Information security policies

" A D I P A "

Information security policies are a set of rules, procedures, and guidelines that define how an organization manages, protects, and uses its information assets. There are various types of security policies in information security, including:

1. Access Control Policy: This policy defines how access to information resources is granted, managed, and revoked. It outlines the procedures for granting and revoking access rights and specifies the roles and responsibilities of individuals who manage access control.
2. Data Classification Policy: This policy defines how information assets are classified based on their sensitivity and criticality to the organization. It outlines the criteria for classifying information and the procedures for handling, storing, and transmitting classified information.
3. Incident Response Policy: This policy outlines the procedures for responding to security incidents, such as data breaches or cyber-attacks. It defines the roles and responsibilities of incident response team members, specifies the procedures for reporting and investigating incidents, and outlines the measures to be taken to mitigate the impact of incidents.
4. Password Policy: This policy outlines the requirements for creating and managing passwords. It defines the criteria for selecting strong passwords, specifies the procedures for changing and resetting passwords, and outlines the measures to be taken to protect passwords from unauthorized access.
5. Acceptable Use Policy: This policy defines the acceptable use of information resources, such as computers, networks, and the Internet, by employees and other authorized users. It outlines the rules and guidelines for using these resources and specifies the consequences of violating the policy.

Network security model

A network security model is a set of principles and guidelines that define the security architecture and mechanisms for securing a computer network. The model specifies how information is protected as it travels across the network, how access to network resources is controlled, and how network devices are secured.

working :

- A message is to be transferred from source to destination across some sort of internet. Both the sides must cooperate for the exchange of the data.
- A logical information channel is established by defining a route through the internet from source to destination.
- All the techniques for providing security have two components :
  1. A security related transformation on the information to be sent.
  2. Some secret information shared by the two principles, it is hoped, unknown to the opponent.
- Fig. 1.7.1 shows the network security model.
- A trusted third party is needed to achieve secure transmission.
- Basic tasks in designing a particular security service.
  1. Design an algorithm for performing the security related transformation.
  2. Generate the secret information to be used with the algorithm.
  3. Develop methods for the distribution and sharing of the secret information.

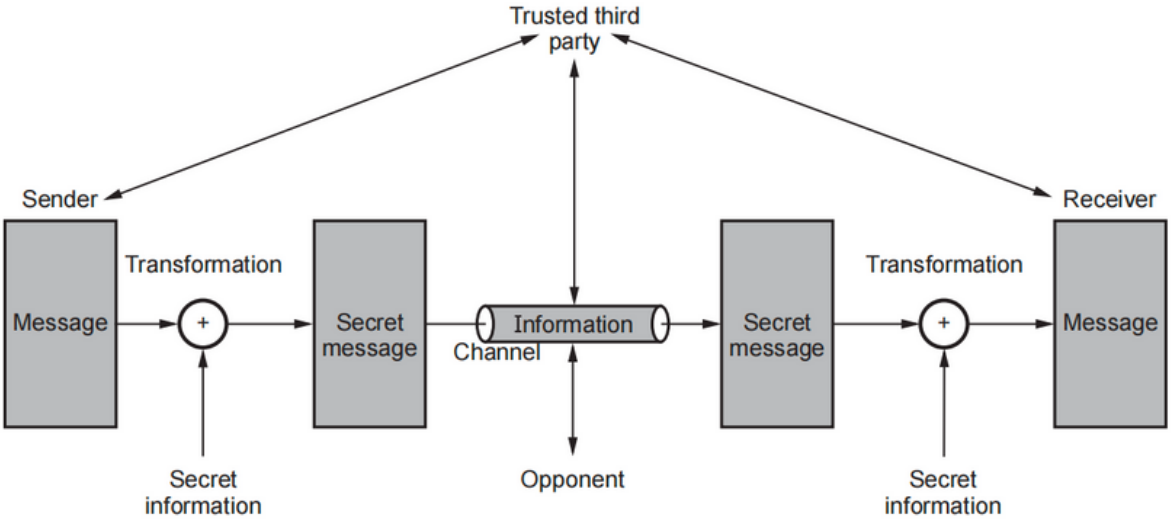


Fig. 1.7.1 Network security model

4. Specify a protocol to be used by the two principles that makes use of the security algorithm and the secret information to achieve a particular security service.

Cryptanalysis

Cryptanalysis is the process of breaking encrypted information, and a cryptanalyst is a person who specializes in this field. They use various methods to analyze and break encryption systems to access protected information.

Techniques:

Cryptanalysis is the art and science of analyzing and breaking cryptographic systems. The goal of cryptanalysis is to gain access to the encrypted information without knowing the key or password used to encrypt it. There are different techniques used in cryptanalysis, including:

1. Known plaintext attack: In this technique, the attacker has access to both the plaintext and its corresponding ciphertext. The attacker uses this information to deduce the key used to encrypt the plaintext.
2. Chosen plaintext attack: In this technique, the attacker can choose the plaintext to be encrypted and has access to its corresponding ciphertext. The attacker can use this information to deduce the key used to encrypt the plaintext.
3. Cipher-text only attack: In this technique, the attacker has access only to the encrypted ciphertext, without knowing anything about the plaintext or the key used to encrypt it. The attacker uses statistical and mathematical analysis to deduce the key used to encrypt the ciphertext.
4. Chosen cipher-text attack: In this technique, the attacker can choose the ciphertext to be decrypted and has access to its corresponding plaintext. The attacker can use this information to deduce the key used to encrypt the ciphertext.
5. Linear Cryptanalysis: Linear cryptanalysis is a statistical technique used to break symmetric-key cryptographic systems. It involves analyzing the linear relationships between the plaintext, ciphertext, and key to deduce the key used to encrypt the plaintext.
6. Differential Cryptanalysis: Differential cryptanalysis is a technique used to break symmetric-key cryptographic systems. It involves analyzing the differences between pairs of plaintext and their corresponding ciphertext to deduce the key used to encrypt the plaintext.

Comparison between linear cryptanalysis & differential cryptanalysis

> BOOK

Distinguish between Substitution and transposition ciphers

	Substitution ciphers	Transposition ciphers
Definition	Each letter or group of letters of the plaintext are replaced by some other letter of group of letters, to obtain the ciphertext.	Letters of the plaintext are permuted in some form.
Example	Hill cipher, one time pad	Rail fence cipher
Strength	1.Exhaustive search is infeasible. 2.Through to be unbreakable by many back then.	1.Reduce redundancies in plaintext. 2.Transposition cipher can be made more secure by performing more than one stage of transposition.
Drawback	1.Brute force attack is easy	1.The ciphertext has the same letter frequency as the original plaintext. 2.Guessing the number of columns and some probable words in the plaintext holds the key.

Comparison between Monoalphabetic & Polyalphabetic cipher

Sr. No.	Monoalphabetic cipher	Polyalphabetic cipher
1.	Once a key is chosen, each alphabetic character of a plaintext is mapped onto a **unique** alphabetic character of a ciphertext.	Each alphabetic character of a plaintext can be mapped onto "**m**" alphabetic characters of a ciphertext.
2.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-one.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-many.
3.	A stream cipher is a monoalphabetic cipher if the value of k_i does not depend on the position of the plaintext character in the plaintext stream	A stream cipher is a polyalphabetic cipher if the value of k_i does depend on the position of the plaintext character in the plaintext stream.
4.	Monoalphabetic cipher includes additive, multiplicative, affine and monoalphabetic substitution cipher.	Polyalphabetic cipher includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor , and Enigma cipher.

Comparison between stream & block cipher

Sr. No.	Stream cipher	Block cipher
1.	Stream ciphers operate on smaller units of plaintext.	Block ciphers operate on larger block of data.
2.	Faster than block cipher.	Slower than stream cipher.
3.	Stream cipher processes the input element continuously producing output one element at a time.	Block cipher processes the input one block of element at a time, producing an output block for each input block.
4.	Requires less code.	Requires more code.
5.	Only one time of key use.	Reuse of key is possible.
6.	Ex. - One time pad	Ex. - DES
7.	Application - SSL (secure connections on the web.)	Application - Database, file encryption.
8.	Stream cipher is more suitable for hardware implementation.	Easier to implement in software.

Security	Low	High
Speed	High	Low
Application	Real time data such as Voice	Non-real time such as documents
Commonly used	No	Yes

Block cipher

A block cipher is an encryption algorithm that operates on fixed-size blocks of data and uses a secret key to convert plaintext into ciphertext. It encrypts each block separately using the same key, and the resulting ciphertext is dependent on both the plaintext and the key.

Dictionary attack

Dictionary attack is a type of password guessing attack used in cryptanalysis. It is a relatively simple and commonly used technique to crack passwords in which the attacker tries to guess the correct password by using a list of words from a dictionary or other commonly used passwords.

The dictionary attack works as follows:

1. The attacker obtains a list of words from a dictionary, commonly used passwords, or other sources.
2. The attacker tries each word in the list as a password until the correct password is found.
3. If the password is not found in the list, the attacker can also try variations of the words, such as adding numbers or special characters to the end of the word.
4. The attacker can also use a hybrid attack, where a combination of words from the dictionary and brute force attacks are used to guess the password.
5. If the password is encrypted, the attacker can use a technique called rainbow tables to speed up the decryption process.
6. Once the correct password is found, the attacker can use it to gain unauthorized access to the system or sensitive information.

Different types of cipher block modes

- ## Electronic Code Book (ECB)

ECB stands for Electronic Codebook mode, which is a block cipher mode used in information security to encrypt and decrypt data.

In ECB mode, a plaintext message is divided into fixed-size blocks, typically 64 or 128 bits, and each block is encrypted independently using the same key. The output of the encryption operation is a ciphertext block, which can be decrypted using the same key and algorithm.

While ECB mode is simple and efficient, it has some weaknesses from a security perspective. In particular, if the same plaintext block is encrypted multiple times with the same key, it will always produce the same ciphertext block. This means that patterns in the plaintext can be easily identified in the ciphertext, and attackers can exploit this to perform certain attacks, such as known plaintext attacks.

As a result, more secure block cipher modes, such as CBC (Cipher Block Chaining) and GCM (Galois/Counter Mode), are typically used in modern cryptographic systems.

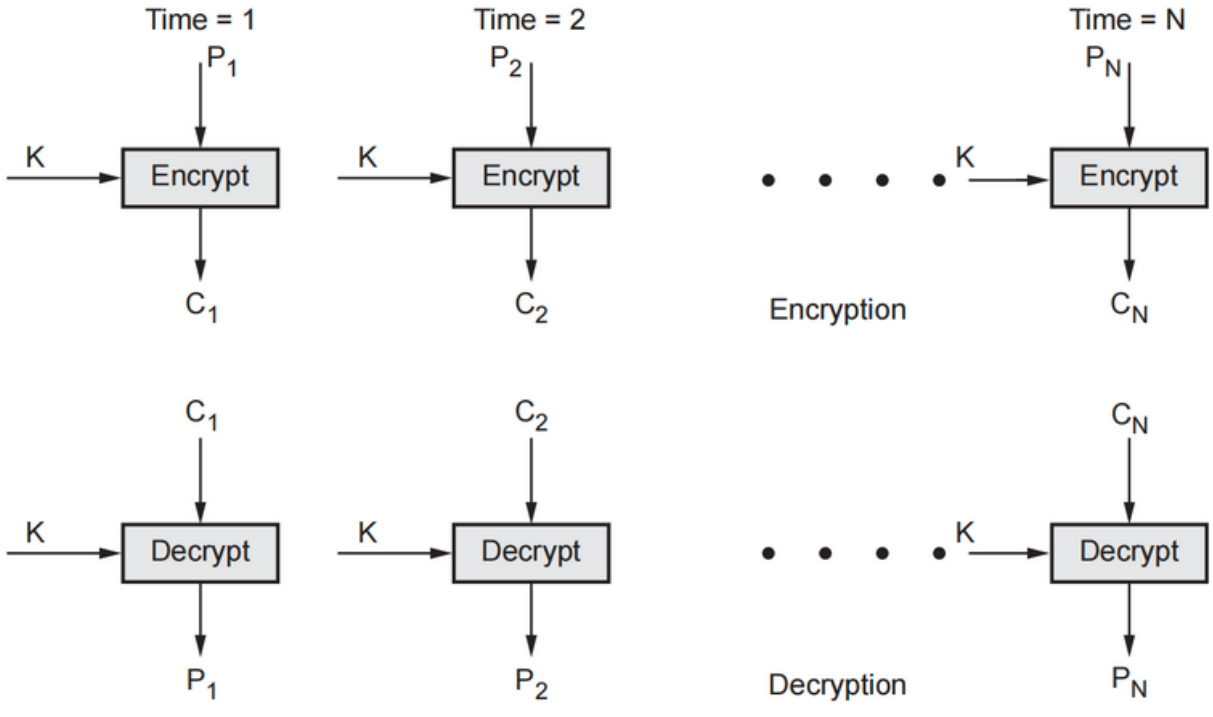


Fig. 2.7.1 ECB mode

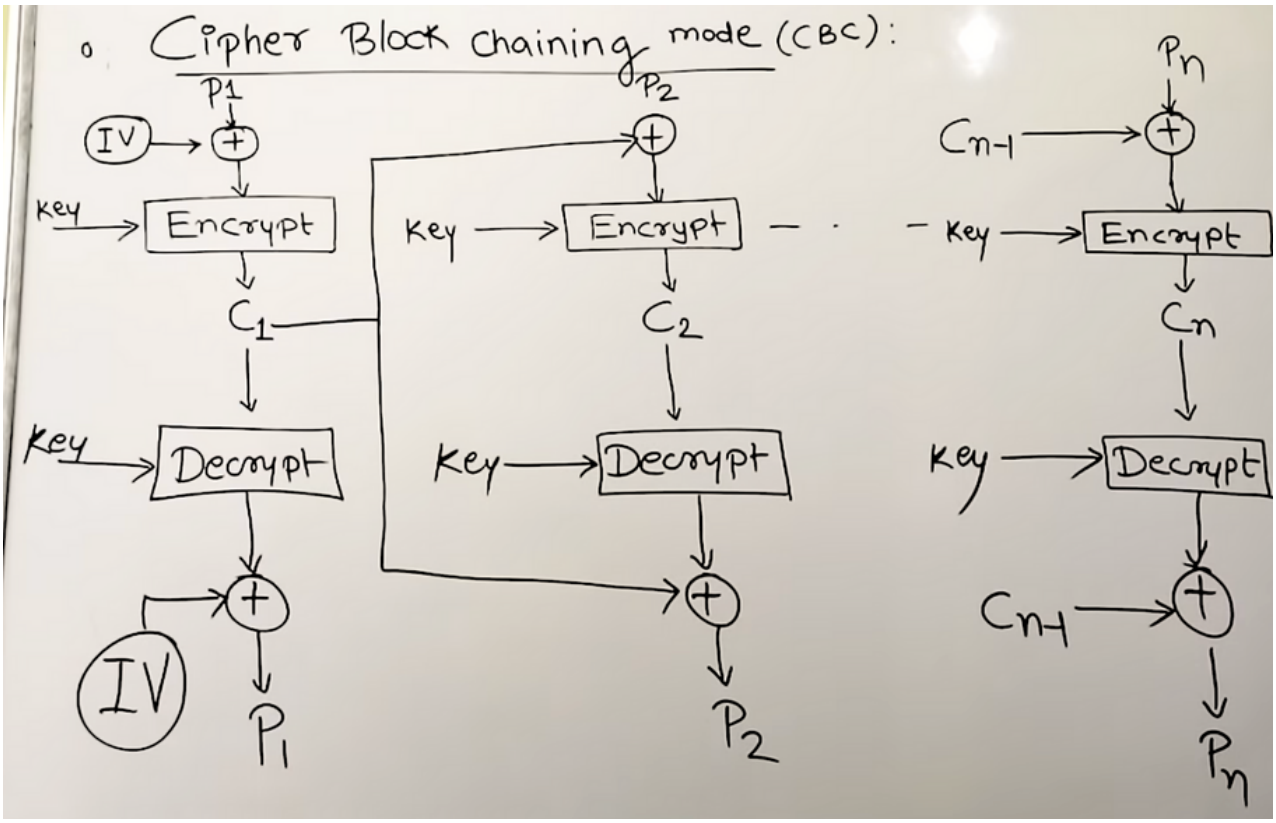
- **Cipher Block Chaining Mode (CBC)**

CBC (Cipher Block Chaining) is a block cipher mode of operation that is commonly used in information security for ensuring the confidentiality and integrity of data.

In CBC mode, plaintext is divided into fixed-length blocks, and each block is XORed with the previous ciphertext block before being encrypted. This means that each ciphertext block depends not only on the plaintext block being encrypted but also on all the previous plaintext blocks, providing better security against certain types of attacks.

To decrypt the ciphertext, the receiver uses the same key and the ciphertext is decrypted block by block. Each decrypted block is XORed with the previous ciphertext block to recover the original plaintext.

CBC is a widely used mode of operation in symmetric-key cryptography, which means that the same key is used for both encryption and decryption. However, it is important to note that CBC does not provide authentication or non-repudiation of data. Therefore, it is often used in combination with other cryptographic techniques, such as digital signatures or message authentication codes (MACs), to provide a more comprehensive security solution.

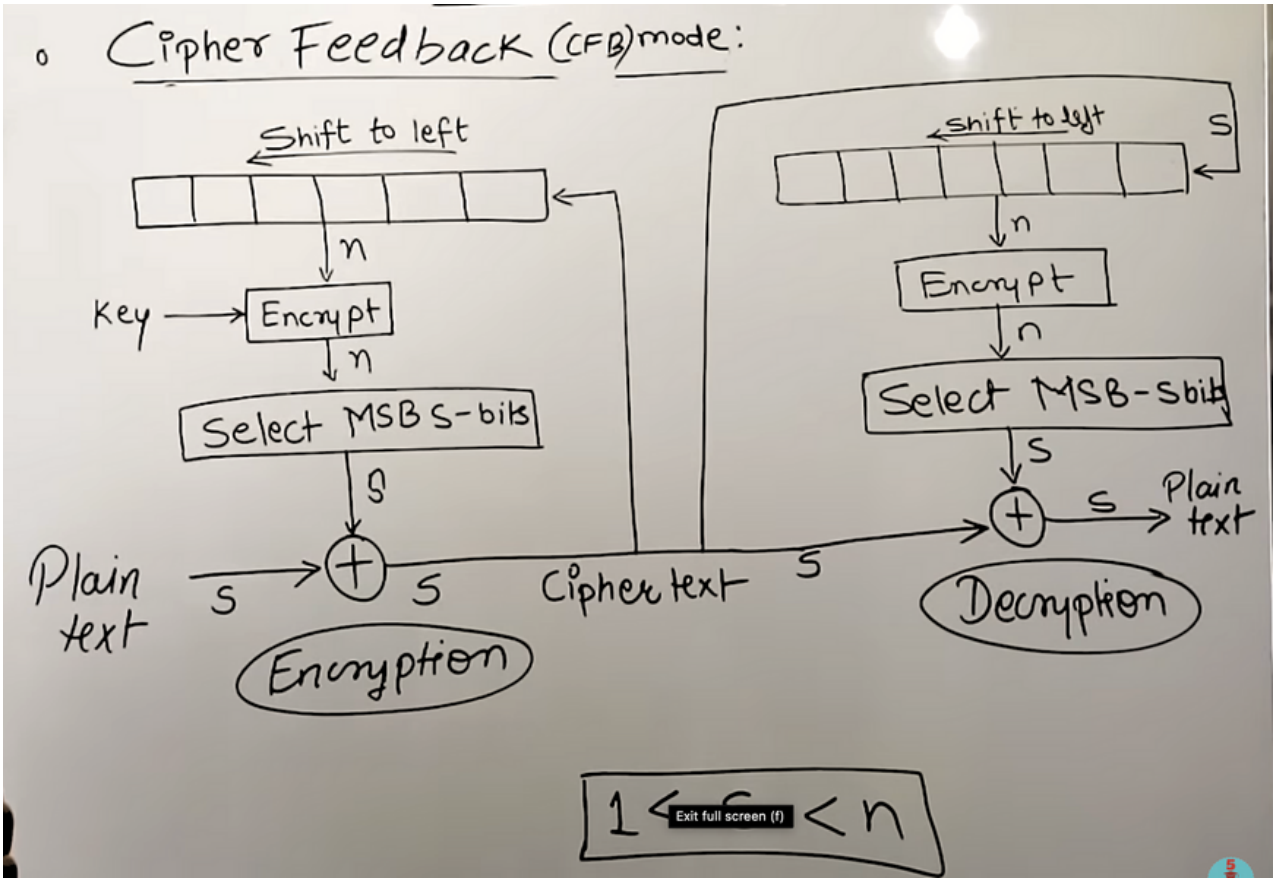


- **Cipher Feedback Mode (CFB)**

CFB (Cipher Feedback) is a method used in information security to encrypt data using symmetric key cryptography.

In CFB mode, encryption is done in blocks, with the output of each block used as input to the next block. The encryption algorithm is run in feedback mode, where the previous ciphertext block is used as input to generate a keystream. This keystream is then combined with the plaintext using XOR to create the ciphertext for the current block.

CFB mode provides confidentiality and message integrity, and can process data efficiently in parallel. However, it is susceptible to error propagation, meaning that an error in one block can affect all subsequent blocks. To prevent this, error detection and correction techniques should be used.



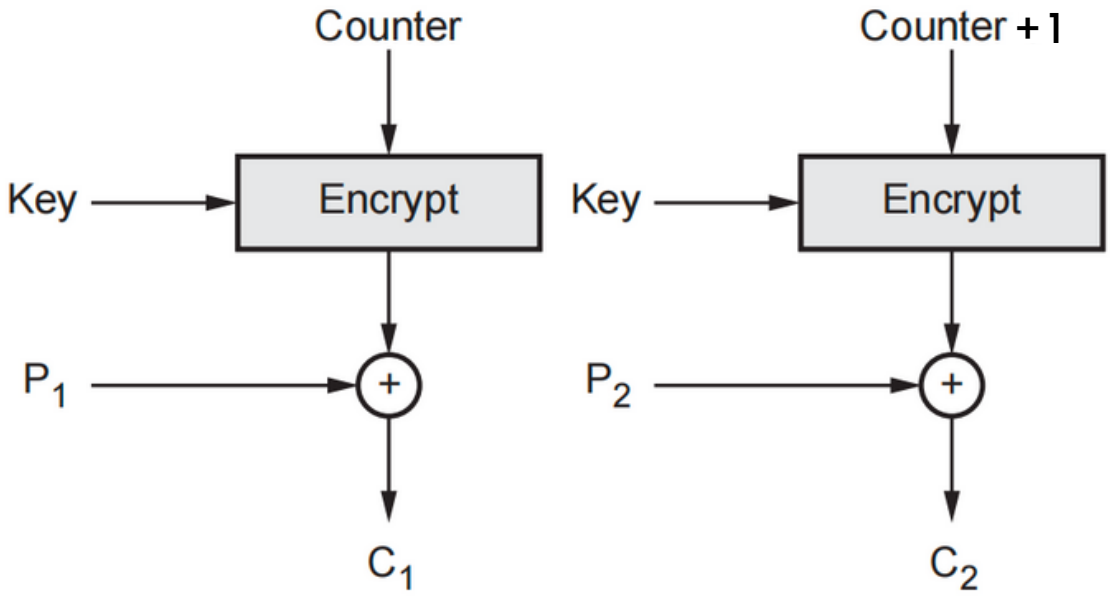
- **Counter mode**

Counter mode is a type of block cipher mode of operation used in cryptography to provide confidentiality for data. It is also known as the "CTR mode" or "encryption counter mode."

In counter mode, a unique counter value is used to generate a stream of pseudorandom numbers, which are then XORed with the plaintext to generate the ciphertext. The counter value is incremented for each block of data that is encrypted, ensuring that each block has a unique keystream.

Here is a step-by-step explanation of how the counter mode works:

1. The encryption algorithm takes as input the key and the initialization vector (IV) to produce a keystream block.
2. The counter value is initialized to a starting value, typically zero.
3. The counter value is combined with the IV to create a unique value for each block of plaintext. This unique value is used as input to the encryption algorithm to generate a keystream block.
4. The keystream block is XORed with the corresponding block of plaintext to produce the ciphertext block.
5. The counter value is incremented by 1, and the process is repeated for the next block of plaintext.



(a) Encryption

DES algorithm

DES is a type of encryption algorithm that uses a secret key to encrypt and decrypt data. It works by breaking data into blocks and applying multiple rounds of encryption using the key. However, DES is now considered outdated and has been replaced by more secure encryption methods.

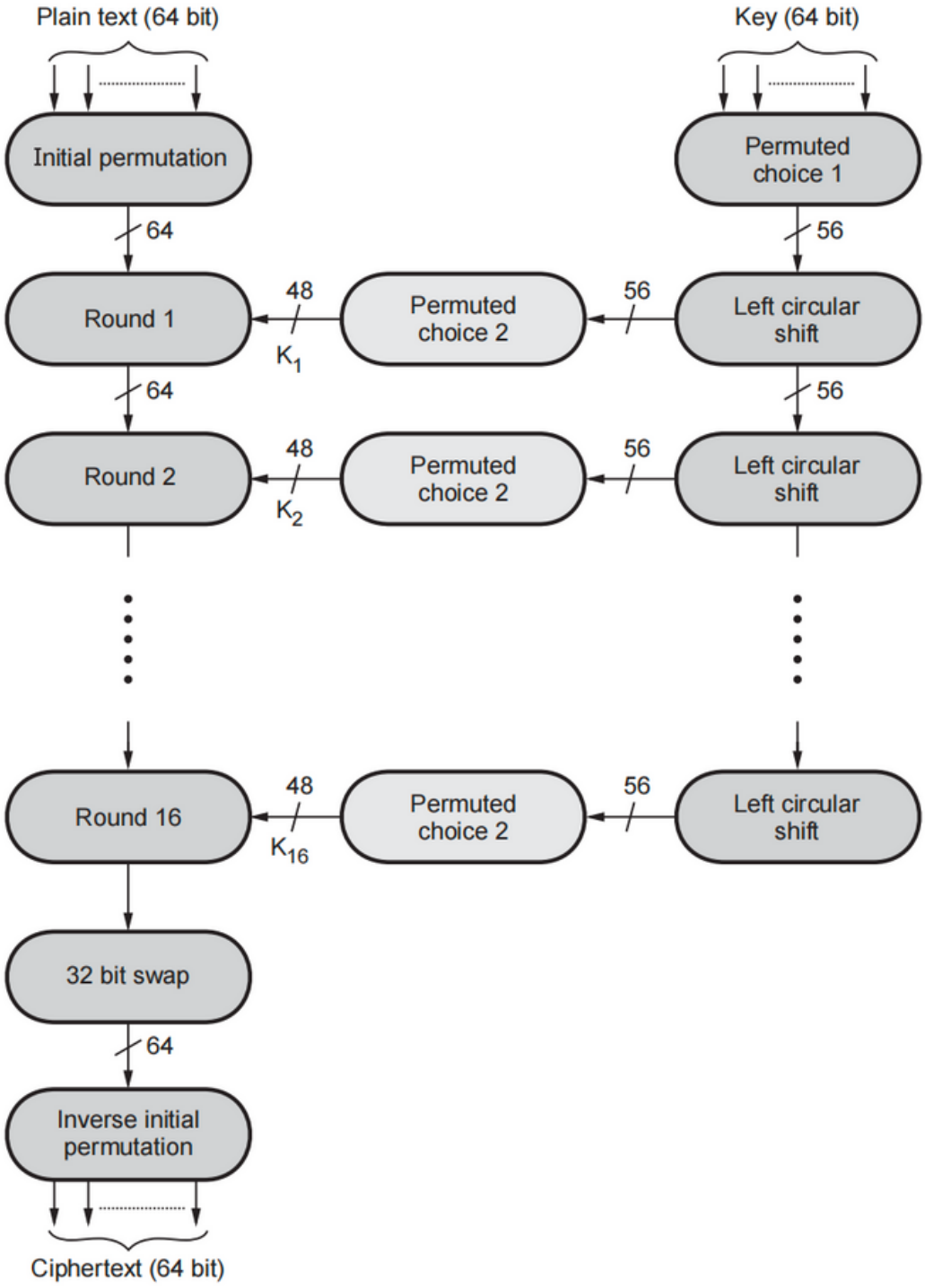


Fig. 2.9.1 DES encryption algorithm

The algorithm consists of the following steps:

1. Initial Permutation (IP): The 64-bit plain text is permuted according to a pre-defined table, resulting in a new 64-bit block.
2. Key Generation: The 64-bit key is used to generate 16 round keys, each of which is 48 bits long. The key is permuted according to another table, and then split into two 28-bit halves. These halves are then rotated left by one or two bits, depending on the round number, and recombined to form a new 56-bit key. This process is repeated 16 times to generate the 16 round keys.
3. Round Function: Each round of DES consists of four main steps. First, the 64-bit block is divided into two 32-bit halves. The right half is expanded to 48 bits by repeating some of its bits. The round key is then XORed with the expanded right half. Next, the result is divided into eight 6-bit blocks, each of which is substituted with a different 4-bit block according to a pre-defined S-box table. The output of the S-boxes is then combined into a 32-bit block. Finally, this block is permuted according to another table to produce a new 32-bit block.
4. Final Permutation (FP): After 16 rounds of the round function, the 64-bit block is divided into two 32-bit halves again, which are swapped. The resulting block is then permuted according to a final table to produce the final cipher text.

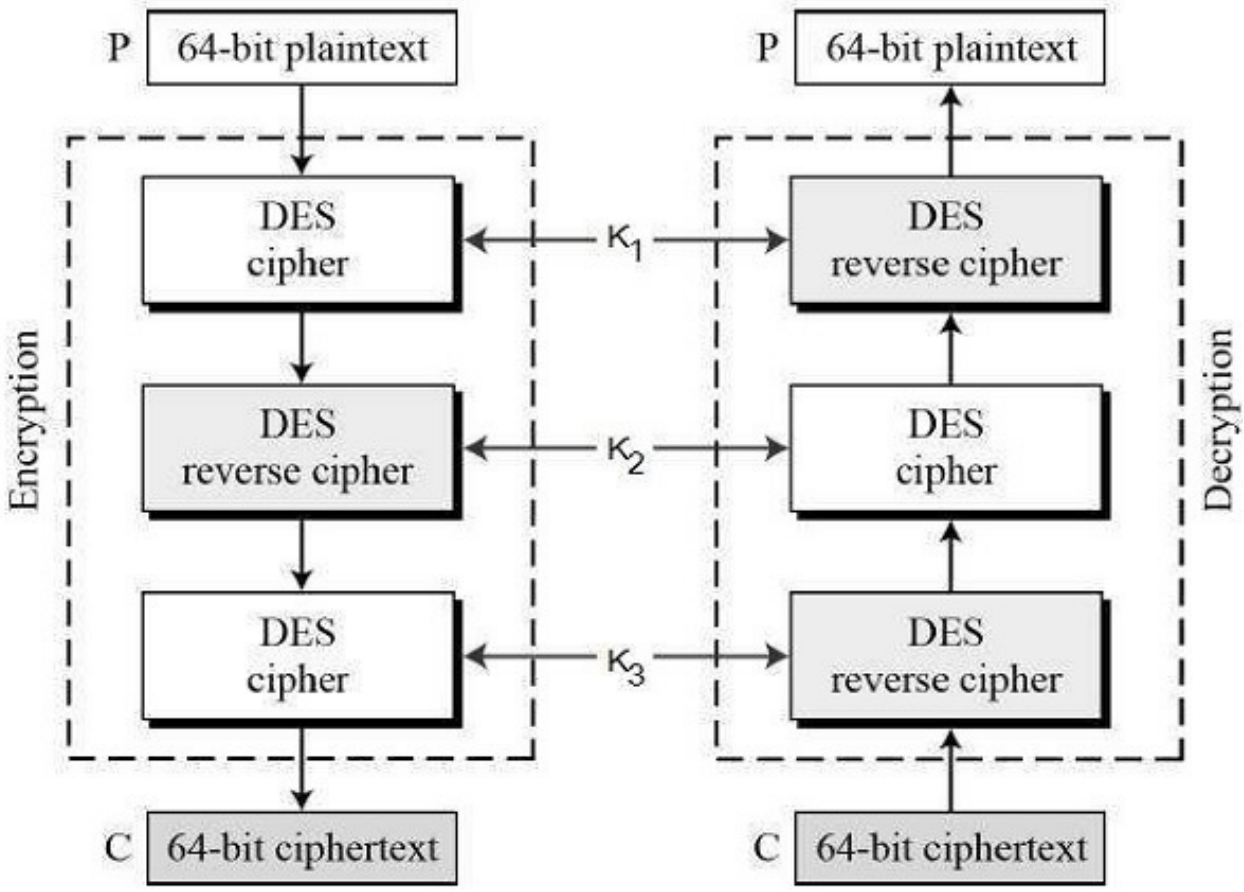
Overall, DES provides good security against attacks, but due to its relatively small key size, it can be susceptible to brute force attacks. To address this issue, the Advanced Encryption Standard (AES) was developed with larger key sizes and improved security.

3DES algorithm

Triple DES (3DES) is a symmetric-key block cipher algorithm that uses a combination of three individual Data Encryption Standard (DES) ciphers to provide increased security.

The 3DES algorithm works by encrypting plaintext in three successive DES operations. Each of the three keys is used to encrypt the data in turn, with the output of each stage being fed as input to the next. This process is also known as the "EDE" (encrypt-decrypt-encrypt) process.

In other words, 3DES encrypts plaintext in three stages using three different keys. The first stage encrypts the plaintext using Key 1, the second stage decrypts the resulting ciphertext using Key 2, and the third stage encrypts the resulting plaintext again using Key 3.



3DES uses a block size of 64 bits, which means that it encrypts 64-bit blocks of plaintext at a time. To ensure that the algorithm can encrypt messages of any length, a technique called padding is used. Padding involves adding extra bits to the plaintext so that it can be divided into 64-bit blocks.

3DES provides a higher level of security than the original DES algorithm, which uses a single 56-bit key. The use of three keys in 3DES increases the key length to 168 bits, making it much more difficult to crack using brute-force methods.

However, 3DES is considered to be relatively slow and inefficient compared to more modern encryption algorithms like Advanced Encryption Standard (AES). As a result, it is no longer widely used in new applications and has been largely replaced by AES.

Working of AES (Advanced Encryption Standard)

AES (Advanced Encryption Standard) is a symmetric-key block cipher algorithm that uses a fixed block size of 128 bits and supports three key sizes: 128-bit, 192-bit, and 256-bit. The algorithm consists of a series of substitution and permutation operations, which are repeated for a fixed number of rounds depending on the key size.

In the case of AES with a 128-bit key, the algorithm performs 10 rounds of substitution and permutation operations. Here is a brief overview of the workings of AES with 10 rounds:

1. Key Expansion: AES generates a series of round keys from the original encryption key. The round keys are used in each round to transform the plaintext.
2. Initial Round: The plaintext is divided into a 4x4 matrix of 16 bytes, called the state. The initial round adds the first round key to the state using XOR.
3. Rounds 1-9: Each round consists of four operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

   - SubBytes: Each byte in the state is replaced with a corresponding byte from a lookup table, called the S-box.
   - ShiftRows: The bytes in each row of the state are shifted cyclically to the left.
   - MixColumns: Each column of the state is multiplied by a fixed matrix, called the MixColumns matrix.
   - AddRoundKey: The round key is added to the state using XOR.

4. Final Round: The final round omits the MixColumns operation and performs only the SubBytes, ShiftRows, and AddRoundKey operations.
5. Output: The resulting state is the ciphertext.

The process of decryption in AES is the reverse of encryption. The same series of operations are performed on the ciphertext using the round keys in reverse order. The decryption process also requires an additional step called InvMixColumns, which is the inverse of the MixColumns operation.

In summary, AES with 10 rounds uses a series of substitution and permutation operations to transform the plaintext into ciphertext. The process includes key expansion, an initial round, 9 rounds of four operations, and a final round. The resulting ciphertext can be decrypted using the same operations in reverse order.

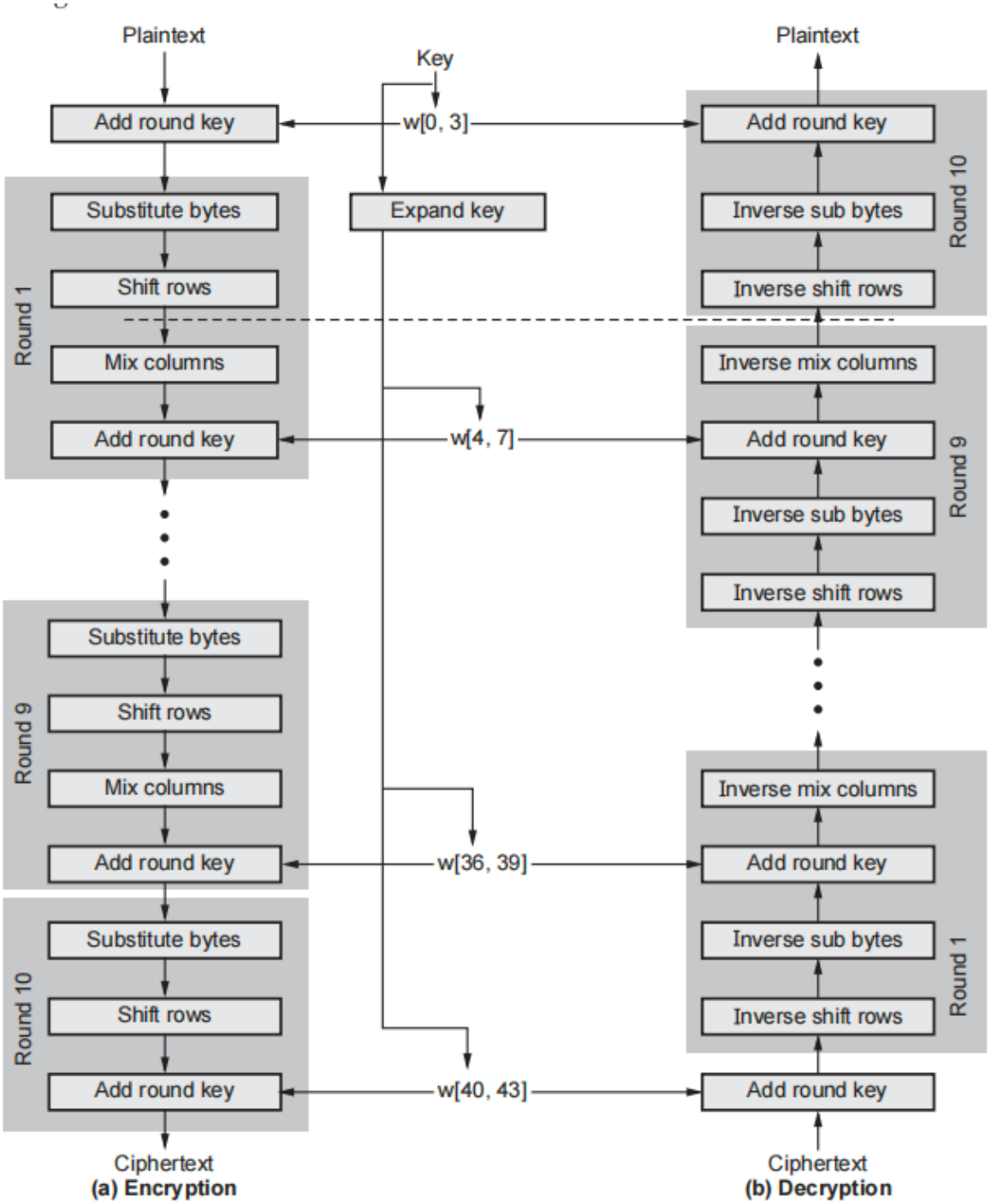


Fig. 2.11.1 AES encryption and decryption