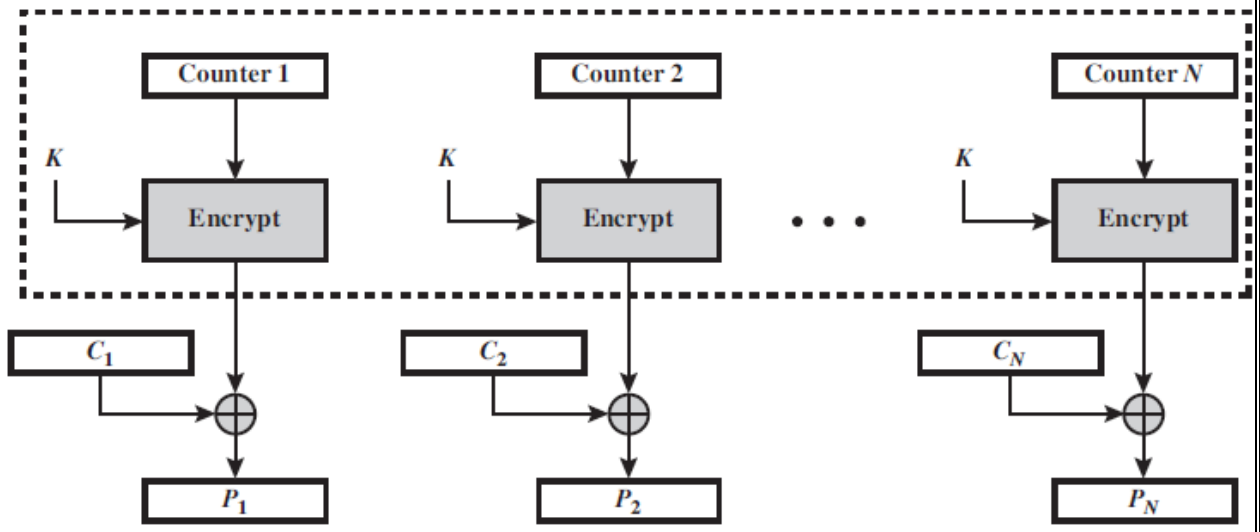
3.6.5 Counter (CTR)a

- similar to OFB but encrypts counter value rather than any feedback value
- A counter equal to the plaintext block size is used.
- the counter value must be different for each plaintext block that is encrypted
- Typically, the counter is initialized to some value and then incremented by 1 for each subsequent block
- For encryption, the counter is encrypted and then XORed with the plaintext block to produce the ciphertext block; there is no chaining.
- For decryption, the same sequence of counter values is used, with each encrypted counter XORed with a ciphertext block to recover the corresponding plaintext block.



(a) Encryption

- Encryption can be expressed as $C_j = P_j \oplus \mathrm{E}(K, T_j)$

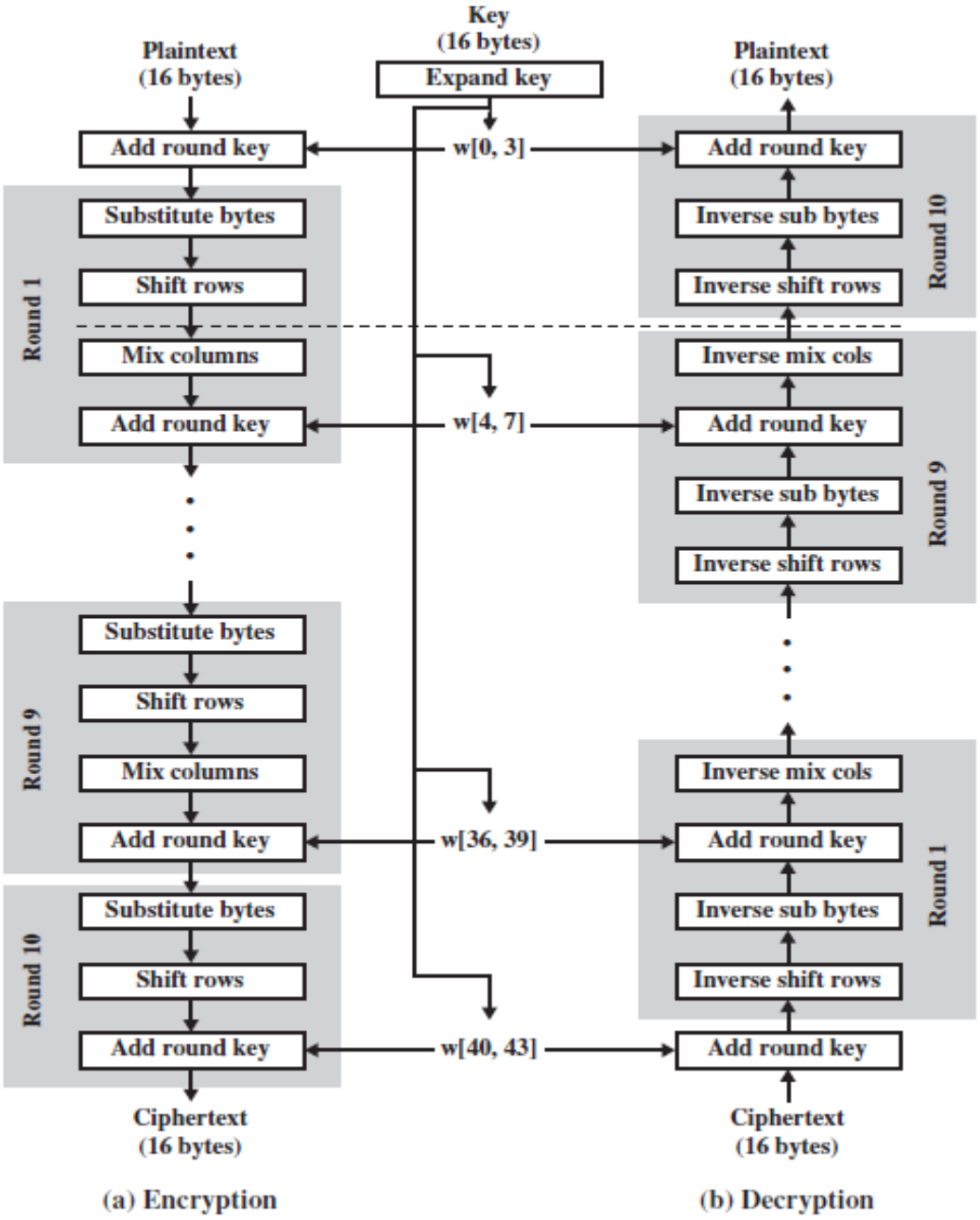


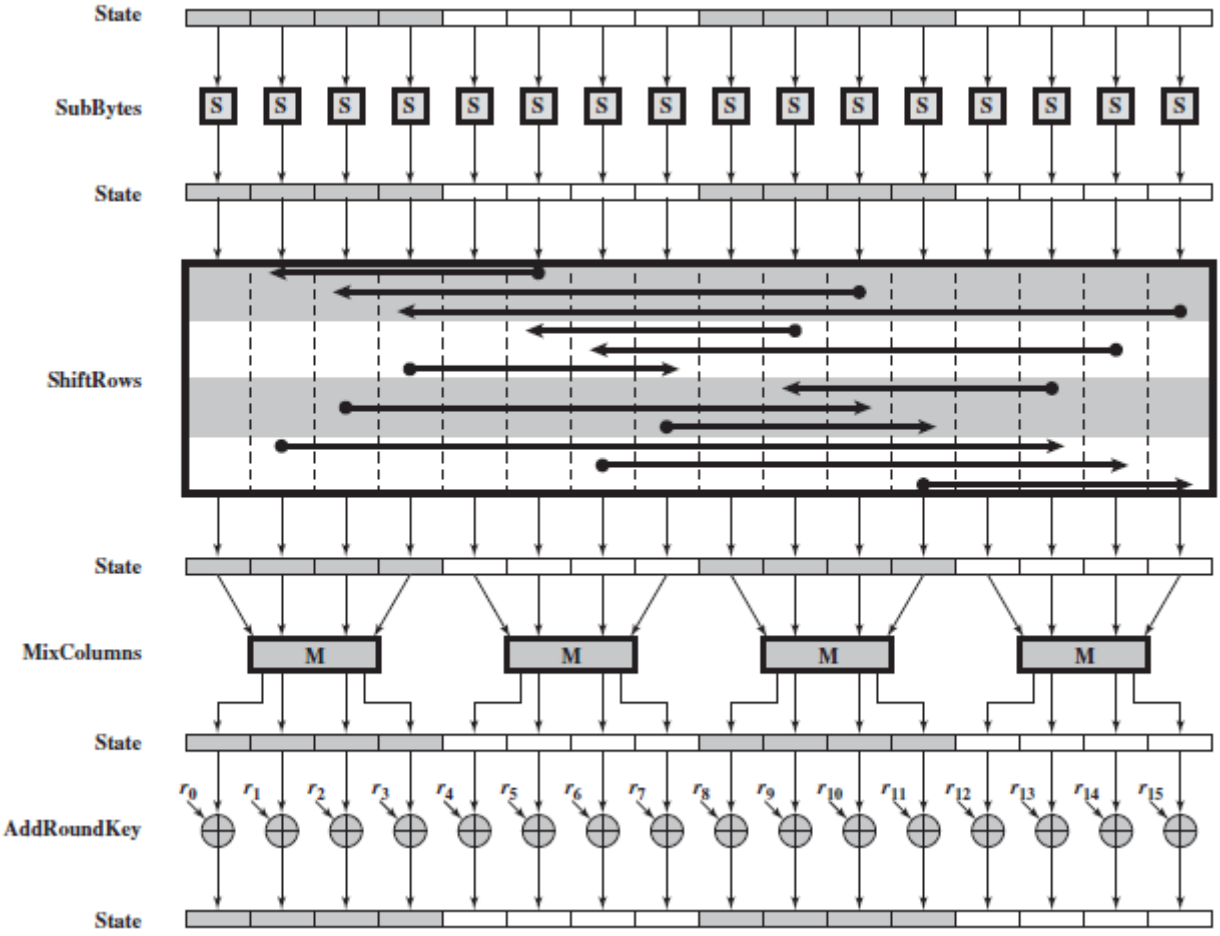
(b) Decryption

- Decryption can be expressed as $P_j = C_j \oplus \mathrm{E}(K, T_j)$

3.8 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. Instead, each full round consists of four separate functions: byte substitution, permutation, arithmetic operations over a finite field, and XOR with a key.
- 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.
- Four different stages are used, one of permutation and three of substitution
    - **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


Key
(16 bytes)
Expand key
Plaintext
(16 bytes)
Add round key
w[0, 3]
Substitute bytes
Shift rows
Mix columns
Add round key
w[4, 7]
Round 1
Substitute bytes
Shift rows
Mix columns
Add round key
w[36, 39]
Round 9
Substitute bytes
Shift rows
Add round key
w[40, 43]
Round 10
Ciphertext
(16 bytes)
(a) Encryption
Plaintext
(16 bytes)
Add round key
Inverse sub bytes
Inverse shift rows
Round 10
Inverse mix cols
Add round key
Inverse sub bytes
Inverse shift rows
Round 9
Inverse mix cols
Add round key
Inverse sub bytes
Inverse shift rows
Round 1
Add round key
Ciphertext
(16 bytes)
(b) Decryption

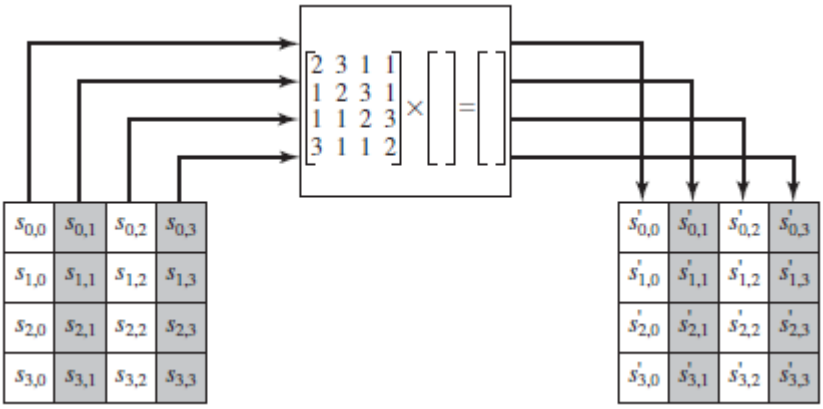


- Substitute Bytes Transformation
  - AES defines a 16 X 16 matrix of byte values, called an S-box.
  - It contains a permutation of all possible 256 8-bit values
  - Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value 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.
  - For example: byte {95} is replaced by row 9 col 5 byte value ie {2A}
- Shift Rows
  - 1st row is unchanged
  - 2nd row does 1 byte circular shift to left
  - 3rd row does 2 byte circular shift to left
  - 4th row does 3 byte circular shift to left
  - decrypt does shifts to right

- since state is processed by columns, this step permutes bytes between the columns

➢ Mix Columns

- each column is processed separately
- each byte is replaced by a value dependent on all 4 bytes in the column



- The transformation can be defined by the following matrix multiplication on State.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

-

➢ Add Round Key

- the 128 bits of State are bitwise XORed with the 128 bits of the round key.
- the operation is viewed as a column wise operation between the 4 bytes of a State column and one word of the round key
- The following is an example of AddRoundKey:

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$\oplus$

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

$=$

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

-
- The first matrix is State, and the second matrix is the round key.
- The inverse add round key transformation is identical to the forward add round key transformation, because the XOR operation is its own inverse.

➢ AES Key Expansion

- takes 128-bit (16-byte) key and expands into array of 44/52/60 32-bit words
- start by copying key into first 4 words
- then loop creating words that depend on values in previous & 4 places back
- in 3 of 4 cases just XOR these together
- every 4th has S-box + rotate + XOR constant of previous before XOR together
- designed to resist known attacks

- AES Decryption
  - AES decryption is not identical to encryption since steps done in reverse
  - 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 columns & add (tweaked) round key

Assignment-Cum- Tutorial Questions

A) Objective Questions

1. _____ is the original intelligible message or data that is fed into the algorithm as input.
2. _____ algorithm performs various substitutions and transformations on the plaintext.
   a. Encryption b. Decryption c. Both
3. _____ is the scrambled message produced as output
   a. Plain Text b. Cipher Text
4. If Encryption algorithm uses single key, it is called as _____
5. _____ uses two different keys, one for encryption and one for decryption.
6. _____ attack The attacker tries every possible key on a piece of ciphertext
   a. Brute-Force attack b. cryptanalysis
7. _____ cipher process one block of data at a time
8. _____ is the size of plain text in DES
   a. 64 bit b. 128 bit c. 32 bit d.56bit
9. What is the size of Key in DES?
   a. 64bit b. 128 bit c. 32 bit d.56bit
10. How many rounds are present in DES??
    a. 12 b. 10 c. 16 d. 11
11. Strength of DES lies in _____
    a. S- Boxes b. 56 bit key c. plain text d. both a, b
12. What is the size of plain text in AES?
    a. 64 bit b. 128 bit C. 56 bit d. 32 bit
13. ShiftRows in AES do simple _____
14. In _____ mode of cipher operation cipher feedback is given as input to the next function
    a. Output feedback mode b. cipher feedback c. counter mode
15. In _____ mode each block of plain text is encoded separately
    a. cipher feedback b. Counter mode c. electronic codebook
16. _____ each element in the plaintext is mapped into another element.
17. _____ technique elements in the plaintext are rearranged.
18. _____ processes the input elements continuously
    a. Block cipher b. stream cipher
19. In which technique the messages are concealed?

a. Steganography b. cryptography

20. In which technique the messages are converted to unreadable format?
    a. Steganography b. cryptography
21. What is the output of Permuted Choice 2 in round function of DES
    a. 48 bit key b. 56 bit key c. 64bit key
22. How many S-boxes are present in DES? _____
23. If an AES algorithm takes an input of 128bits plain text and 128 bit key, how many rounds need to be present in the algorithm? _____
    a. 10 rounds b. 12 rounds c. 14 rounds
24. Different names of AES (like AES-128, AES-192, AES-256) are based on _____
25. The input size of plaintext in Electronic codebook mode is _____
    a. 64bit b. 56 bit c. 128bit d. 192 bit
26. Each block of plaintext in COUNTER (CTR) mode is _____ with an encrypted counter
    a. AND b. OR c. XOR d. NAND

B. Descriptive Questions

1. **What are the five ingredients to a symmetric encryption scheme? Explain with a diagram.**
2. **Define stream cipher and block cipher?**
3. **Give the general depiction of DES encryption algorithm**
4. **State the round function of DES algorithm**
5. Describe the block cipher design principles
6. **State the encryption and decryption process of AES algorithm**
7. Define the electronic code book mode of operation
8. Recall the counter mode in block cipher mode of operations
9. Differentiate block cipher and stream cipher mode of operations
10. **Identify the strengths of DES Algorithm.**
11. Distinguish Cipher feedback mode and output Feedback mode
12. **Describe the purpose of a counter in COUNTER (CTR) mode.**

C. GATE oriented

I Objective Questions

1. If both sender and receiver uses a single key for both encryption and decryption it is known as _____
2. Symmetric encryption algorithm is also called as _____
3. If sender and receiver uses different keys for encryption and decryption, the algorithm is known as _____
4. Asymmetric encryption algorithm is also known as _____

II Descriptive Questions

1. Differentiate the symmetric and asymmetric encryption process.