UNIT I

Computer Security concepts:

Computer security is the protection of computer systems and the information they contain.

- The objectives of computer security are to preserve the integrity, availability, and confidentiality of information system resources.
- Information system resources include hardware, software, firmware, data, and telecommunications.
- Computer security is necessary to prevent unauthorized access of information system resources.
- Computer security measures include the use of firewalls, antivirus software, and other security protocols.
- Computer security is important for individuals, organizations, and governments to protect sensitive and confidential information from potential risks and threats.

The five concepts of computer security:

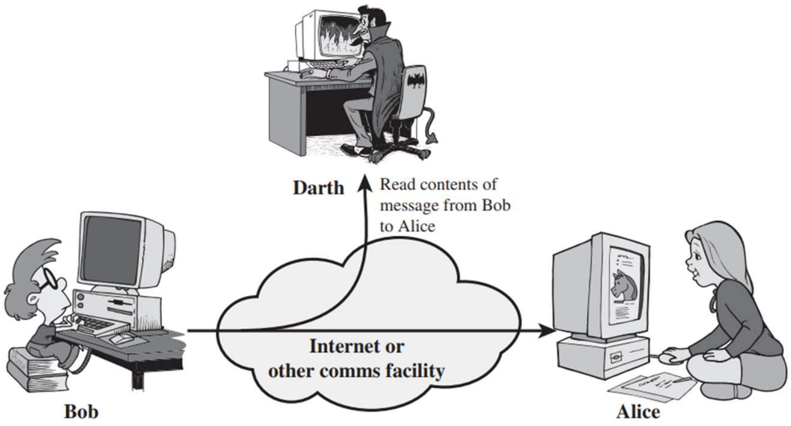
- **Confidentiality:** Keeping information private and only accessible to authorized individuals. Loss of confidentiality occurs when information is disclosed to unauthorized individuals.
- **Integrity:** Ensuring information is accurate, complete, and unmodified, and that it comes from a trusted source. Loss of integrity occurs when information is modified or destroyed without authorization.
- **Availability:** Ensuring that authorized individuals have timely and reliable access to information and systems. Loss of availability occurs when access to information or systems is disrupted.
- **Authenticity:** Verifying that users are who they say they are and that information comes from a trusted source.
- **Accountability:** The ability to track and trace the actions of an individual or a system to identify who is responsible in case of a security breach.

Security Attacks:

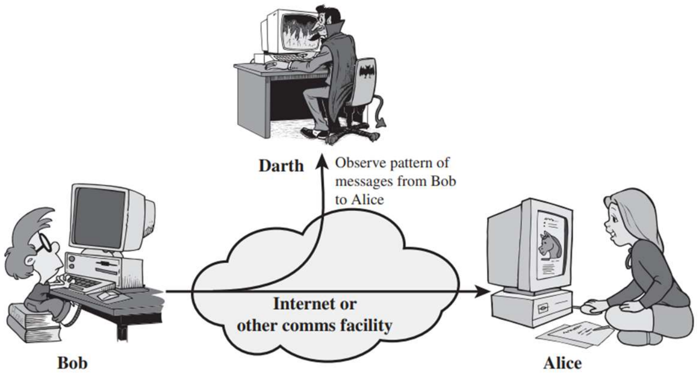
Passive Attacks:

Passive attacks involve monitoring or eavesdropping on information transmissions with the goal of obtaining sensitive or confidential information. There are two types of passive attacks

- **Release of message contents:**


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

- **Traffic analysis:**


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

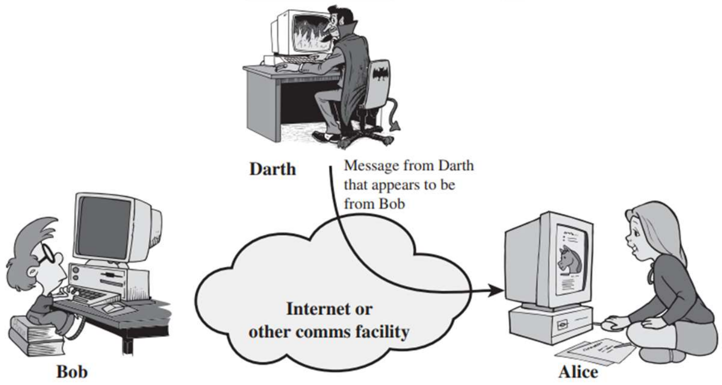
Encryption can prevent the release of message contents, but an attacker may still be able to observe the pattern of messages, which can give them some useful information

Passive attacks are difficult to detect, and prevention through encryption is the primary means of dealing with them.

Active attacks:

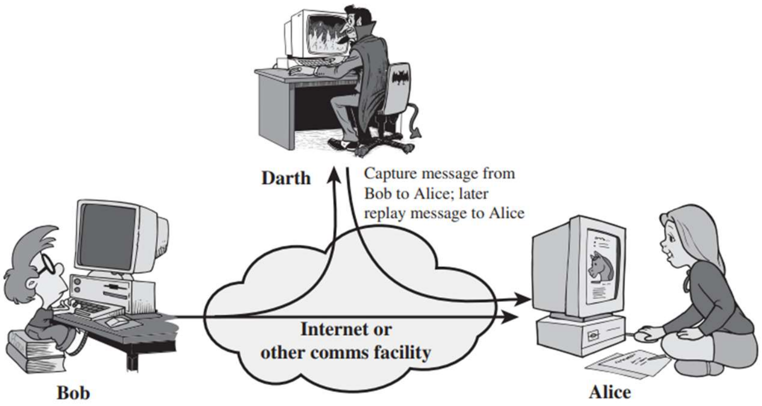
Active attacks involve modifying data or creating false data streams, and can be classified into four categories:

- **Masquerade:**


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

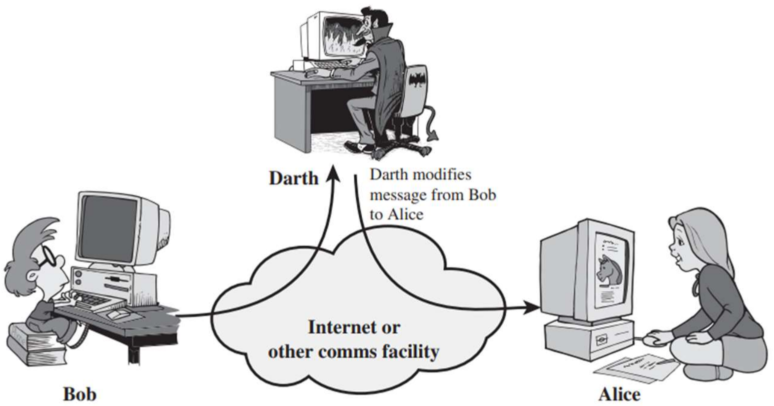
Masquerade is when one entity pretends to be another entity

- **Replay:**


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

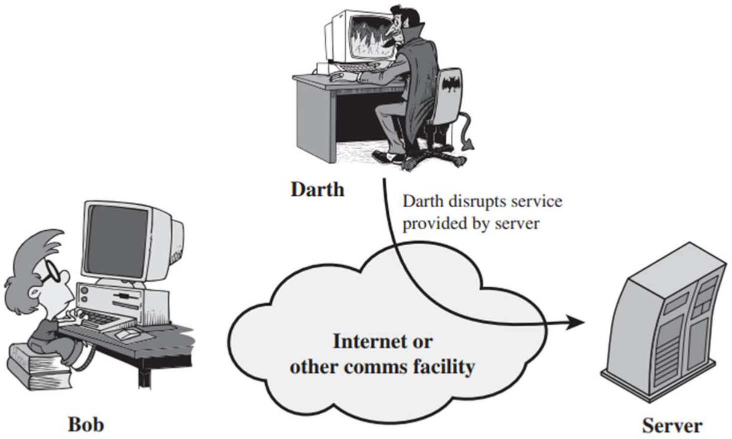
Replay is when captured data is retransmitted to produce an unauthorized effect.

- **Modification of messages:**


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Modification of messages is altering legitimate messages to produce an unauthorized effect.

- **Denial of service:**


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Denial of service inhibits or prevents normal communication use or management, and can have specific targets or disrupt an entire network.

Active attacks are difficult to prevent absolutely due to various vulnerabilities, but detecting them can help recover from their effects and deter future attacks.

Security Services:

Authentication:

The authentication service verifies that a communication is authentic. It has two aspects:

- Verifying the identities of two entities during the connection initiation
- Preventing unauthorized transmission or reception during the connection.

There are two specific authentication services defined in X.800:

- Peer entity authentication, which confirms the identity of a peer entity in a connection
- Data origin authentication, which verifies the source of a data unit but does not protect against duplication or modification of data units.

These services are used for applications such as electronic mail.

Access control:

Access control in network security means controlling and limiting the access to host systems and applications through communication links.

- Before granting access, each entity attempting to gain access must first be identified or authenticated, so that access rights can be customized to the individual.

Data Confidentiality:
Confidentiality in network security is about protecting transmitted data from passive attacks.

- There are several levels of protection, with the broadest service protecting all user data transmitted between two users over a period of time.
- Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message.
- Additionally, confidentiality involves protecting traffic flow from analysis, so attackers cannot observe the source, destination, frequency, length, or other characteristics of the traffic on a communications facility.

Data Integrity:
Integrity refers to the protection of data from active attacks, such as modification or deletion.

- Total stream protection is the most useful and straightforward approach to integrity.
- Connection-oriented integrity service assures that messages are received as sent, without modification, duplication, insertion, reordering, or replays, and also covers destruction of data.
- Connectionless integrity service provides protection against message modification only.
- Integrity service can be with or without recovery. With recovery, automated mechanisms are used to recover from the loss of integrity of data.

Nonrepudiation:
Nonrepudiation ensures that neither the sender nor the receiver can deny sending or receiving a message.

- This means that the sender cannot deny sending a message, and the receiver cannot deny receiving it.
- This helps to establish trust and accountability between parties in a communication.

Availability Service:
Availability is the property of a system being accessible and usable upon demand by an authorized entity.

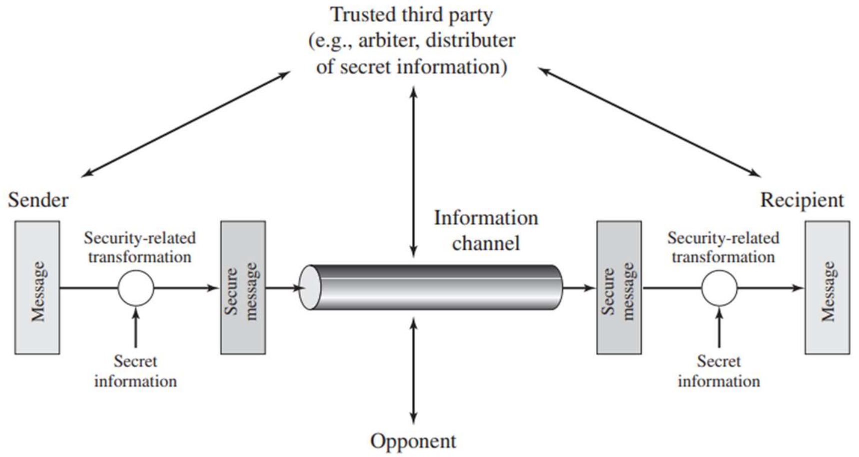
- Attacks can result in loss or reduction of availability, some can be countered with automation, while others require physical action.
- An availability service is one that protects a system to ensure its availability and addresses security concerns raised by denial-of-service attacks.
- It depends on proper management and control of system resources and thus depends on access control service and other security services.

A model for network security:

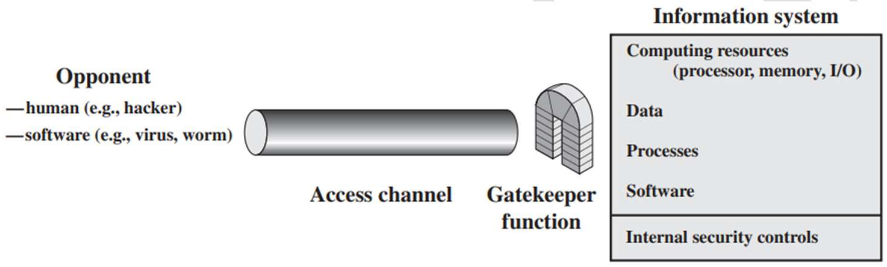
The basic model for secure information transmission involves two parties cooperating to establish a logical information channel and using security-related transformations and secret information to protect the transmission from opponents who may threaten confidentiality or authenticity. Four basic tasks are required:

- Designing the transformation algorithm
- Generating secret information
- Developing methods for sharing the secret information

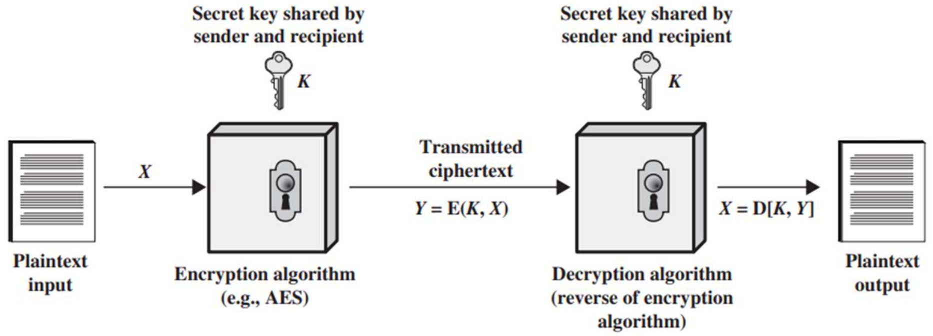
- Specifying a protocol to be used by the two parties.



- Unwanted access to computer systems can be caused by hackers, disgruntled employees, or criminals seeking financial gain, and can be prevented by gatekeeper functions like password-based login procedures and screening logic, as well as internal controls that monitor activity and detect unwanted intruders.



Symmetric cipher model:



- Encryption is a method of transforming a message or data to make it unreadable to unauthorized users.
- The process involves an encryption algorithm, which performs substitutions and transformations on the original message (plaintext), and a secret key that is independent of the plaintext and the algorithm.
- The output of the encryption algorithm is called cipher text, which is unintelligible and depends on both the plaintext and the secret key.
- To read the original message, the receiver uses a decryption algorithm that uses the same secret key to reverse the encryption process and produce the original plaintext.

- For secure use of symmetric encryption, two things are essential: a strong encryption algorithm and keeping the key secret. The algorithm does not need to be secret, but the key must be kept secure.
- Symmetric encryption is widely used because the encryption algorithm does not need to be kept secret, and low-cost chip implementations of data encryption algorithms are available.

Substitution techniques:

Caesar cipher:

The Caesar cipher is one of the simplest and most widely known encryption techniques.

- It is a type of substitution cipher in which each letter in the plaintext is shifted a certain number of positions down the alphabet.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- For encryption we use

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

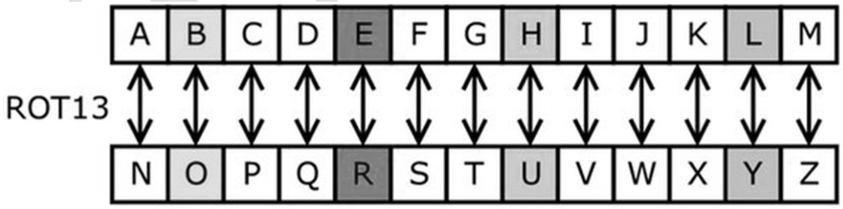
- For decryption we use

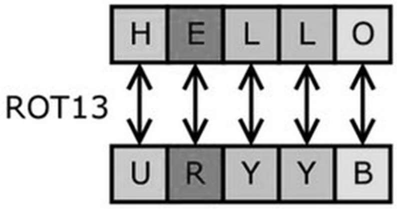
$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$

- It can be easily broken by a brute-force attack, where an attacker tries all possible shift values until the correct one is found.
- Also, since the same shift value is used for every letter in the message, patterns in the plaintext can still be observed in the cipher text.

Monoalphabetic Ciphers:

Monoalphabetic ciphers are a type of substitution cipher where each letter in the plaintext is replaced by a fixed letter in the cipher text.



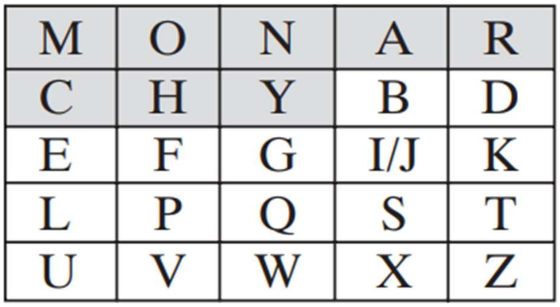


Monoalphabetic ciphers can be broken using several techniques like frequency analysis, and pattern recognition

PlayFair Cipher:

The Playfair cipher is a polygraphic substitution cipher that encrypts pairs of letters instead of single letters.

- The Playfair cipher uses a 5x5 matrix of letters, usually with the letters "I" and "J" combined, to encrypt plaintext
- To use the Playfair cipher, first, the plaintext is divided into pairs of letters. If there is an odd number of letters, the message is padded with a trailing "X"
- Then, each pair of letters is encrypted using the following steps:
    - If both letters are the same, insert an "X" between them.
    - If the letters are different, find their positions in the 5x5 matrix.
    - If the letters are in the same row, replace them with the letters to their right, wrapping around to the left side of the matrix if necessary.
    - If the letters are in the same column, replace them with the letters below them, wrapping around to the top of the matrix if necessary.
    - If the letters are not in the same row or column, replace each letter with the letter in the same row but in the other column of the pair.



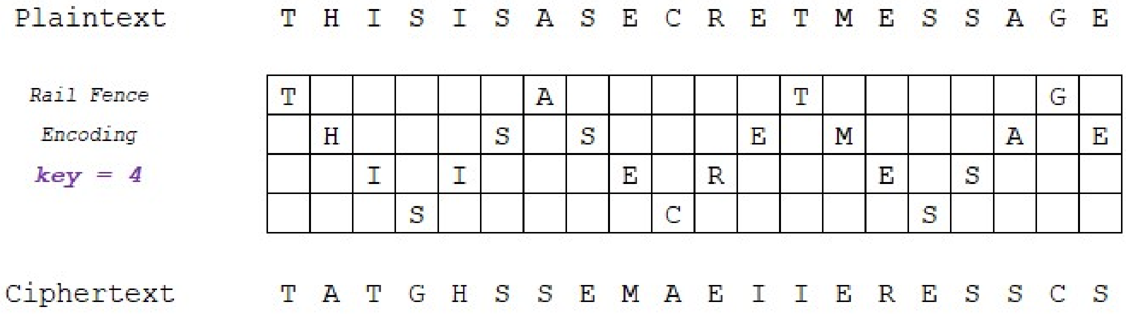
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

It was used as the standard field system by the British Army in World War I and still enjoyed considerable use by the U.S. Army and other Allied forces during World War II.

Transposition techniques:

Rail Fence Cipher:

Rail fence cipher is a transposition cipher that works by writing the plaintext message in a zigzag pattern on a series of horizontal "rails" (lines), and then reading off the message from left to right to create the cipher text.



Plaintext T H I S I S A S E C R E T M E S S A G E

Rail Fence Encoding key = 4

T						A						T						G	
	H				S		S				E		M				A		E
		I		I				E		R				E		S			
			S						C						S				

Ciphertext T A T G H S S E M A E I I E R E S S C S

Columnar transposition Cipher:

Columnar Transposition Cipher is a type of transposition cipher where the order of the letters in the plaintext message is rearranged according to a predetermined key.

- The resulting reordered letters are written out in rows and read column by column to produce the cipher text.
- Columnar Transposition Cipher is a relatively weak encryption method, as it is vulnerable to brute force attacks and frequency analysis attacks.

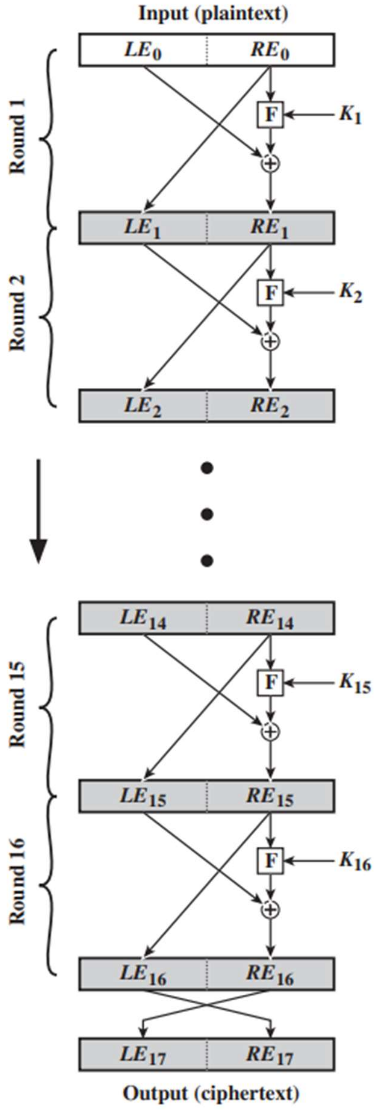
```
Key:           4 3 1 2 5 6 7
Plaintext:     a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
Ciphertext:    TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Traditional block cipher structure:

Feistel Cipher:

Feistel proposed a way to create a strong block cipher by combining multiple simple ciphers in sequence and this approach is called a product cipher.

- Feistel's cipher alternates substitutions and permutations to make it difficult to analyze statistically.
- This is done by using diffusion to break up the statistical structure of the plaintext and confusion to make the relationship between the cipher text and encryption key complex. These concepts have become the cornerstone of modern block cipher design.



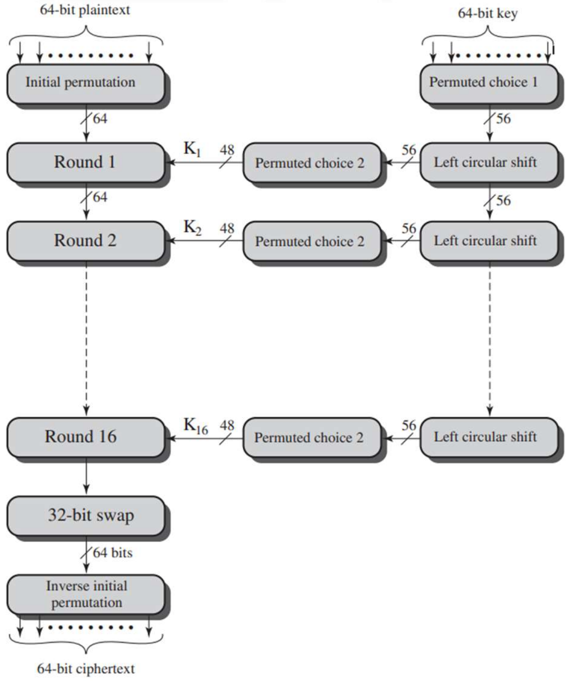
- The main design parameters include block size, key size, number of rounds, sub key generation algorithm, and round function, each of which impacts the security and efficiency of the cipher.
- The encryption algorithm takes a plaintext block and a key as inputs and the plaintext block is divided into two halves.
- The two halves of the data pass through rounds of processing and then combine to produce the cipher text block.
- Each round has a substitution and permutation step.
- The substitution step is performed on the left half of the data using a round function F that takes the right half of the data and a sub key as inputs.
- The permutation step involves interchanging the two halves of the data.
- This structure is known as a substitution-permutation network (SPN) and was proposed by Shannon.
- For the ith iteration of the encryption algorithm,

$$LE_i = RE_{i-1}$$
$$RE_i = LE_{i-1} \oplus \mathrm{F}(RE_{i-1}, K_i)$$

<u>The Data Encryption Standard:</u>

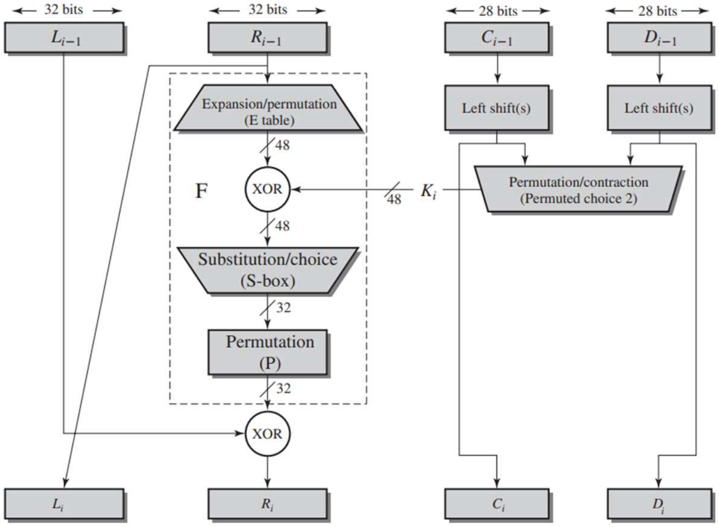
The Data Encryption Standard (DES) is a symmetric key encryption algorithm that uses a block cipher to encrypt and decrypt data.

- DES has been widely used for many years, but its short key length of 56 bits makes it vulnerable to brute force attacks in the modern era of computing.
- DES operates on 64-bit blocks of data and uses a 56-bit key to encrypt and decrypt messages.
- The algorithm is a Feistel cipher that uses 16 rounds of processing to transform the input plaintext into cipher text.



- **Substitution Boxes (S-boxes):** These are lookup tables that take a 6-bit input and produce a 4-bit output. There are 8 S-boxes in DES, and each one is used in every round of the algorithm.

- **Permutation Boxes (P-boxes):** These are fixed permutations that rearrange the bits of the input data. There are two P-boxes in DES: one that is used in every round and another that is used in the key generation process.
- **Round keys:** These are 48-bit keys that are derived from the main key and used in each round of the algorithm.
- **Key schedule:** This is the algorithm used to generate the 16 round keys from the main key and it involves several permutations and bit shifts, as well as a compression function that reduces the size of the key from 56 bits to 48 bits.
- **Feistel network:** This is the structure of the algorithm that performs the substitution, permutation, and XOR operations in each round of the algorithm.



The Strength of DES:

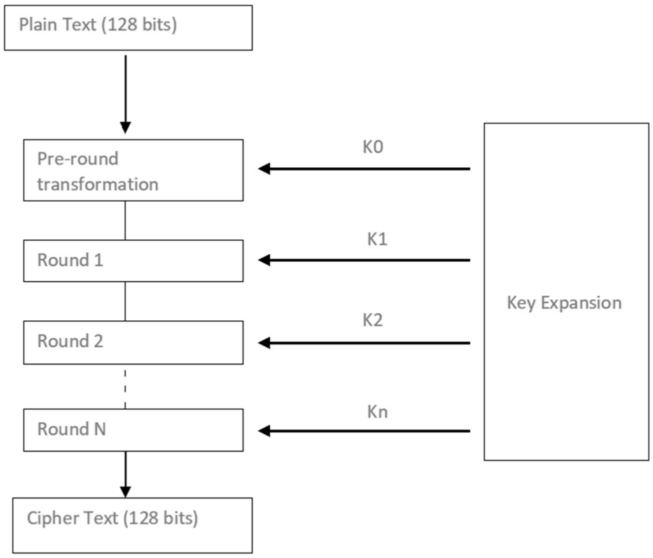
The Data Encryption Standard (DES) is a cryptographic algorithm with a key length of 56 bits, which means there are 72 quadrillion possible keys.

- While brute-force attacks would take thousands of years to break the cipher, in 1998, a special-purpose machine built for less than $250,000 cracked a DES encryption in less than three days.
- The algorithm's eight substitution tables or S-boxes are a concern because they were not publicly designed, leading to suspicions that they may contain weaknesses.
- There have been attempts to use timing attacks to break DES, but it appears to be resistant to this type of attack.
- There are now alternatives to DES, such as AES and triple DES that provide stronger security.

AES Structure:

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm that uses fixed block size of 128 bits and variable key lengths of 128, 192, or 256 bits.

- It consists of a series of transformations that operate on a two-dimensional array of bytes, called the State, which is initially filled with the plaintext.
- The AES algorithm consists of several rounds of these four operations, depending on the key length used i.e. the number of rounds is 10 for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys.



AES transformation functions:

The AES transformation functions are the mathematical operations used in the AES algorithm to transform plaintext into cipher text. There are four main transformation functions used in AES:

- **SubBytes:** This operation replaces each byte in the state with a corresponding byte from a substitution table, called the S-box.
- **ShiftRows:** This operation shifts the bytes in each row of the state by a certain number of bytes i.e. the first row is not shifted, the second row is shifted one byte to the left and so on.
- **MixColumns:** This operation mixes the columns of the state using a fixed matrix multiplication.
- **AddRoundKey:** This operation performs a bitwise exclusive-OR (XOR) between the state and a round key.

AES Key Expansion:

AES key expansion algorithm transforms a 16-byte key into a linear array of 44 words.

- The expanded key is used to provide a round key for each of the 10 rounds of the cipher.
- The first four words of the expanded key are the original key.
- Each added word depends on the immediately preceding word and the word four positions back.
- For every fourth word, a more complex function is used.

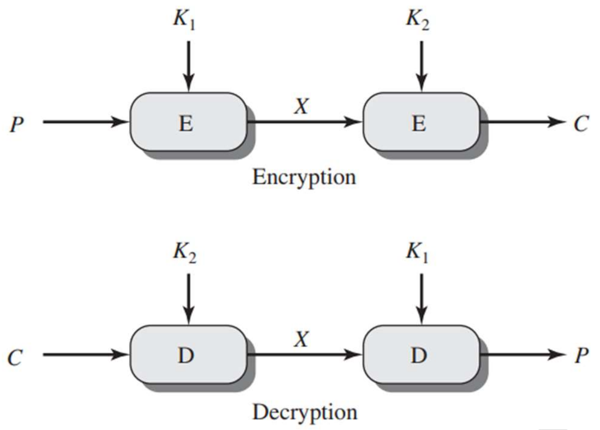
Block Cipher Operation:

Multiple Encryption and Triple DES:

Double DES:

$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

$$P = \mathrm{D}(K_1, \mathrm{D}(K_2, C))$$



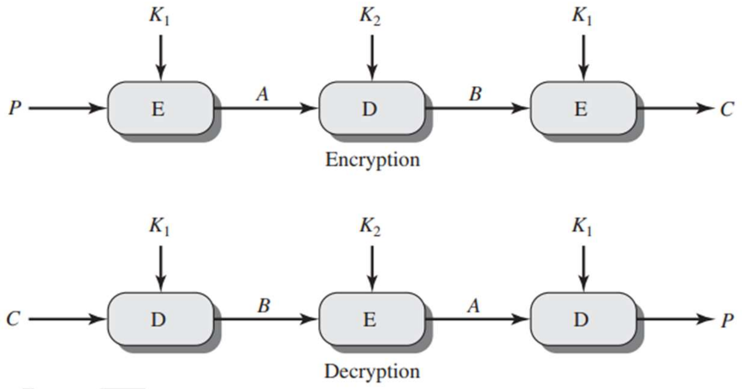
Encryption

Decryption

Triple DES [2keys and 3keys]:

$$C = \mathrm{E}(K_1, \mathrm{D}(K_2, \mathrm{E}(K_1, P)))$$

$$P = \mathrm{D}(K_1, \mathrm{E}(K_2, \mathrm{D}(K_1, C)))$$



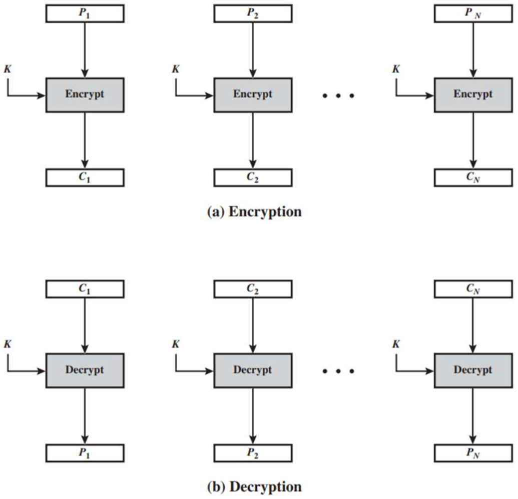
Encryption

Decryption

$$C = \mathrm{E}(K_3, \mathrm{D}(K_2, \mathrm{E}(K_1, P)))$$

Electronic Code Book:

ECB mode is a block cipher mode of operation that operates on fixed-size blocks of plaintext independently and each block of plaintext is encrypted using the same key and the resulting cipher text blocks are concatenated to form the overall cipher text.

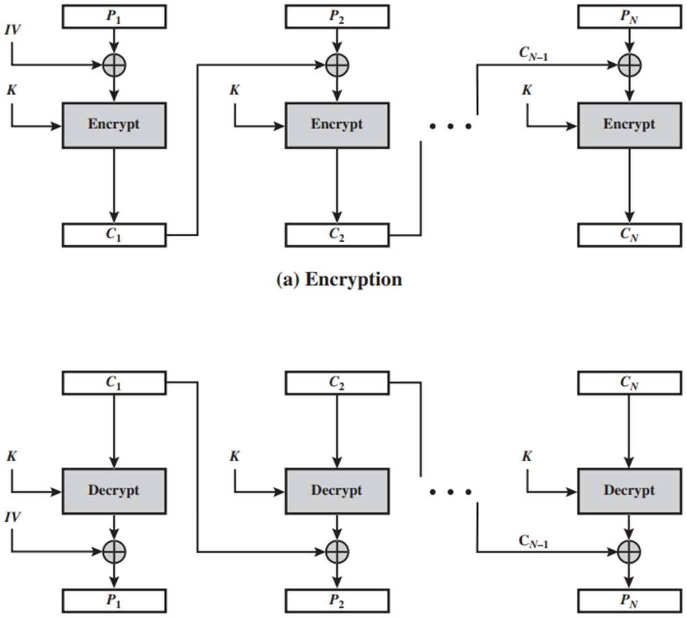


(a) Encryption

(b) Decryption

Cipher Block Chaining Mode:

CBC mode is a block cipher mode that operates on plaintext messages of fixed length, typically 64 or 128 bits and is more secure than ECB mode because it adds an element of randomness to the encryption process.

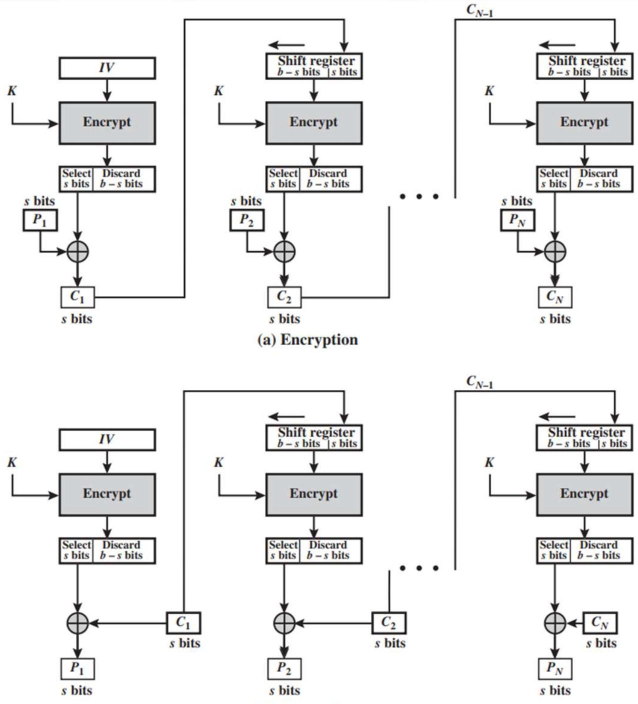


(a) Encryption

(b) Decryption

Cipher Feedback Mode:

CFB mode is a type of encryption mode that operates on blocks of data and allows for encryption of individual bytes or bits of data, making it useful for streaming data such as video or audio.

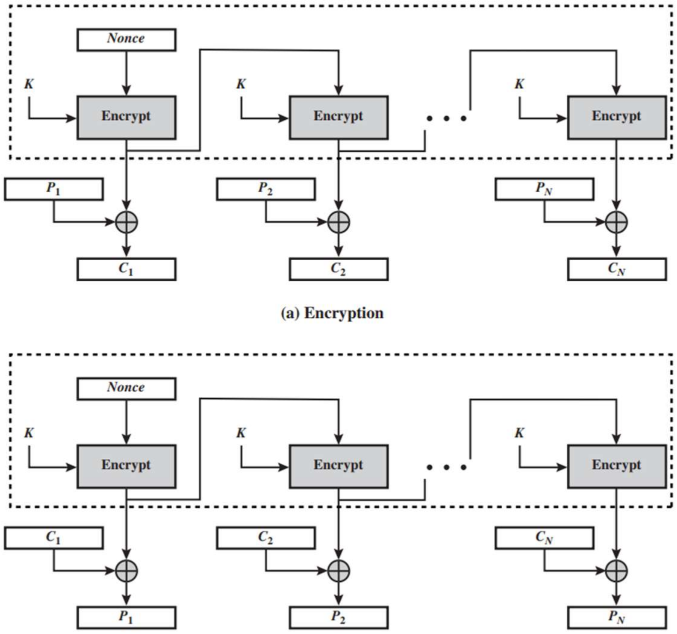


(a) Encryption

(b) Decryption

Output Feedback Mode:

OFB Mode is a type of stream cipher mode that converts a block cipher into a synchronous stream cipher and it is similar to CFB mode, but the keystream blocks are not added to the plaintext to form the cipher text.

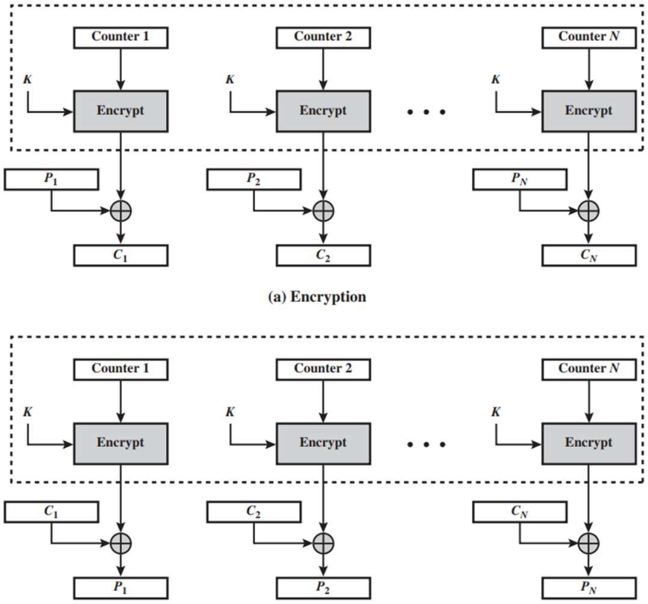


(a) Encryption

(b) Decryption

Counter Mode:

CTR mode is a type of block cipher mode that converts a block cipher into a stream cipher and a counter value is encrypted to produce a stream of pseudorandom bits, which are then XORed with the plaintext to generate the cipher text.



(a) Encryption

(b) Decryption