Part-A

1. What is avalanche effect?

Avalanche affect:

If a small change in the key or plaintext were to produce a corresponding small change in the cipher text, this might be used to effectively reduce the size of the plaintext (or key) space to be searched. The avalanche effect is, in which a small change in plaintext or key produces a large change in the ciphertext.

2. Define steganography:

Steganography:

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data stenography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

3. What is the difference between a block cipher and a stream cipher?

Block cipher	stream cipher .
*A block cipher process the input one block of elements at a time	*A stream cipher processes the input elements continuously .
* Block cipher produce an output block for each input block	*stream cipher produce output for one element at a time .
* Example of block cipher : DES .	* Example of stream cipher: Caeser cipher .

4. Give the five modes of Operation of block cipher.

Five modes of Operation:

* Electronic code Block (ECB)
* Cipher Block chaining (CBC)
* Cipher Feed back (CFB)
* Output Feed Back (OFB)
* Caunter (CTR).

5. Compare DES and AES

DES	AES .
DES stands for Data Encryption standard	AES stands for Advanced Encryption Standard
key length is 56 bits	key length can be of 128

	bits , 192-bits and 256 bits.
DEs involves 16 rounds of identical operations	Number of rounds depends on key length : 10 (128-bits), 12 (192-bits) or 14(256-bits)
DEs can encrypt 64 bits of plaintext	AES can encrypt 128 bits of plaintext.

Part-B

1. Explain OSI security architecture model with neat diagram.

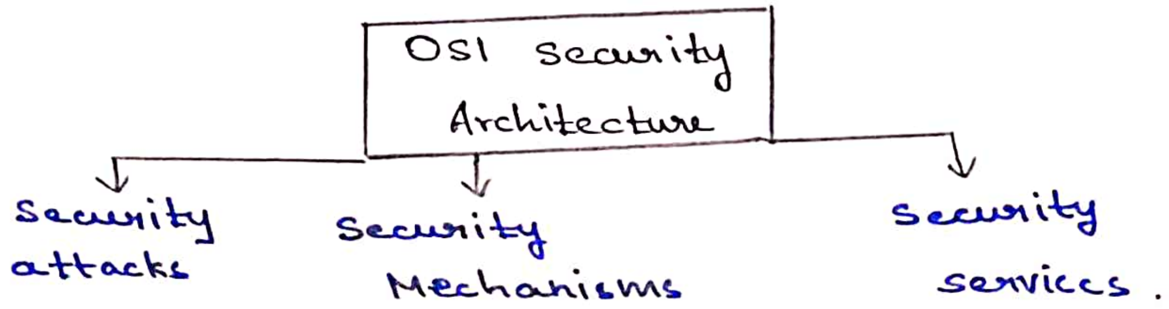
OSI Security Architecture

* The OSI security architecture is useful to managers as a way of organizing the task of providing security.

* The OSI security Architecture defines a systematic approach to providing security at each layer.

* It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network.

ITU-T4 Recommendation X.800, Security Architecture for OSI, defines such a systematic approach



Security Attack:

* Any action that compromise the security of information owned by an organization.

* Securities of these components are evaluated in terms of Vulnerability, threats, attacks and Control.

Two types.

* Passive attacks
* Active attacks.

Passive Attack:

* passive attacks are those, wherein the attacker indulges in eavesdropping on, or monitoring of data transmission. A passive attack attempts to learn or make use of

information from the system but does not affect system resources.

passive attacks are of two types.

* Release of message contents
* Traffic analysis.

Release of message Content:

A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information we would like to prevent an opponent from learning the content of these transmissions.

Traffic analysis:

* Mask the contents of message so that Opponents could not extract the information from the message. Encryption is used for marking

* This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device.

Active Attacks:

Active attacks involves some modification of the data stream or the creation of a false stream. These attacks can not be prevented easily.

Active attacks can be subdivided into 4 types.

- * Masquerade
- * Replay
- * Modification of Message
- * Denial of message.

Masquerade:

It takes place when one entity pretends to be a different entity.

Replay:

It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of Message:

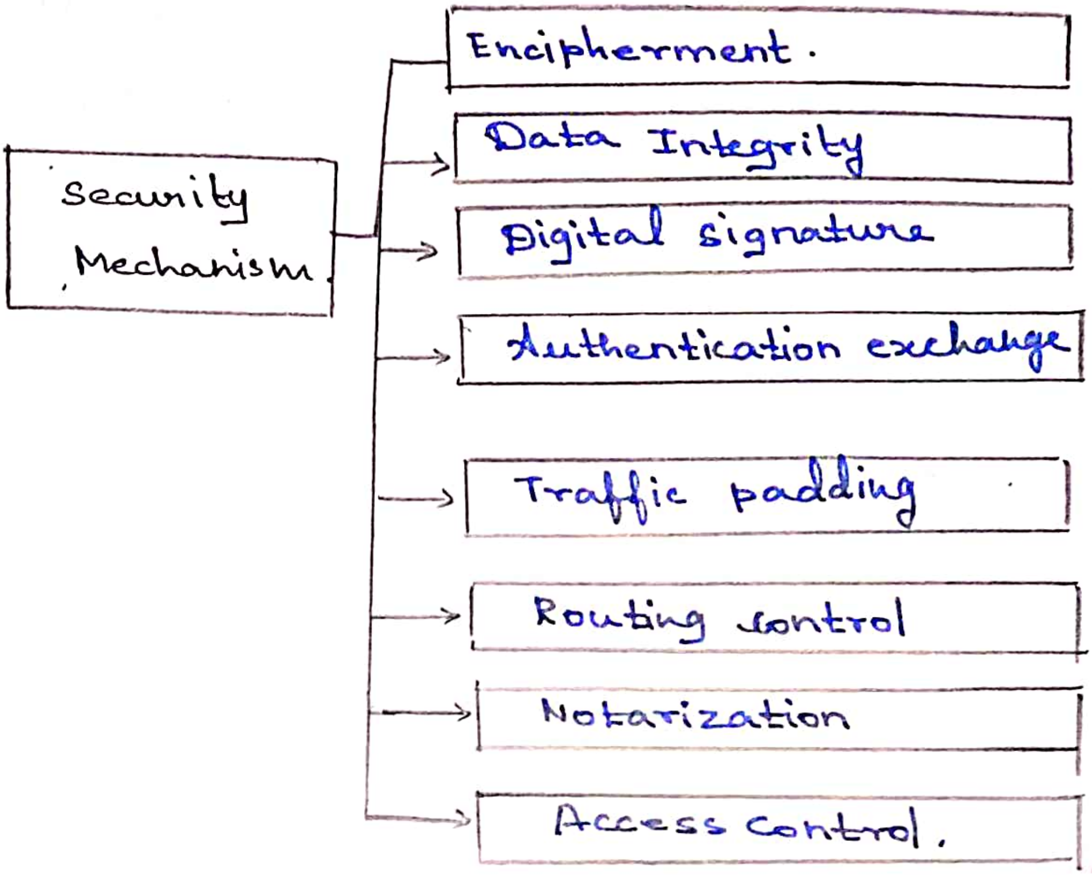
It involves some change to the original message. It produces an unauthorized effect.

Security Mechanism:

* A Mechanism that is designed to detect, prevent or recover from a security attack.

* A security Mechanism are technical tools and techniques that are used to implement security services. A Mechanism might operate by

itself, or with others, to provide a particular service .



Pervasive Security Mechanism .

- Trusted functionality
- Event detection
- Security label
- security Recovery .

* Security Services :

Security services refer to the different services available for maintaining the security and safety of an organization .

∴ 5 types :

Authentication: is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.

Access control:

It Involves the use of policies and procedures to determine who is allowed to access specific resource. within a system.

Data Integrity:

It is a security Mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.

Non-reputation:

It involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent.

Data confidentiality

It is responsible for the protection of information from being accessed or disclosed to unauthorized parties.

2. Explain DES Algorithm with neat diagram and explain the steps.

Data Encryption standard

* DES Encryption standard (DES) is a Symmetric key block cipher published by the National Institute of standards and Technology (NIST).

* It encrypts data in 64-bit block.

* DES is Symmetric key algorithm: The same key and algorithm is used for both encryption and decryption.

* key size is 56-bit.

* The encryption process is made of .2 permutations i.e. P-boxes, which is called initial and final permutations.

* The cipher Consist of 16 rounds or iterations. Each round uses a separate Key of 48-bits.

Steps:

1. Initial permutation (IP):

Rearrange the 64-bit plaintext according to a fixed permutation table

Divide the 64 bits into two 32-bit blocks: left (L0) and right (R0).

2. key Schedule Generation:

* The 56-bit key is divided into two 28-bit halves (C0 and D0).

* Generate 16 rounds keys (k1 to k16) using a shifting and permutation process.

3. 16 Rounds of Substitution and permutation

For each round (1 to 16)

* Expand Rn-1 to 48 bits using an expansion Permutation (E-bit Selection).

* XOR the expanded result with the round key kn.

* Divide the XORed result into eight 6-bit blocks.

* Apply the S-boxes to each 6-bit block, producing eight 4-bit outputs.

* Permute the 32-bit output using a fixed permutation table (P-box)

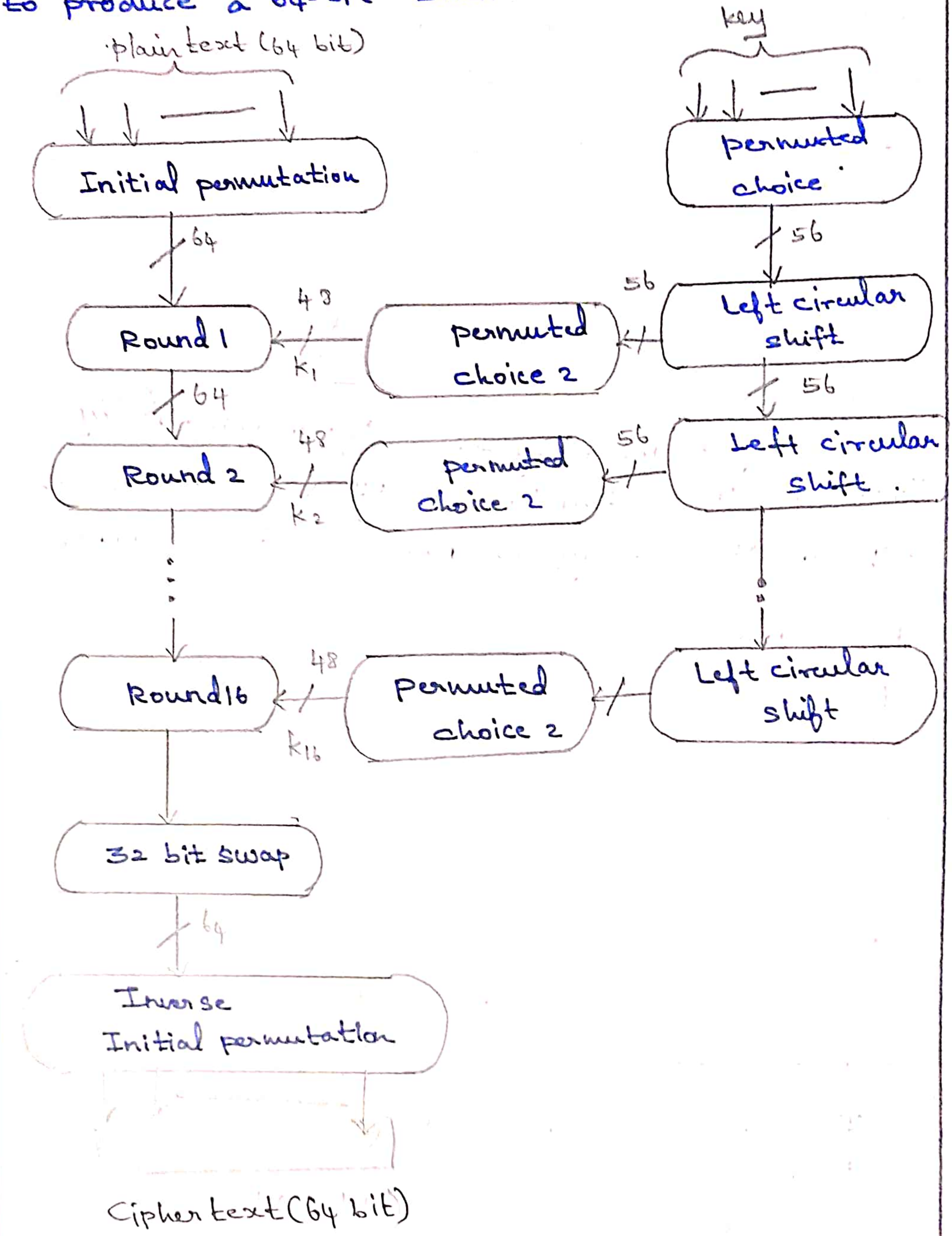
* XOR the permuted result with Ln-1

* Swap Rn-1 and Ln-1 (Rn = Ln-1, Ln = Rn-1 XOR F(Rn-1, kn))

4. Inverse permutation (IP^{-1})

After 16 rounds, combine the final left and right halves (L16 and R16).

* Apply the inverse of the initial permutation to produce a 64-bit block.



5.
Final ciphertext :

* The 64-bit block obtained from the inverse Permutation is the ciphertext.

* Each round of DES involves expansion, substitution, Permutation, and XOR operations, Contributing to the encryption process. The steps are reversible for decryption by using the round keys in reverse order.

3. What do you mean by AES? Diagrammatically illustrate the Structure of AES and describe the steps in AES encryption process with example.

AES Cipher :

* AES is a non-Feistel cipher that encrypts and decrypts a data block of 128-bit.

* The key size can be 128, 192 or 256 bits. It depends on number of rounds

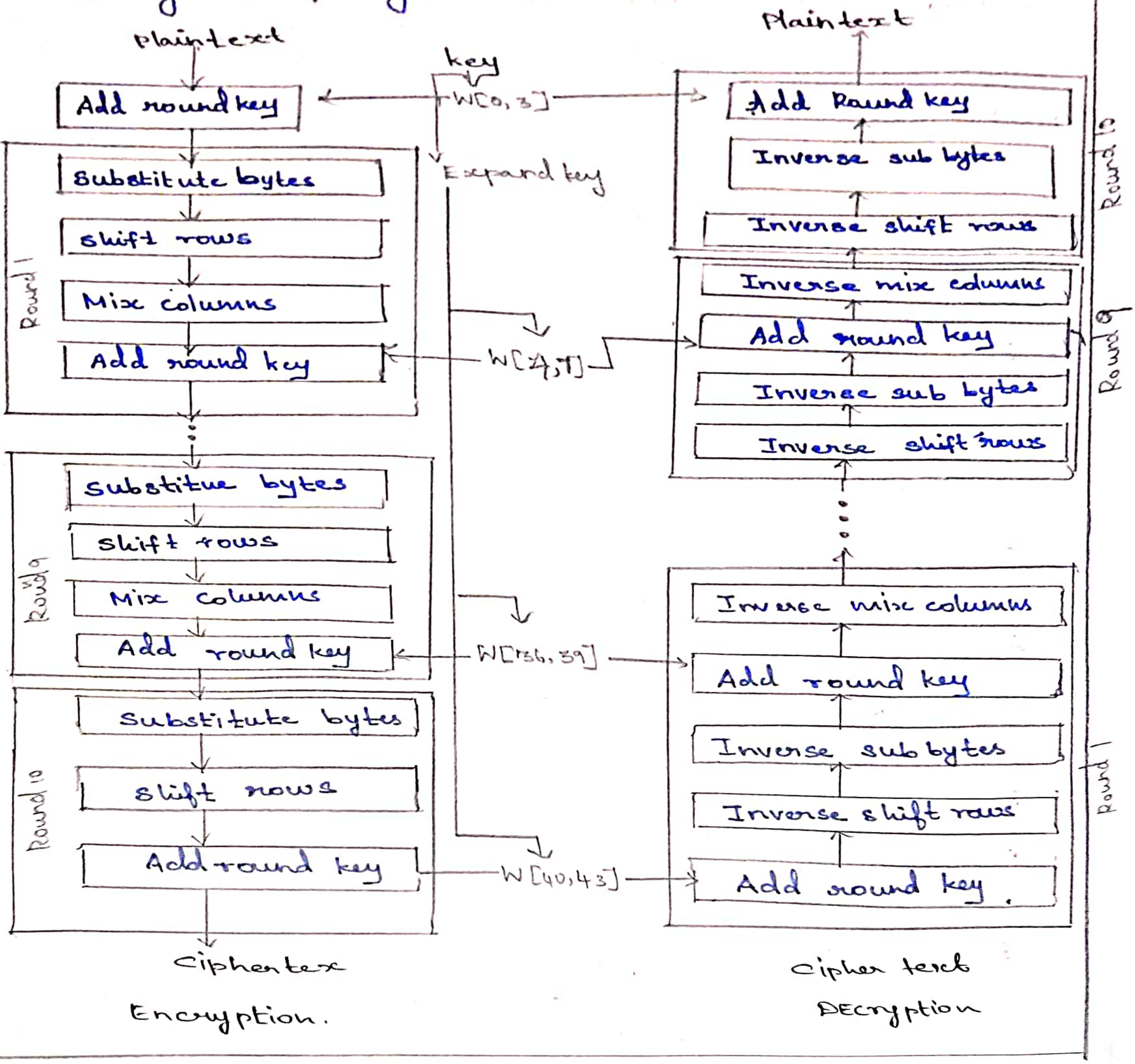
* The number of rounds: 10 rounds for 128-bits, 12 rounds for 192-bits, and 14 rounds for 256-bits.

Characteristics :

* Resistance against all known attacks.

* Speed and code compactness on a wide range of platforms.

* Design simplicity.



Comments about the AES structure :

* AES structure is not a Feistal structure

* The key that is provided as input is expanded into an array of forty-four 32 bit words. W(i)

* Four different stages are used, one of permutation and three of substitution.

* For both encryption and decryption, the cipher begins with an AddRoundkey stage, followed by nine rounds that each includes all four stages followed by tenth round of three stages.

* Only the AddRoundkey stage make use of the key.

* The AddRoundkey stages is in effect, a form of Vernam cipher. and by itself would not be formidable.

* Each stage is easily reversible.

* The decryption algorithm makes use of the expanded key in reverse order.

* Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext.

* The final round of both encryption and decryption consist of only three stages.

AES Encryption process

* key Expansion: The secret encryption key is expanded into a set of round key that will be used in each encryption round.

* Initial Round:
The input data is divided into blocks. In the initial round, the plaintext block is combined with the first round key using a process called "Add Round key".

* Main Rounds:
A set number of main rounds (10, 12, or 14) depending on key size) Each round consist of four main transformations.

SubBytes: Bytes of the block are replaced with values from a Substitution table (S-box).

ShiftRows: Bytes within each row of the block are shifted left.

Mixcolumns: columns of the block are mixed using matrix multiplication.

AddRoundkey : The block is XORed with a round key derived from the main encryption key.

* Final Round : In the last round, the MixColumns transformation is skipped.

* Cipher Text : After all rounds, the resulting transformed data is the cipher text.

Decryption Follows similar process in Reverse.