CYBER SECURITY & CRYPTOGRAPHY (part-1)

techworldthink • February 09, 2022

1. Compare phishing and ransomware attacks.

Phishing is a type of cybersecurity attack during which malicious actors send messages pretending to be a trusted person or entity. Phishing messages manipulate a user, causing them to perform actions like installing a malicious file, clicking a malicious link, or divulging sensitive information such as access credentials. Phishing is the most common type of social engineering, which is a general term describing attempts to manipulate or trick computer users. Social engineering is an increasingly common threat vector used in almost all security incidents. Social engineering attacks, like phishing, are often combined with other threats, such as malware, code injection, and network attacks.

The basic element of a phishing attack is a message, sent by email, social media, or other electronic communication means.

A phisher may use public resources, especially social networks, to collect background information about the personal and work experience of their victim. These sources are used to gather information such as the potential victim's name, job title, and email address, as well as interests and activities. The phisher can then use this information to create a reliable fake message.

Typically, the emails the victim receives appear to come from a known contact or organization. Attacks are carried out through malicious attachments or links to malicious websites. Attackers often set up fake websites, which appear to be owned by a trusted entity like the victim's bank, workplace, or university. Via these websites, attackers attempt to collect private information like usernames and passwords, or payment information.

Some phishing emails can be identified due to poor copywriting and improper use of fonts, logos, and layouts. However, many cybercriminals are becoming more sophisticated at creating authentic-looking messages, and are using professional marketing techniques to test and improve the effectiveness of their emails.

5 Types of Phishing Attacks

Email Phishing

Most phishing attacks are sent via email. Attackers typically register fake domain names that mimic real organizations and send thousands of common requests to victims.

For fake domains, attackers may add or replace characters (e.g. my-bank.com instead of mybank.com), use subdomains (e.g. mybank.host.com) or use the trusted organization's name as the email username (e.g. mybank@host.com).

Many phishing emails use a sense of urgency, or a threat, to cause a user to comply quickly without checking the source or authenticity of the email.

Email phishing messages have one of the following goals:

- Causing the user to click a link to a malicious website, in order to install malware on their device.
- Causing the user to download an infected file and using it to deploy malware
- Causing the user to click a link to a fake website and submit personal data.
- Causing the user to reply and provide personal data.

Spear Phishing

Spear phishing includes malicious emails sent to specific people. The attacker typically already has some or all of the following information about the victim:

- Name
- Place of employment
- Job title
- Email address
- Specific information about their job role

- Trusted colleagues, family members, or other contacts, and samples of their writing

This information helps increase the effectiveness of phishing emails and manipulate victims into performing tasks and activities, such as transferring money.

Whaling

Whaling attacks target senior management and other highly privileged roles. The ultimate goal of whaling is the same as other types of phishing attacks, but the technique is often very subtle. Senior employees commonly have a lot of information in the public domain, and attackers can use this information to craft highly effective attacks.

Typically, these attacks do not use tricks like malicious URLs and fake links. Instead, they leverage highly personalized messages using information they discover in their research about the victim. For example, whaling attackers commonly use bogus tax returns to discover sensitive data about the victim, and use it to craft their attack.

Smishing and Vishing

This is a phishing attack that uses a phone instead of written communication. Smishing involves sending fraudulent SMS messages, while vishing involves phone conversations.

In a typical voice phishing scam, an attacker pretends to be a scam investigator for a credit card company or bank, informing victims that their account has been breached. Criminals then ask the victim to provide payment card information, supposedly to verify their identity or transfer money to a secure account (which is really the attacker's).

Vishing scams may also involve automated phone calls pretending to be from a trusted entity, asking the victim to type personal details using their phone keypad.

Angler Phishing

These attacks use fake social media accounts belonging to well known organizations. The attacker uses an account handle that mimics a legitimate organization (e.g. “@pizzahutcustomercare”) and uses the same profile picture as the real company account.

Attackers take advantage of consumers’ tendency to make complaints and request assistance from brands using social media channels. However, instead of contacting the real brand, the consumer contacts the attacker’s fake social account.

When attackers receive such a request, they might ask the customer to provide personal information so that they can identify the problem and respond appropriately. In other cases, the attacker provides a link to a fake customer support page, which is actually a malicious website.

2.Ransomware

is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn’t pay in time, the data is gone forever or the ransom increases.

Ransomware is malware that employs encryption to hold a victim’s information at ransom. A user or organization’s critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.

2. What is OSI security architecture?

The OSI security architecture helps the managers responsible for the security of an organization in defining the requirements for security. The OSI security architecture was introduced as an ‘international standard’ which let the computer and communication vendor develop the products that have security features based on this architecture.

The OSI security architecture has a structure definition of services and mechanism for providing security to the organization’s information.

OSI Security Architecture Defines:

1. Security Attacks
2. Security Mechanism
3. Security Services

Security Attacks

Security attacks can be defined as an action that risks the security of information owned by the company.

1.Passive Attack

In a passive attack, the attacker monitors or eavesdrops the transmission between and sender and receiver and the attacker try to retrieve the information being transmitted. In passive attack neither the sender nor the receiver is aware of the attack as the attacker only retrieve the message, he doesn’t perform any alteration to the captured message. The message is sent and received in the normal fashion.Therefore, is more difficult to identify the passive attack. Though identification of passive attack is tedious, you can definitely implement encryption in order to prevent the success of this attack which means even if the attack happens the attacker is unable to extract the information.

The passive attack is further classified into two types.

Release of message content

- The release of the message content is a kind of attack where the attacker listens to the telephone conversation, tracks electronic mail or the transferred file to retrieve the confidential message being transmitted. The opponent is quite interested in the content of the released message.

Traffic analysis

- To protect the released message content the organization may apply a mask over the content of the message so that even if the attacker captures the message, he would not be able to understand the message. This technique of masking the released message is termed as encryption.
- In traffic analysis passive attack, the attacker monitors the pattern, length and frequency of the released message to guess the original message.

2.Active Attack

We have seen that in the passive attack the attacker does not alter the message, but in the active attack the attacker alters, modify the transmitted message by creating a false data stream.It is quite difficult to prevent the active attack instead the goal is to identify the source of active attack and apply a recovery measure.

The active attack is further classified into four types

- Masquerade

In masquerade active attack, the attacker pretends to be the sender.

- Replay

In the replay, the message is captured in a passive way and is retransmitted to produce an unauthorized effect.

- Modification of message

Modification of message means some data stream of the message is altered or modified to create an unauthorized effect.

- Denial of services

The attacker suppresses all the messages directed to a particular receiver by overloading the network to degrade the network performance

Security SERVICES

The security mechanism is an entire process that is specifically designed to identify the attack and develops a strategy to recover or prevent the attack.

- Authentication: It assures that the entity involves in the communication is the one it is claiming for.
- Access Control: This service assures that only the authorized entities are accessing the resources and prevents unauthorized access.
- Data Confidentiality: This service manages to maintain the confidentiality of data by preventing the exposure of the message content to the attacker.
- Data Integrity: This service makes it sure that the data received at the receiver end is from an authorized entity.
- Nonrepudiation: This service restricts the sending and receiving entity from denying the transmitted message.

In all the OSI security architecture the things that need to be concentrated are security attack, service and mechanism to prevent the risk to the security of information of an organization.

3. SECURITY MECHANISMS

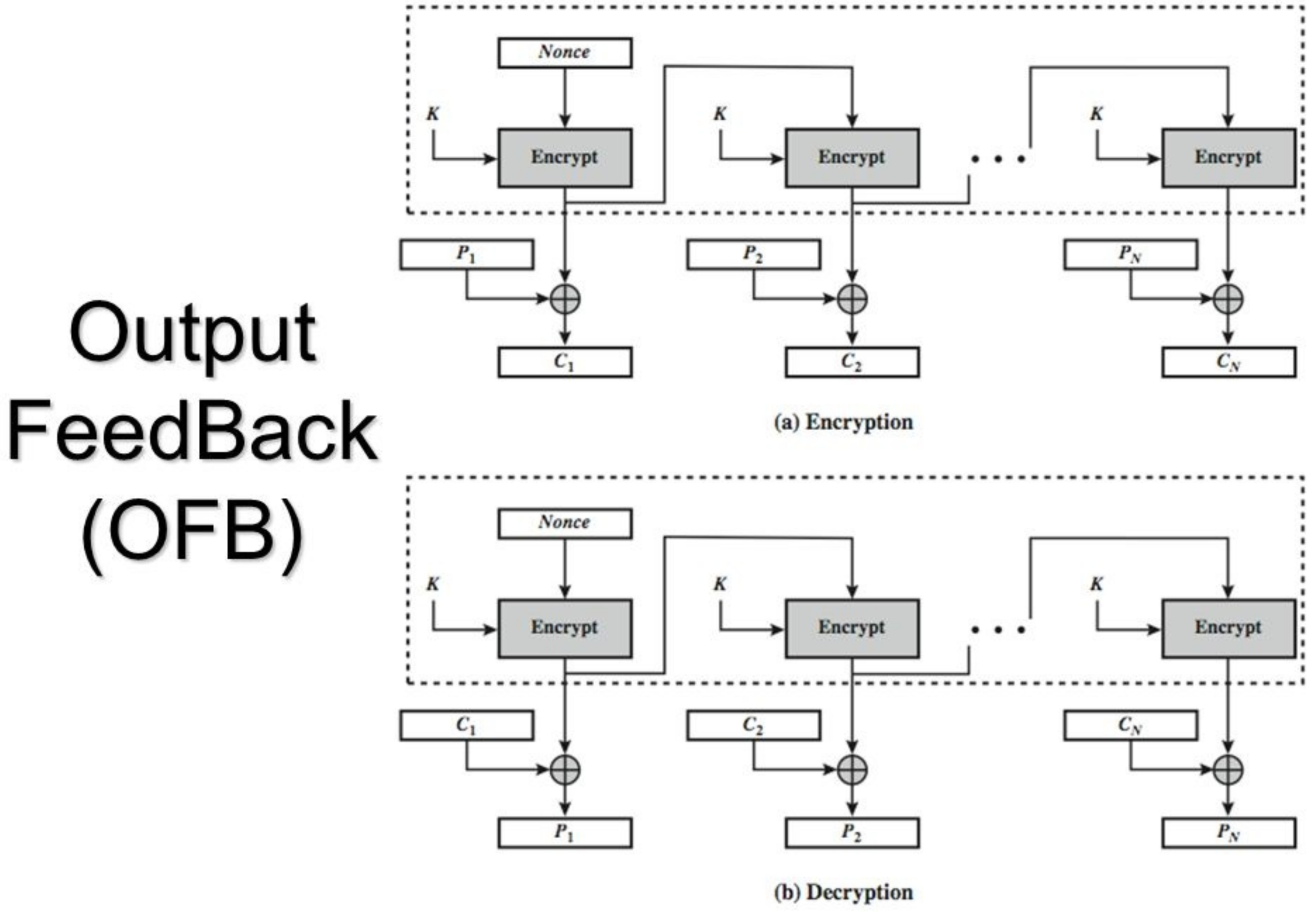
One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are:

Encipherment

Digital Signature

Access Control

3. List out the advantages and disadvantages of Output Feed Back mode



(a) Encryption

(b) Decryption

OFB (short for output feedback) is an AES block cipher mode similar to the CFB mode. What mainly differs from CFB is that the OFB mode relies on XOR-ing plaintext and ciphertext blocks with expanded versions of the initialization vector.

This process can be seen as a one-time pad and the expanded vectors as *pad vectors*. The following formula depicts how a sequence of pad vectors is created:

Vi = EK(Vi-1)

> *where EK denotes the block encryption algorithm using key K and Vi and Vi-1 are adjacent vectors.Note: In the formula above, we are assuming Vo to be the initialization vector.*

Once the sequence of pad vectors is generated, encryption with the OFB mode can be carried out using the following formula:

Ci = Vi ⊕ Bi

Decryption is carried out in a similar way:

Bi = Vi ⊕ Ci

> *Note: Like the CFB mode, OFB also makes use of a single encryption algorithm for both encryption and decryption.*

Advantages and disadvantages of using the OFB mode

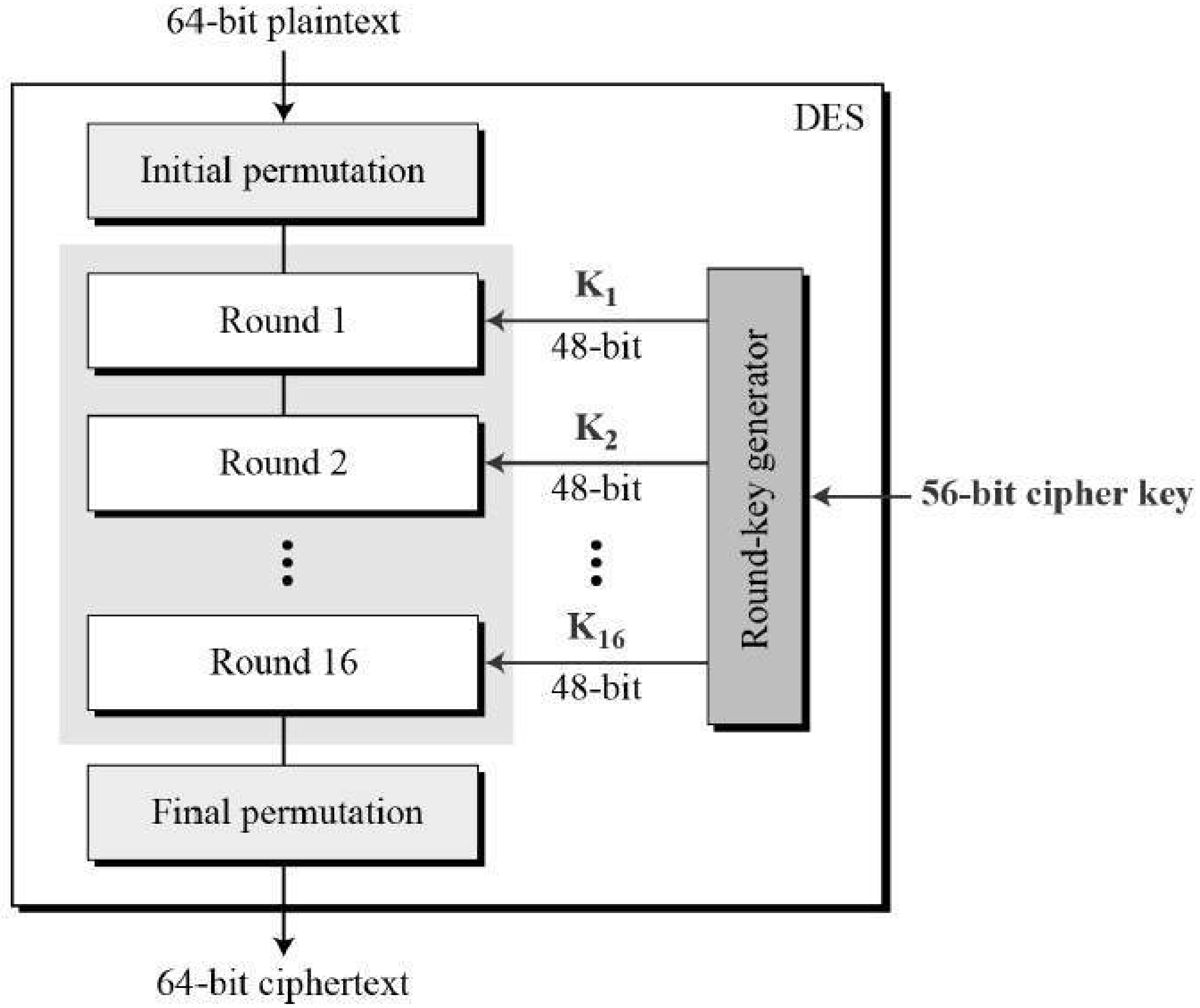
Since blocks are independent of one another using the OFB mode, both encryption and decryption of blocks can be done in parallel once the pad vectors have been generated. The lack of interdependency also means that the OFB mode is tolerant to the loss in blocks. The main advantage of the OFB method is that bit errors in transmission do not propagate in the encryption.

A significant drawback of the OFB is that repeatedly encrypting the initialization vector may produce the same state that has occurred before. This is an unlikely situation, but in such a case, the plaintext will start to be encrypted by the same data as it was previously. The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than is CFB in the modes of operation.

4. Explain round functions used in DES.

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −



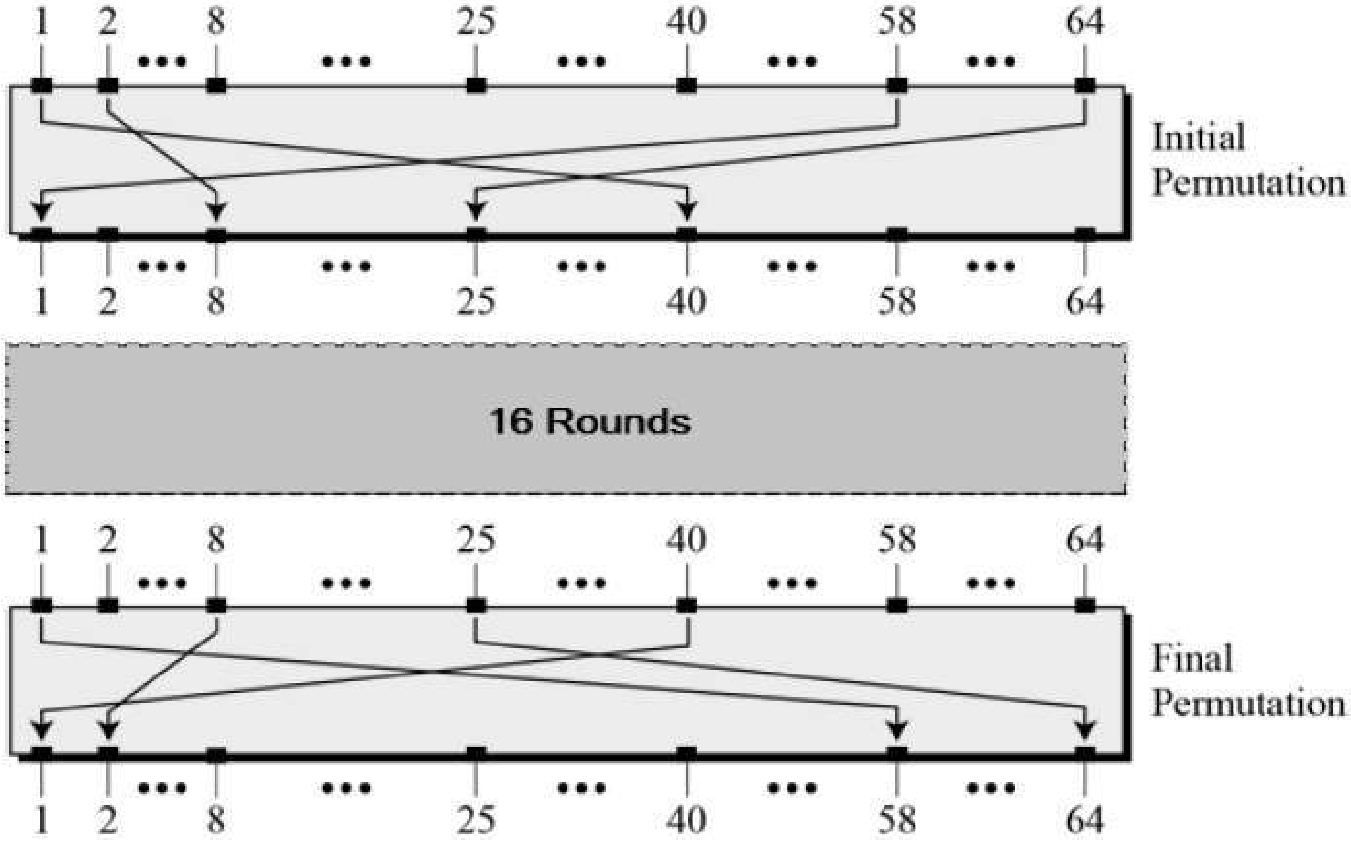
Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule

- Any additional processing − Initial and final permutation

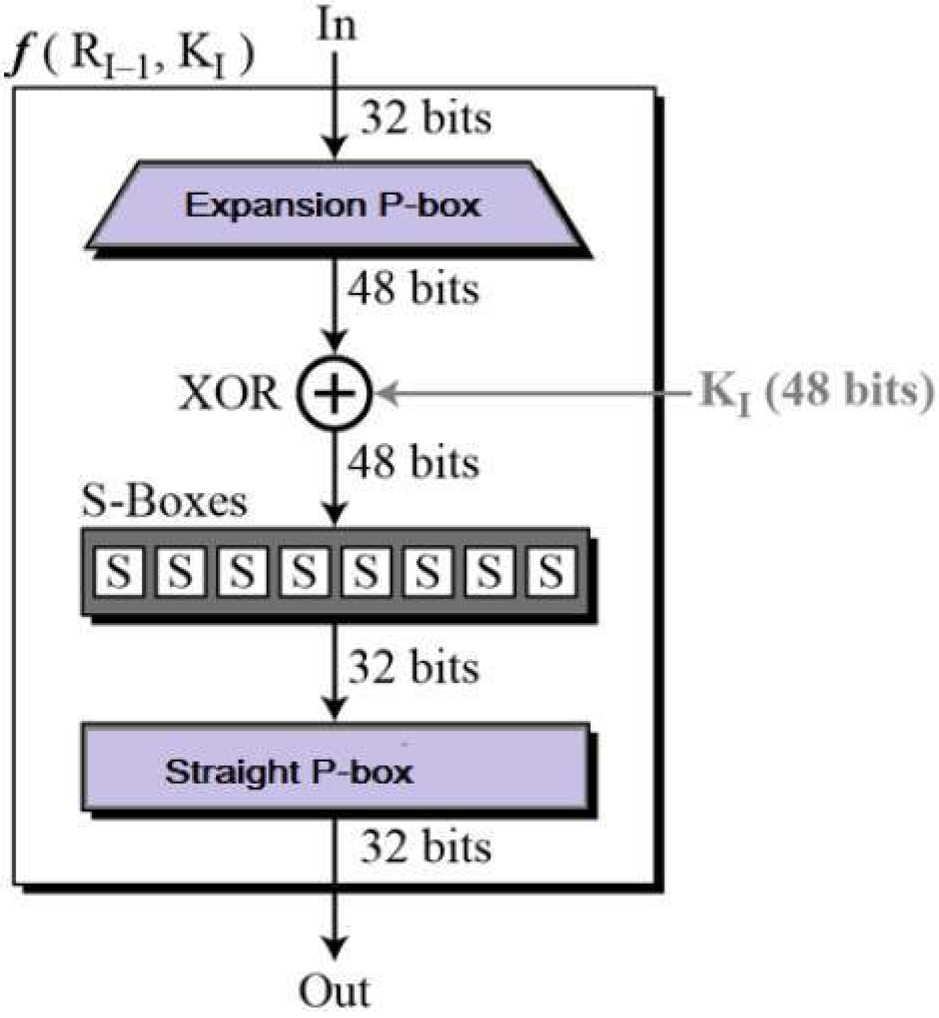
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows −

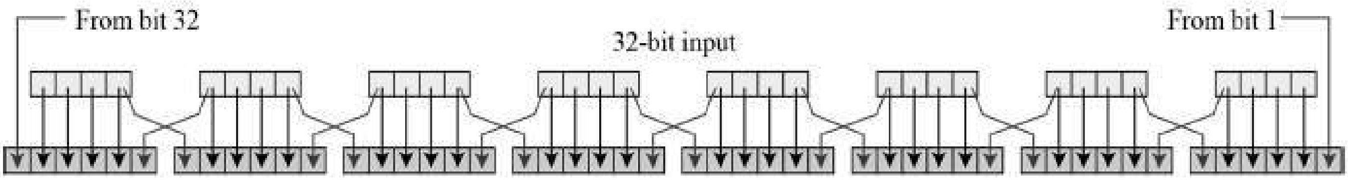


Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



- Expansion Permutation Box − Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −



- XOR (Whitener). − After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- Substitution Boxes. − The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.
- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.
- Straight Permutation − The 32 bit output of S-boxes is then subjected to the straight permutation

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- Avalanche effect − A small change in plaintext results in the very great change in the ciphertext.
- Completeness − Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.