Unit 6

Security

Introduction

- Security is concerned with the protection of systems, networks, applications, and information.
- The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity.

Types of Security

- **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.
- **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.

- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.
- **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
- **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
- **User Education:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

Network Security

- Network Security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses government agencies and individuals.

Need of Security

- Protect vital information while still allowing access to those who need it. Eg. Trade secrets, medical records etc.
- Provide authentication and access control for resources.
- Guarantee availability of resources.

Key principles of security

- Confidentiality
- Authentication
- Integrity
- Non-Repudiation

Authentication

- Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

Integrity

- Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

Non-Repudiation

- Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

Availability

- The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

Security Goals

- Confidentiality
- Integrity
- Availability

Threats & Vulnerability

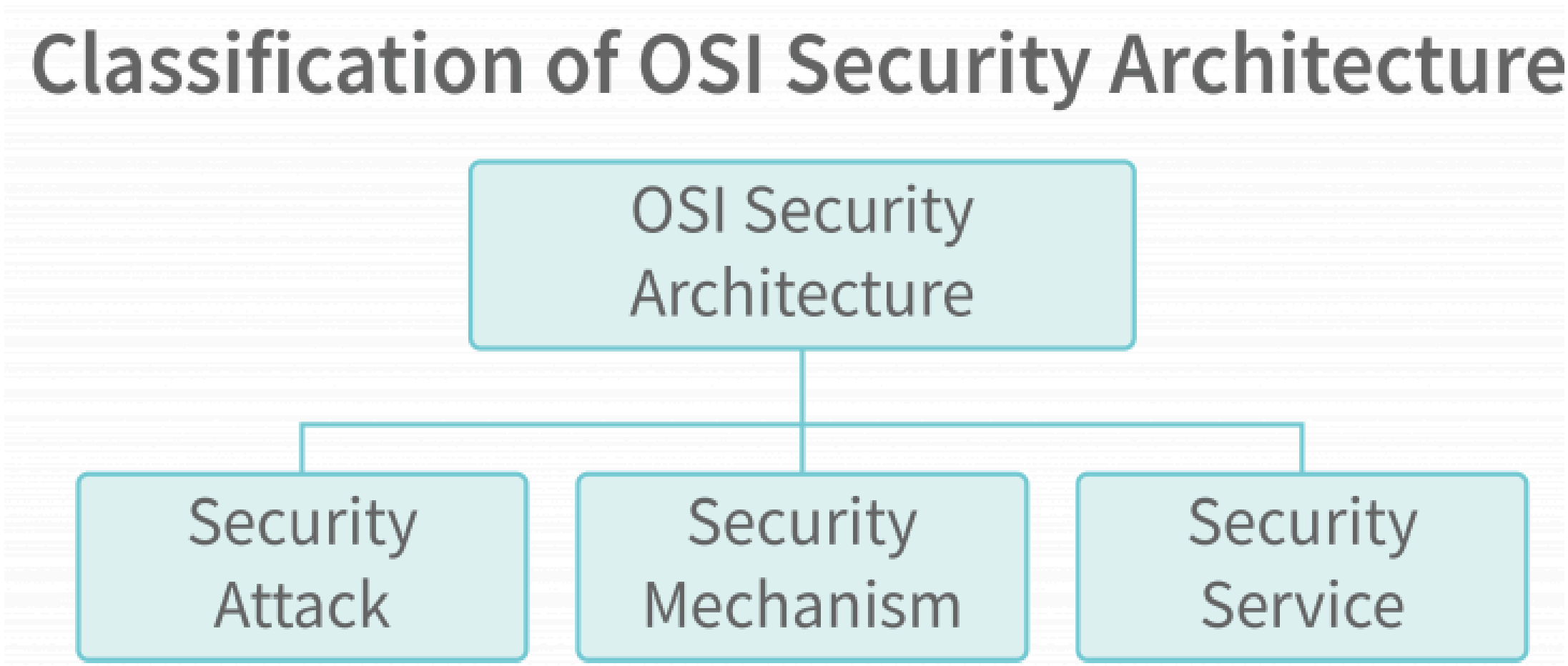
- Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
- **Threat** can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

OSI Security Model

- The data travels from the Application layer of the sender to its Physical layer and then from the Physical Layer of the sender to the Physical layer of the receiver. So, in between, this data can be modified, stolen, or just being read by an attacker for some future use. This is not safe as the data can be used for criminal activities as well and in any big organization, the data being stolen/modified can be of major concern.
- So, the OSI Security model provides a standard for the security of data by identifying the attacks, security services, and security mechanisms and also identifies which security services should be implemented in which layer of the OSI model and what security mechanisms should be used to do so.

OSI Security Architecture

- The OSI Security model identifies the attacks on a system (data) and also identifies various security services and the mechanisms to implement those services in various layers of the OSI model.



Security Attacks

- A security attack means any action that puts the data or overall security of the system at risk. An attack might be successful or unsuccessful. In case of a successful attack, the attacker can complete his/her motive of breaking the security of the system in any way he/she wants to. In case of an unsuccessful attack, the system remains secured and no harm to the security is done. There are majorly 2 types of attacks: active attacks and passive attacks.

Network Attack

- A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity. There are two main types of network attacks:
  - **Passive:** Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
  - **Active:** Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.

Types of attacks

- **Endpoint attacks**— gaining unauthorized access to user devices, servers or other endpoints, typically compromising them by infecting them with malware.
- **Malware attacks**— infecting IT resources with malware, allowing attackers to compromise systems, steal data and do damage. These also include ransomware attacks.
- **Vulnerabilities, exploits and attacks**— exploiting vulnerabilities in software used in the organization, to gain unauthorized access, compromise or sabotage systems.
- **Advanced persistent threats**— these are complex multilayered threats, which include network attacks but also other attack types.

Passive Attack

- A passive attack is a kind of attack in which the data that is sent from the sender to the receiver is read by the attacker in the middle of the transmission.
- However, the main point to note here is that the passive attack is the attack in which the attacker does not modify or corrupt the data.
- No changes are made to the data. The attacker just observes the data sent to the receiver from the sender and can know a lot of information about the sender and the receiver just by observing the communication between them.

There are 2 types of passive attacks.

- **Traffic Analysis:** As the name suggests, this attack focuses on the amount or volume of data sent between the sender and the reciever.**1.** The attacker can predict a lot of information about the sender and the receiver by knowing the amount of data sent. For example, if a lot of data is being sent from the sender to the receiver, it is assumed as there is an emergency, or a task is happening on an urgent basis. If less data is shared between the sender and the receiver, it is assumed that there is a lack of communication and so on.
- **Eavesdropping:** In this kind of attack, the attacker reads the communication that happens between the sender and the receiver and then can use this information for many things. For instance, an attacker can use the information to know about the financial details of the user. Also, this can be used for criminal activities as the attacker can send a lot of personal information to a criminal. The difference between eavesdropping and traffic analysis is that in traffic analysis, the attacker does not even read the data. He/she is just focused on the volume of the data. Whereas on the other hand, in eavesdropping, the focus is on the actual data being exchanged between the sender and the receiver.

Active Attack

- In an active attack, the focus of the attacker is to modify the data that is being exchanged between the sender and the receiver. The most dangerous thing about this attack is that most of the time, the sender and the receiver do not even know that an attack has happened. There are several types of active attacks.
- Replay
- Masquerade:
- Denial of Service (DOS)
- Distributed Denial of Service (DDOS)

Security Attacks

- Attacks on confidentiality:

1. Snooping
2. Traffic analysis

- Attacks on integrity:

1. Modification
2. Replaying
3. Repudiation
4. Masquerading

- Attacks on Availability:

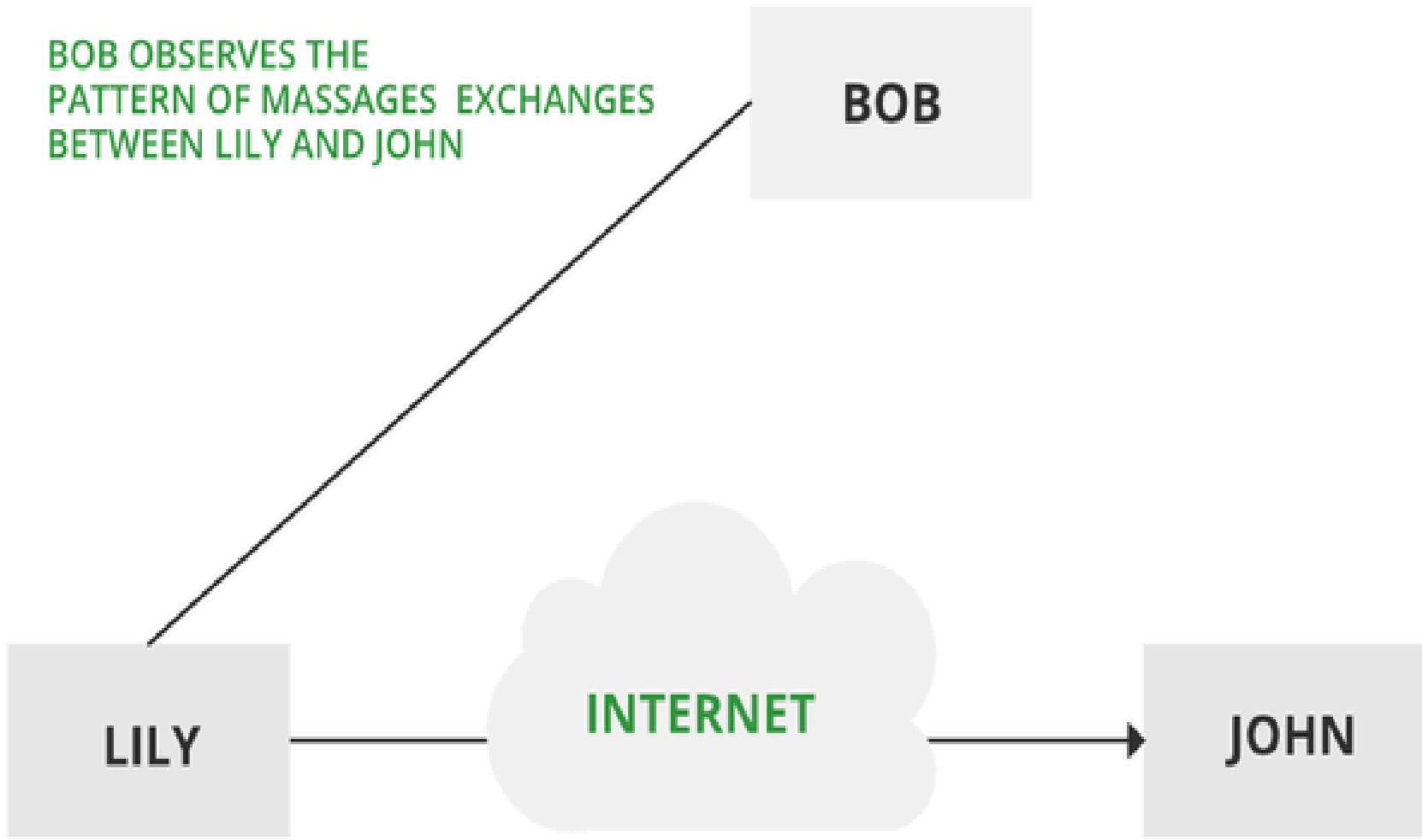
1. Denial of Service

Snooping

- Snooping in network security is a technique in which criminals get unauthorized access to another person's data or company's data. Snooping in network security includes casual observance of an email that appears on the user's computer screen. Mo re sophisticated Snooping in network security uses software programs to remotely monitor activity on a computer/network device.
- Snooping in network security leads to loss of privacy of several kinds of information that should be private for a computer network. They may be one or all the following:
- Passwords
- Financial details
- Private data
- Low-level internet protocol information

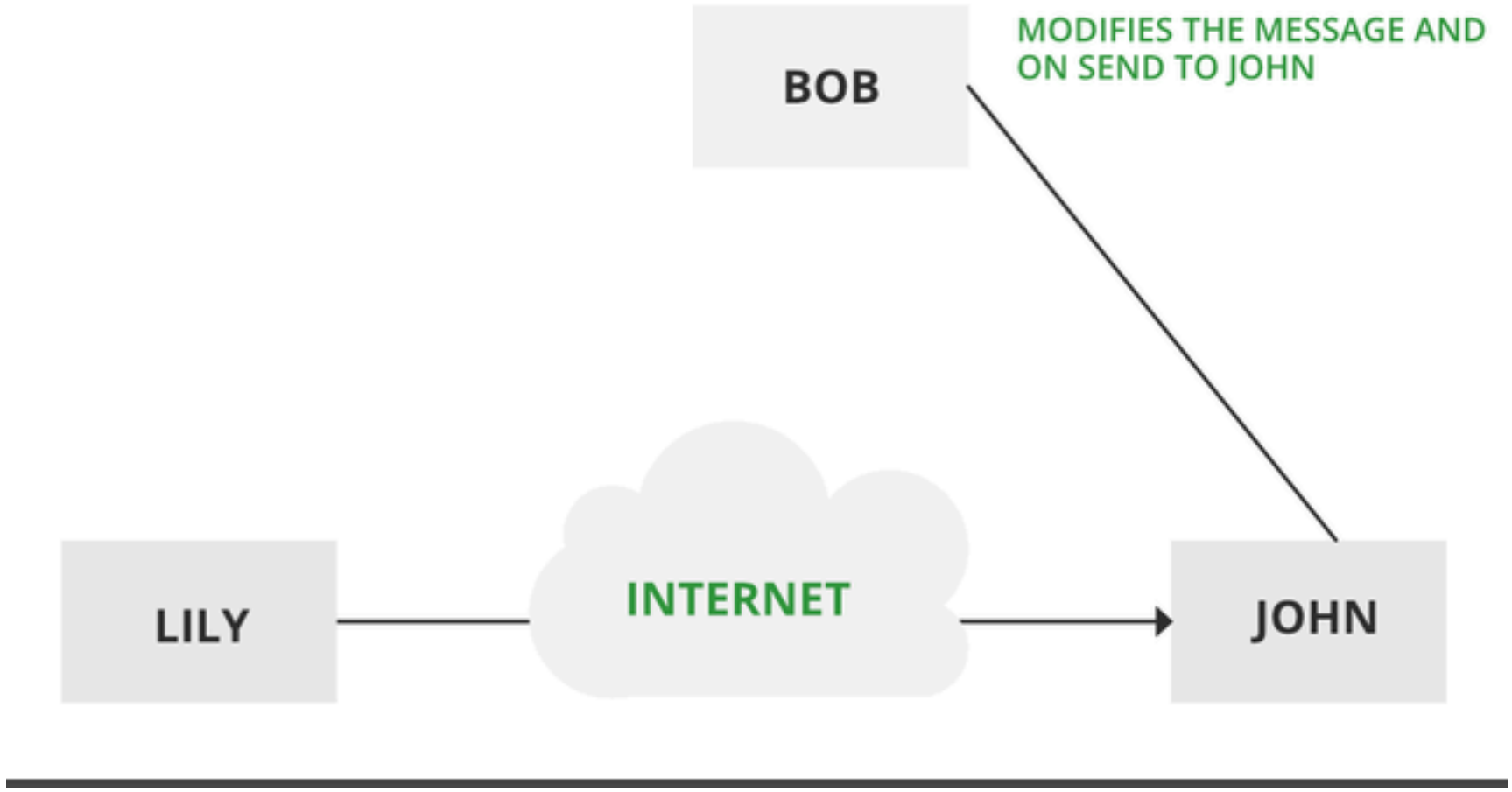
Traffic analysis

- Suppose that we had a way **of** masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.
  The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
  The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.


BOB OBSERVES THE
PATTERN OF MASSAGES EXCHANGES
BETWEEN LILY AND JOHN
BOB
LILY
INTERNET
JOHN

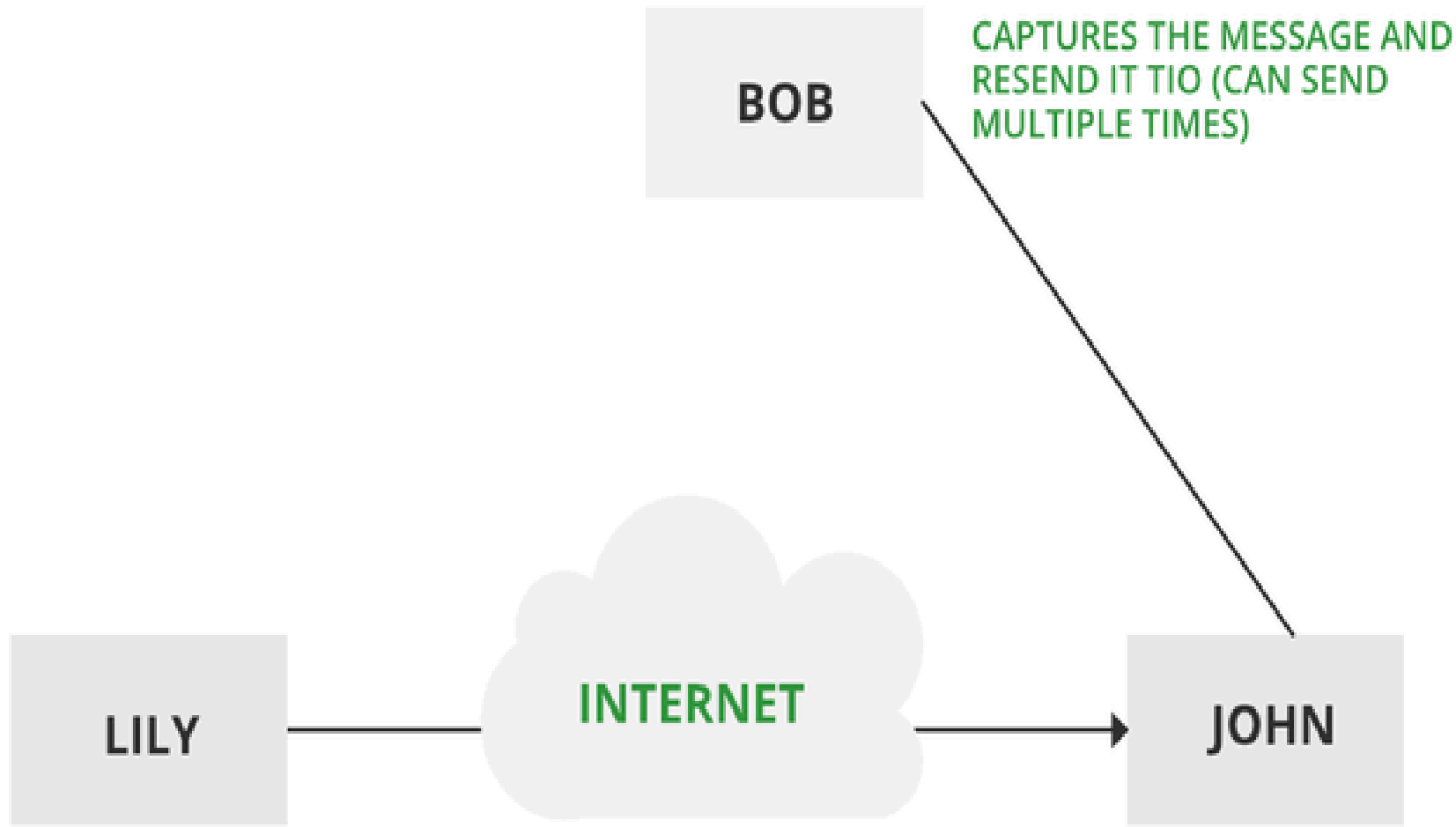
Modification of messages

- It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. Manufacturing is an attack on authentication. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.


BOB
MODIFIES THE MESSAGE AND
ON SEND TO JOHN
LILY
INTERNET
JOHN

Replaying

- It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.

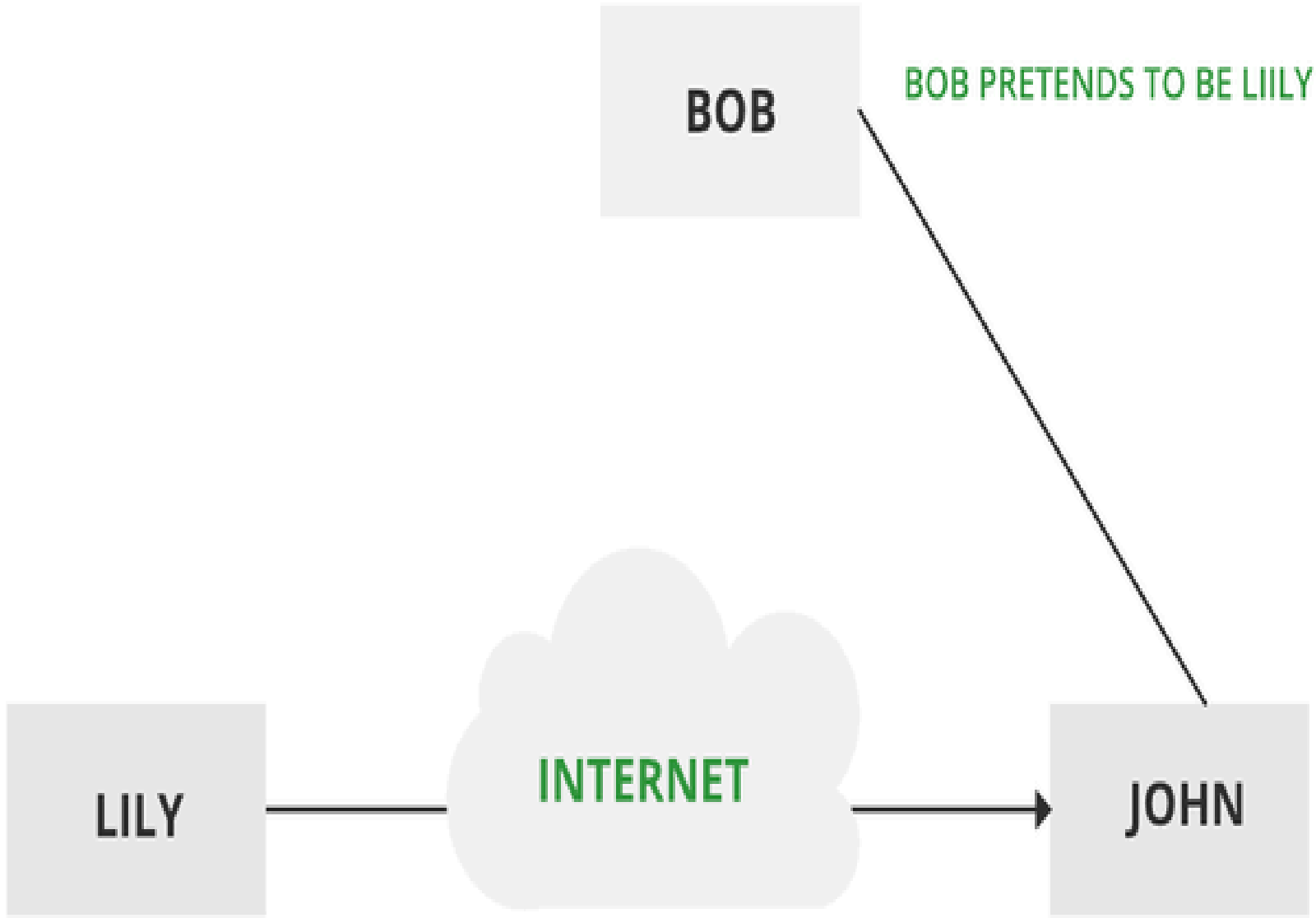

BOB
CAPTURES THE MESSAGE AND RESEND IT TIO (CAN SEND MULTIPLE TIMES)
LILY
INTERNET
JOHN

Repudiation

- This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author’s information can be ch anged by actions of a malicious user in order to save false data in log files, up to the general manipulation of data on behalf of others, similar to the spoofing of e-mail messages

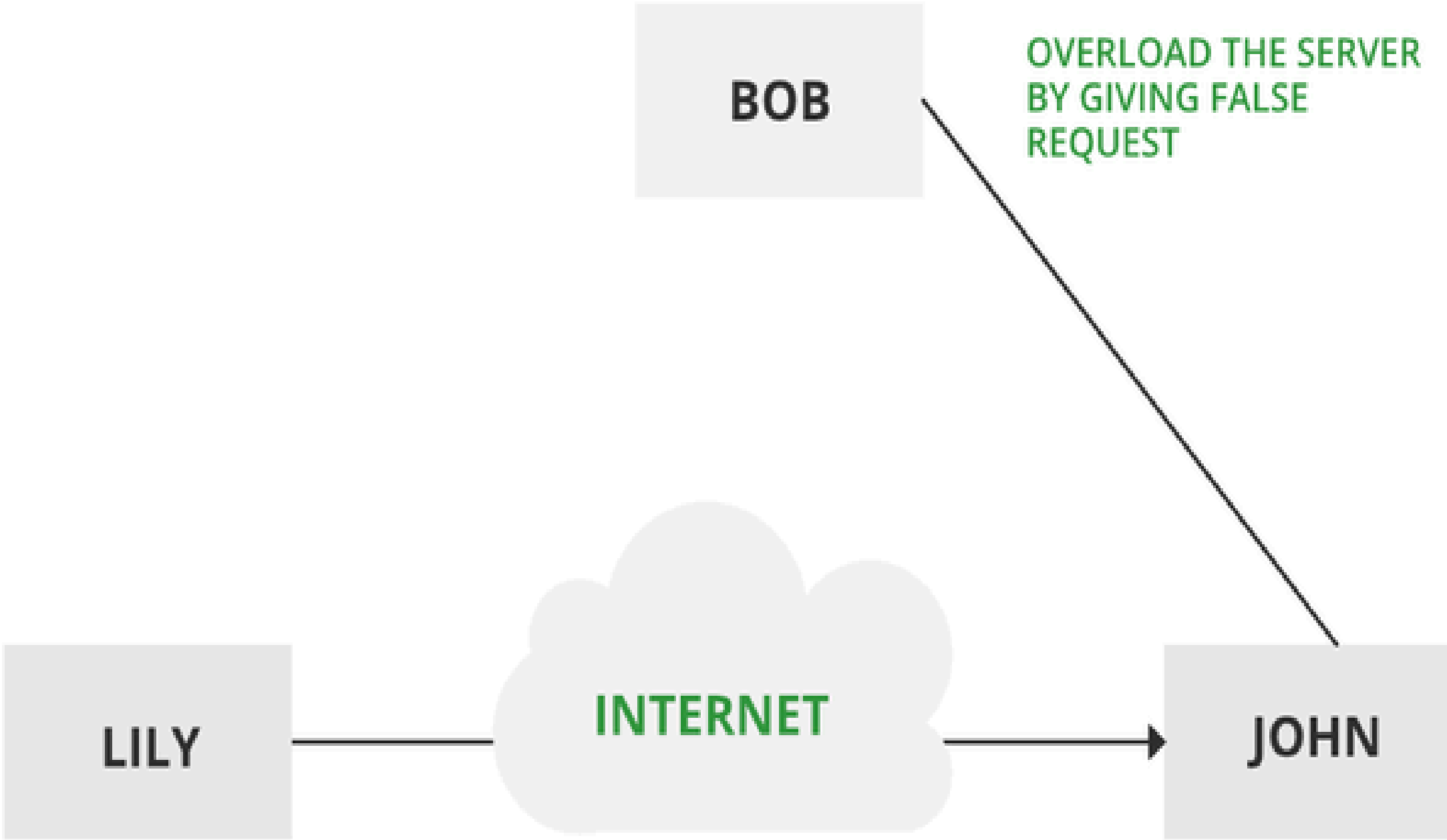
Masquerade

- A masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks. If an authorization procedure isn't always absolutely protected, it is able to grow to be extraordinarily liable to a masquerade assault. Masquerade assaults may be performed using the stolen passwords and logins, with the aid of using finding gaps in programs, or with the aid of using locating a manner across the authentication process.


BOB
BOB PRETENDS TO BE LIILY
LILY
INTERNET
JOHN

Denial of Service

- It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.


BOB
OVERLOAD THE SERVER BY GIVING FALSE REQUEST
LILY
INTERNET
JOHN

Common Types of Network Attacks

- **1. Unauthorized access**
  Unauthorized access refers to attackers accessing a network without receiving permission. Among the causes of unauthorized access attacks are weak passwords, lacking protection against social engineering, previously compromised accounts, and insider threats.
- **2. Distributed Denial of Service (DDoS) attacks**
  Attackers build botnets, large fleets of compromised devices, and use them to direct false traffic at your network or servers. DDoS can occur at the network level, for example by sending huge volumes of SYN/ACC packets which can overwhelm a server, or at the application level, for example by performing complex SQL queries that bring a database to its knees.
- **3. Man in the middle attacks**
  A man in the middle attack involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.

4. **Code and SQL injection attacks**
   Many websites accept user inputs and fail to validate and sanitize those inputs. Attackers can then fill out a form or make an API call, passing malicious code instead of the expected data values. The code is executed on the server and allows attackers to compromise it.
5. **Privilege escalation**
   Once attackers penetrate your network, they can use privilege escalation to expand their reach. Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.
6. **Insider threats**
   A network is especially vulnerable to malicious insiders, who already have privileged access to organizational systems. Insider threats can be difficult to detect and protect against, because insiders do not need to penetrate the network in order to do harm. New technologies like User and Even Behavioral Analytics (UEBA) can help identify suspicious or anomalous behavior by internal users, which can help identify insider attacks.

Security Services

- Message Confidentiality
- Message Integrity
- Message Authentication
- Message Non-Repudiation
- Entity Authentication

Message Confidentiality

- Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

Message Integrity

- Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial.
- For example, it would be disastrous if a request for transferring 100changedtoarequestfor100changedt oarequestfor10,000 or $100,000. The integrity of the message must be preserved in secure communication.

Message Authentication

- Message authentication is a service beyond message integrity. In message authentication, the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

Confidentiality

- The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message. For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

Message Nonrepudiation

- Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver.
- For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

Entity Authentication

- In entity authentication (or user identification), the entity or user is verified prior to access to the system resources (files, for example).
- For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

Security Mechanisms

- The mechanisms that help in setting up the security services in different layers of the OSI model and that help in identifying any attack or data breach are called security mechanisms. The security mechanisms provide a way of preventing, protecting, and detecting attacks.
- **Encipherment (Encryption):** One of the most popular security mechanisms is encryption. The message/data sent from the sender to the receiver is usually encrypted to some format that even if the message is stolen, cannot be decrypted easily by the attacker. Some of the popular encryption algorithms are AES, RSA, Triple DES, etc.

- **Traffic Padding:** The sender and receiver send the data to each other. Now, sometimes there is a gap between the sender and receiver. This means that for some time when the sender and receiver are not sharing the data, the attacker can act as if it is the sender and send some data to the receiver to attack it. So, this can be avoided if the gap (empty time) between the sender and the receiver is not known to the attacker. For this, during the gap duration, the sender keeps on sending some dummy data to the receiver and the receiver knows that this is the dummy data by using some identification. Hence, no gap is created between the sender and the receiver and the attacker cannot attack the system.
- **Routing Control:** The messages that a sender sends to a receiver travel different routes, However, in some cases, the sender and receiver might communicate mostly via the same route. In this case, the attacker tracks this route and can make changes to the data or take advantage of this. So, routing should be controlled in such a way that mostly, a different route is selected between the sender and the receiver to deliver the message.

Benefits of OSI Security Architecture

- Benefits of the OSI Security Architecture are as follows:

1. OSI Security Architecture Provides International Standards
2. Easy for the Managers
3. OSI Security Architecture Provides Security

Techniques to achieve Security Goals

1. Cryptography
2. Steganography

Cryptography

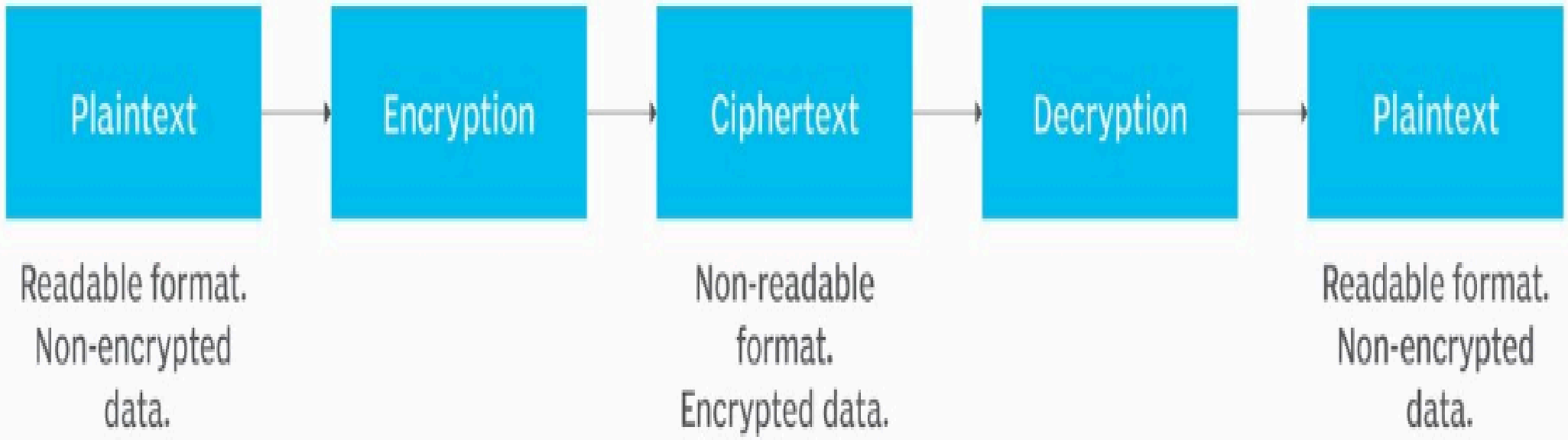
- Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.
- Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication.

components of cryptography

1. Plaintext and Ciphertext: The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.
2. Cipher: We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for secure communication. On the contrary, one cipher can serve millions of communicating pairs.

- Key :A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

Cryptography



Encryption

- Encryption is the process of transforming information using algorithm to make it unreachable to anyone except those possessing special knowledge, usually referred to as a key.
- Decryption is the reverse process of Encryption to make the encrypted information readable again.

Encryption : Uses

- Encryption can be used to protect data “ at rest”, such as files on computers and storage devices.
- It is used to protect data in transit.
- Encryption by itself can protect the confidentiality of message.

Types of Cryptography

1. Symmetric Key Cryptography

   In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

2. Asymmetric-Key Cryptography

   In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

   In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public, and the private key is available only to an individual.

   3. Hash Functions:

   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

Symmetric encryption

Asymmetric encryption

Steganography

- As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover image and the image obtained after steganography is called the stego image.
- Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

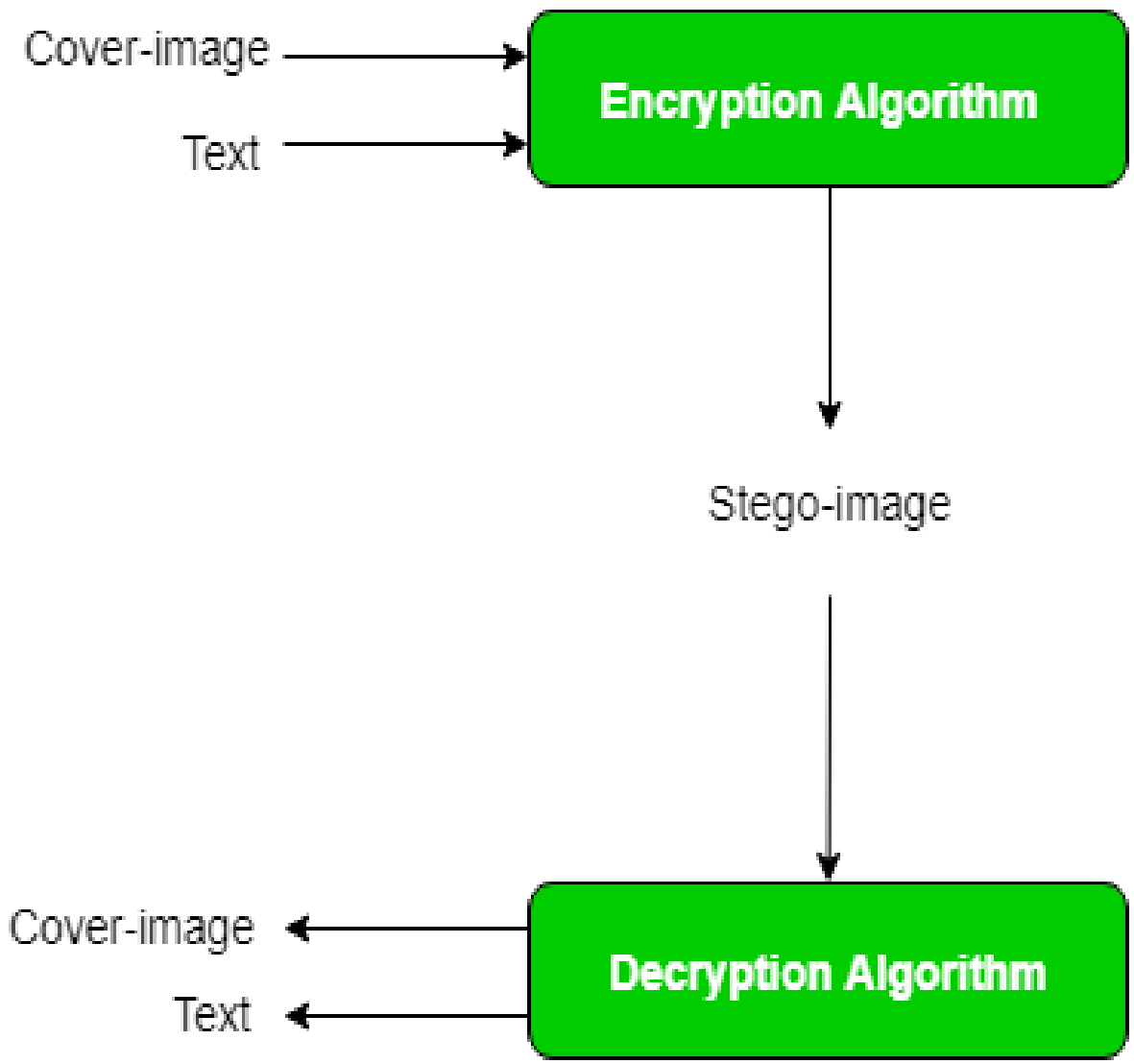
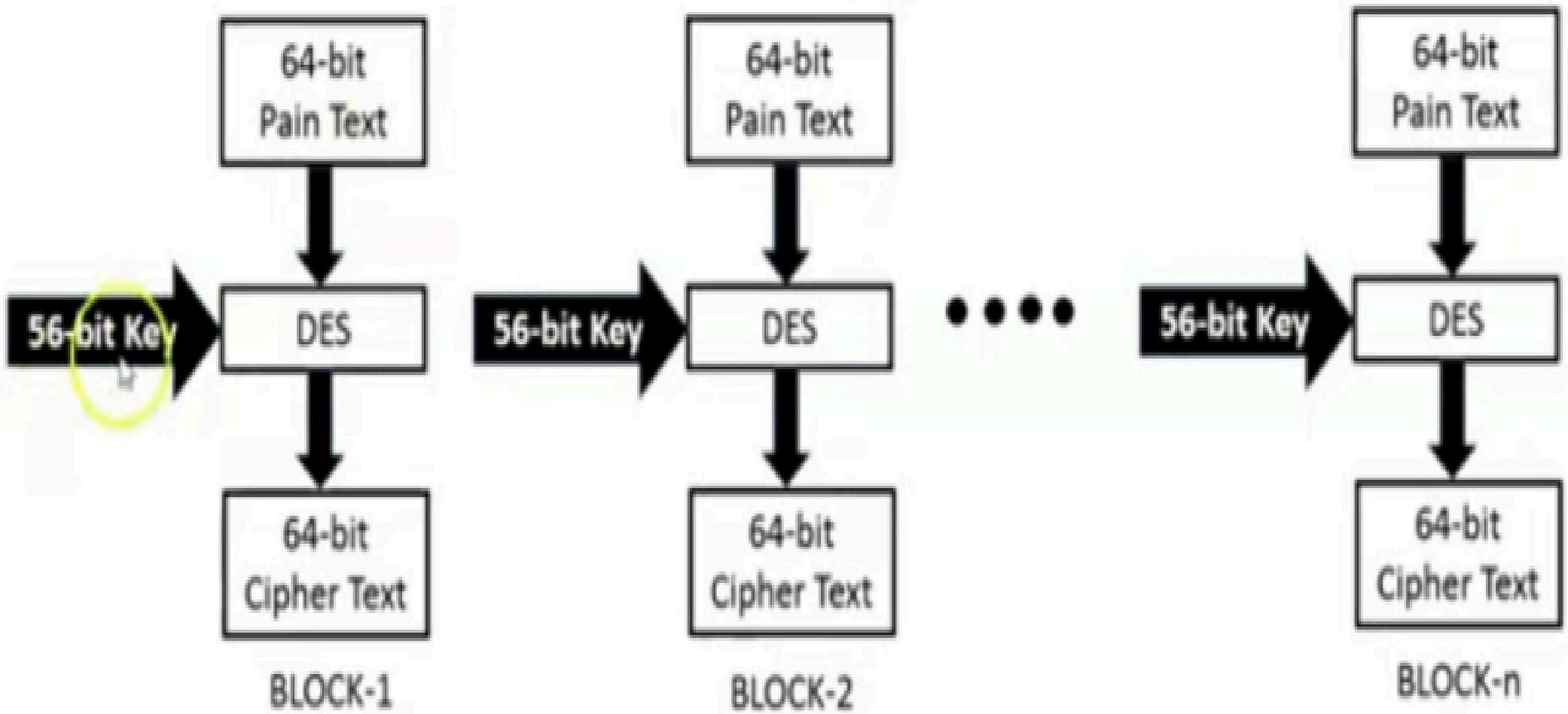


Figure – Process of Image Steganography

Data Encryption Standard(DES)

- Developed in early 1970's at IBM & submitted to NBS.
- DES is landmark in cryptographic algorithms.
- DES works based on Feistel Cipher Structure.
- DES is Symmetric cipher algorithm & use block cipher method for encryption & decryption.

Process of DES



Key discarding Process

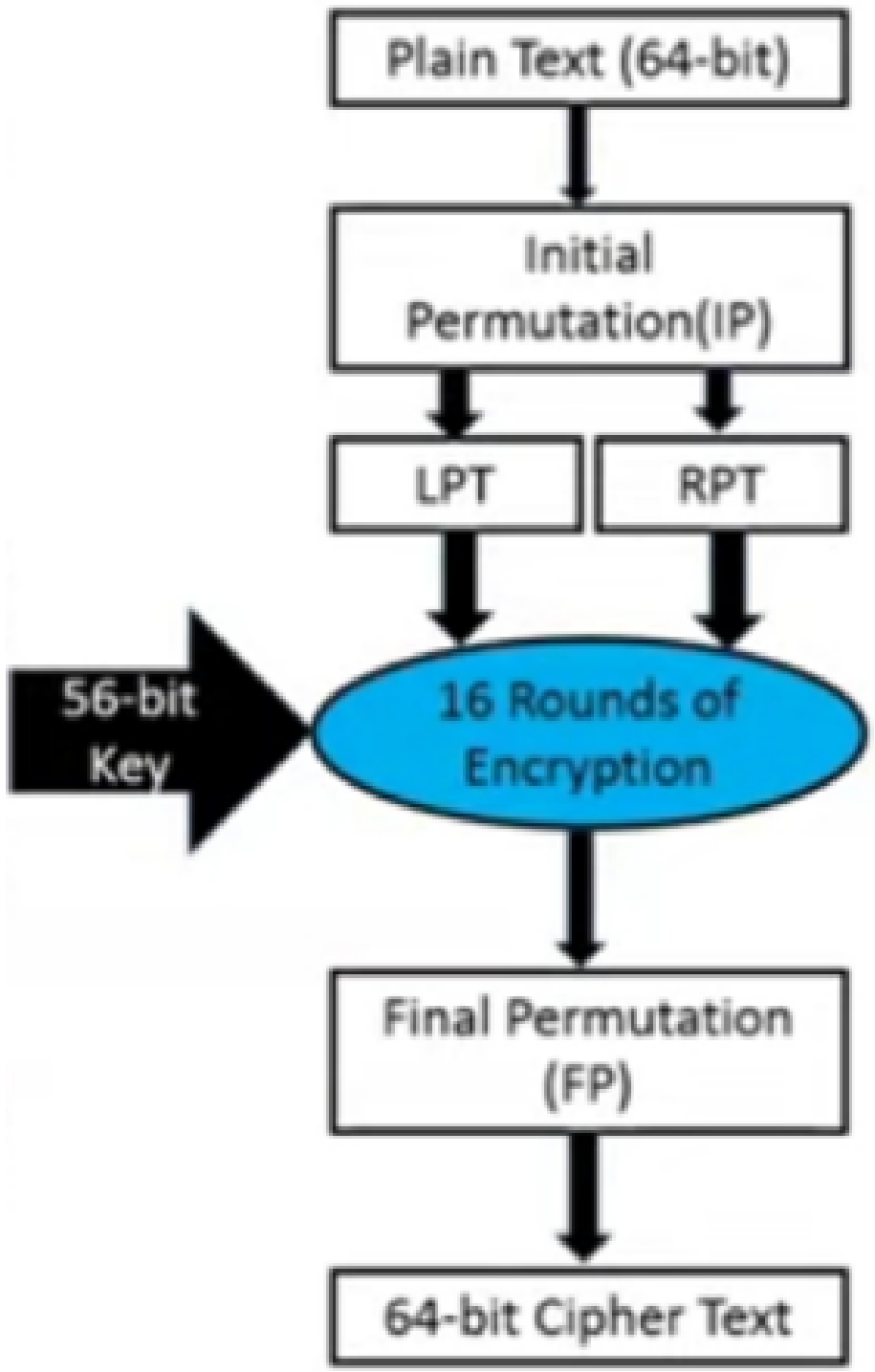
- **Key discarding process**

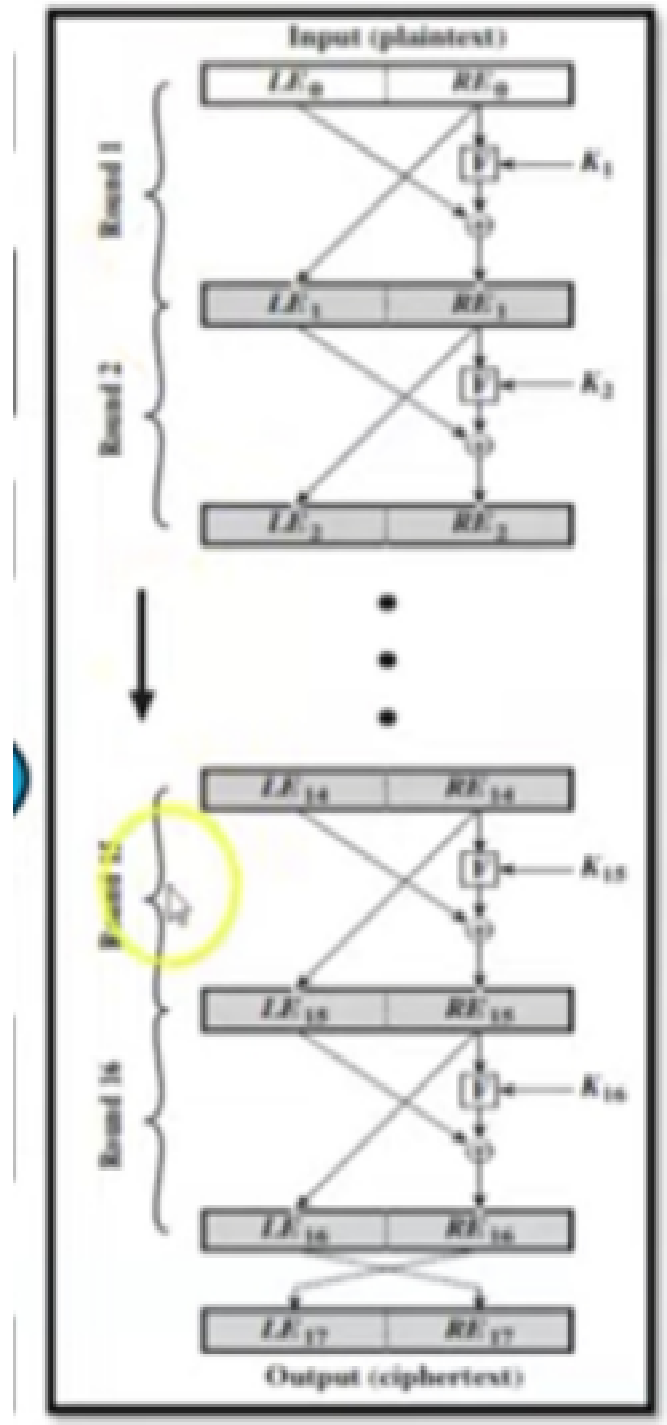
1	2	21	38	58	15	37	26
22	55	44	3	53	27	11	60
49	28	14	42	61	48	63	41
18	39	56	10	64	16	62	8
45	40	20	54	4	33	34	52
7	30	47	59	32	5	35	25
29	12	13	6	24	46	57	36
17	23	50	31	43	51	9	19

1	2	21	38	58	15	37
22	55	44	3	53	27	11
49	28	14	42	61	48	63
18	39	56	10	64	16	62
45	40	20	54	4	33	34
7	30	47	59	32	5	35
29	12	13	6	24	46	57
17	23	50	31	43	51	9

Steps of DES

1. 64-bit plain text block is given to Initial Permutation (IP) function.
2. IP performed on 64-bit plain text block.
3. IP produced two halves of the permuted block known as Left Plain Text(LPT) and Right Plain Text(RPT).
4. Each LPT & RPT performed 16-rounds of encryption process.
5. LPT & RPT rejoined and Final permutation (FP) is performed on combined block.
6. 64-bit Cipher text block is generated.





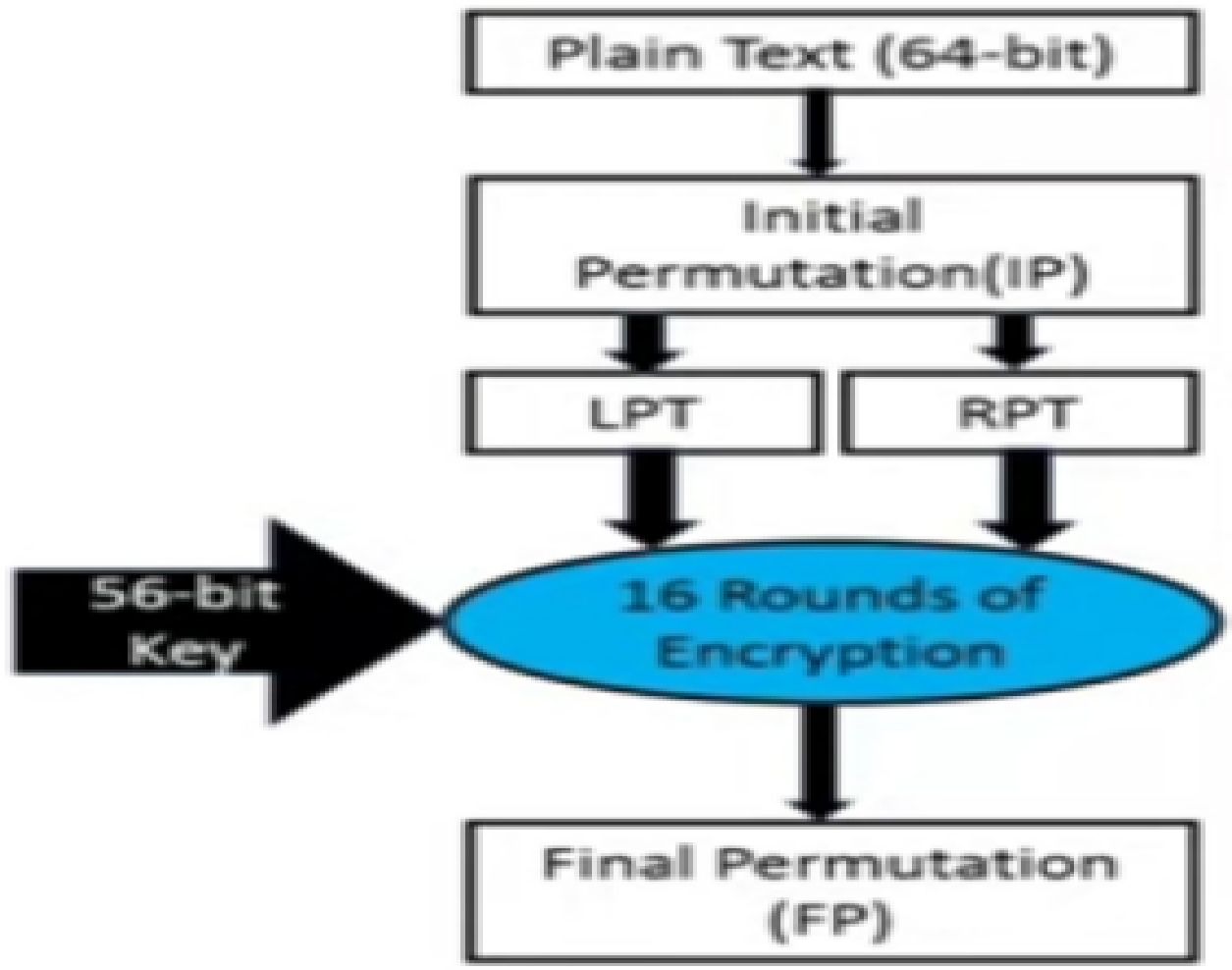
Feistel Cipher Structure

Initial Permutation(IP) & Generate LPT-RPT

- Initial permutation performed by only once.
- Bit sequence have changed as per IP table.
- For eg.
- 1^{st} bit take 40^{th} position.
- 58^{th} bit take 1^{st} position.

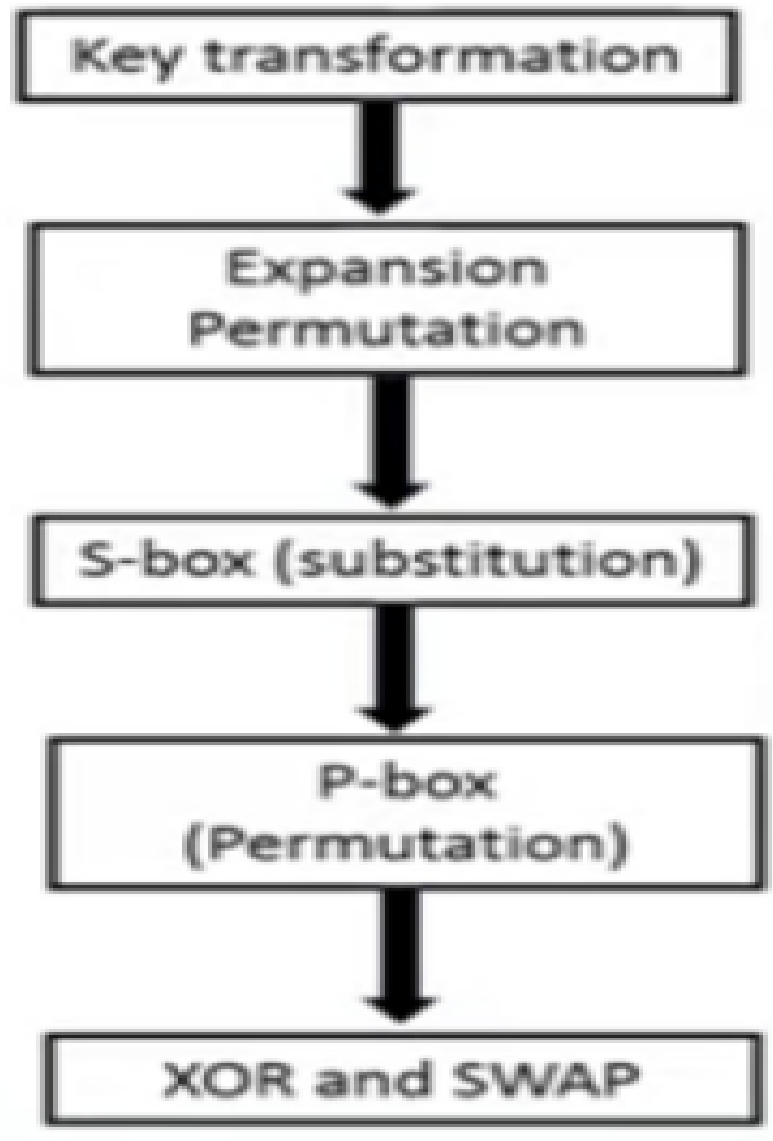
- Output of IP is divided into two equal halves known as LPT, RPT. (LPT- 32 bit, RPT-32 bit).

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25



16 Rounds of Encryption

1. Key Transformation (56-bit key)
- Key Bit Shifted per round
- Compression Permutation
2. Expansion permutation of Plain Text & X-OR (P.T. size:48 bit, C.T. size: 48 bit)
3. S-box Substitution
4. P-box(Permutation)
5. X-OR and Swap.


Key transformation
Expansion
Permutation
S-box (substitution)
P-box
(Permutation)
XOR and SWAP

Key Bit Shifted per Round

- 56-bit key is divided into two halves each of 28-bits
- Circular left shift is performed on each halves
- Shifting of Bit position is depending on round
- For round number 1,2,9 & 16 shift is done b

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Key bit shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

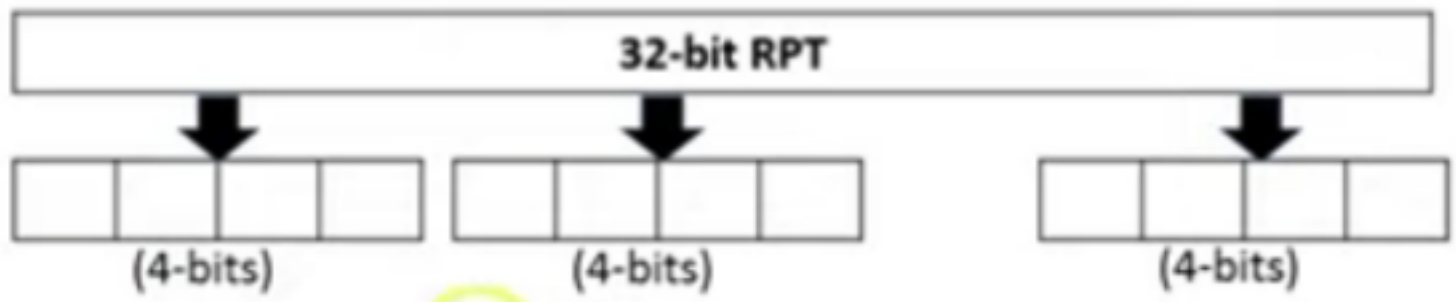
Compression Permutation

- 56-bit input with bit shifting position
- Generate 48-bit key (Compression of Key bit)
- Drop 9,18,22,25,35,38,43 and 54 bits

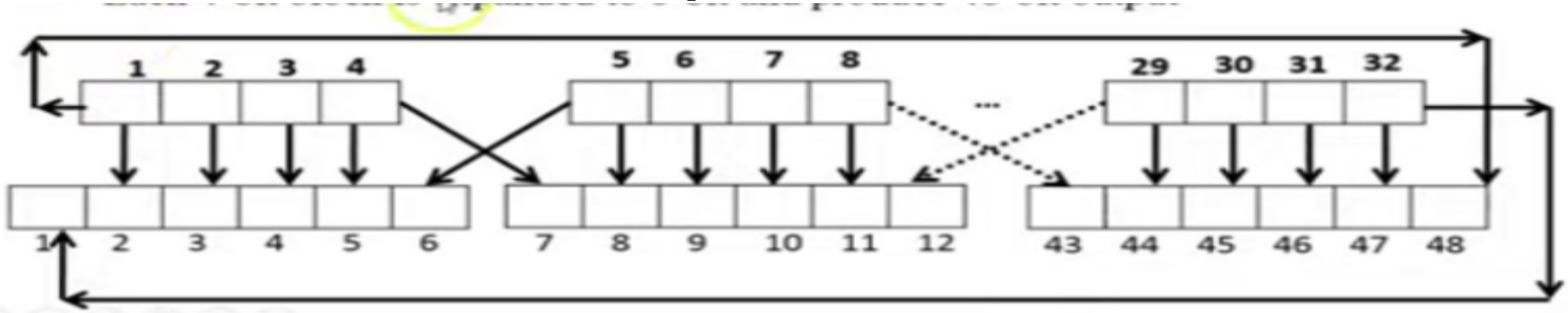
14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Expansion Permutation

- 32-bit RPT of IP is expanded to 48-bits
- Expansion permutation steps:
- 32-bit RPT is divided into 8-blocks each of 4-bits



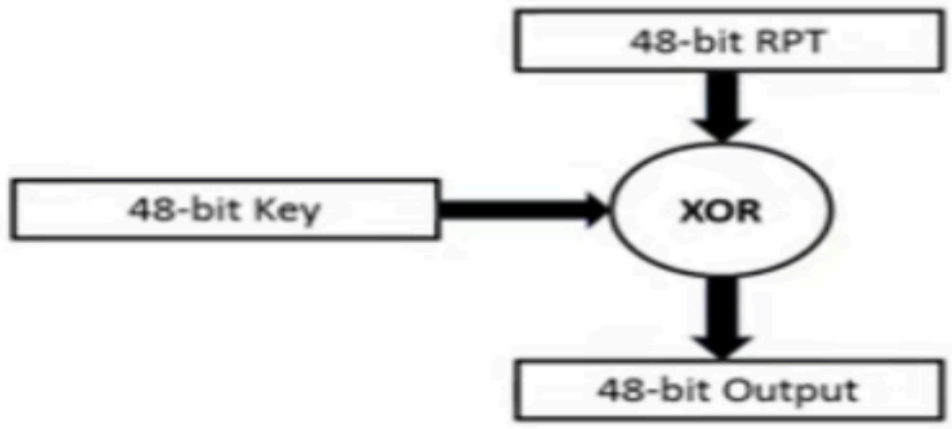
- Each 4-bit block is expanded to 6-bit & produce 48-bit output.

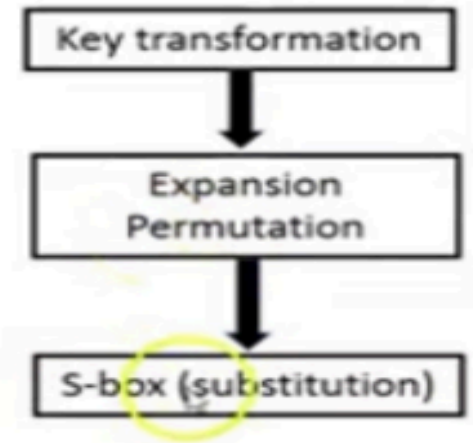


Expansion permutation

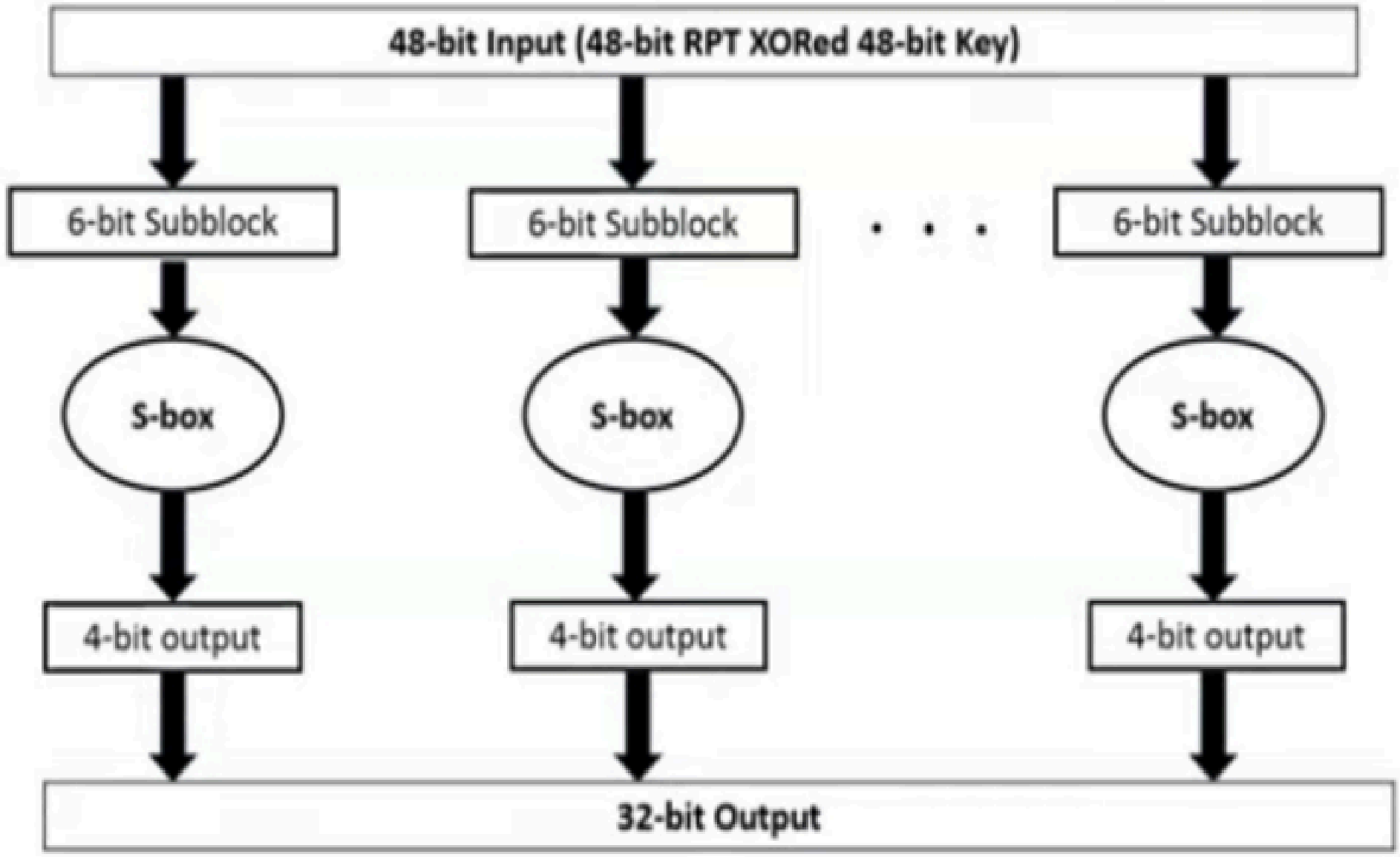
- 48-bit RPT is X-OR ed with 48-bit key & output is given to S-Box.

Expansion Permutation

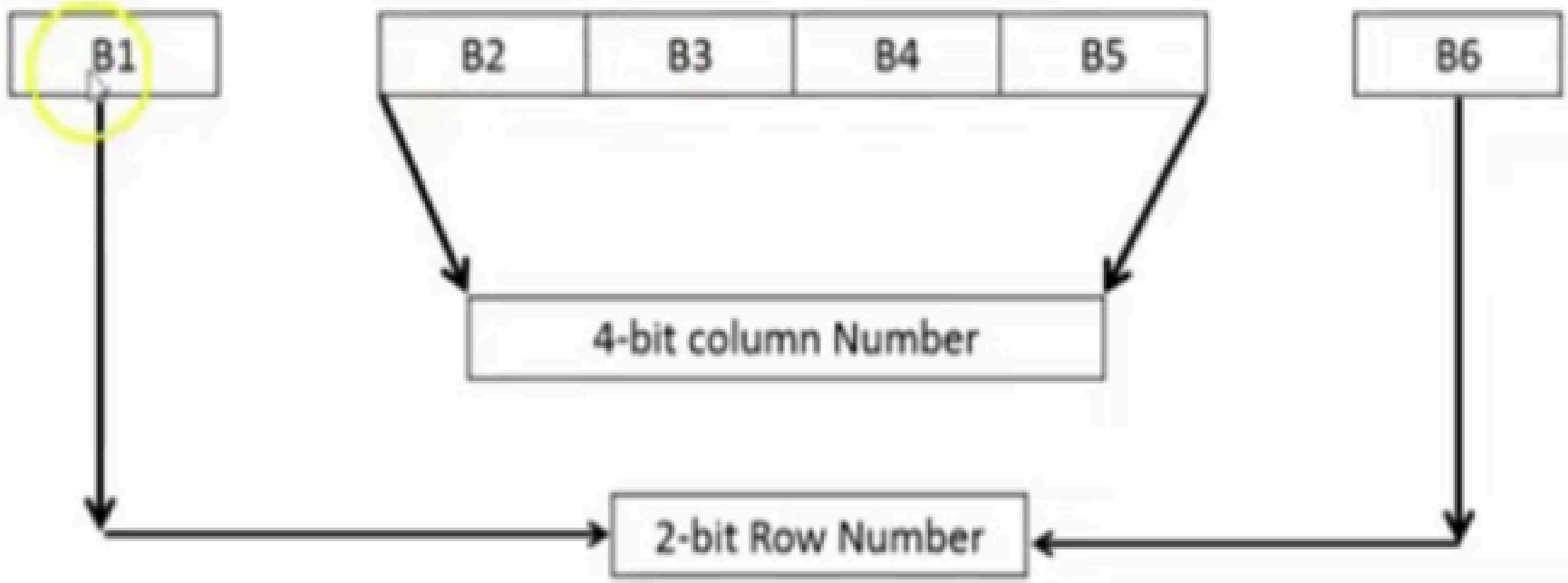




S-BOX Substitution



S-BOX working



S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Example: 011011 → 1001

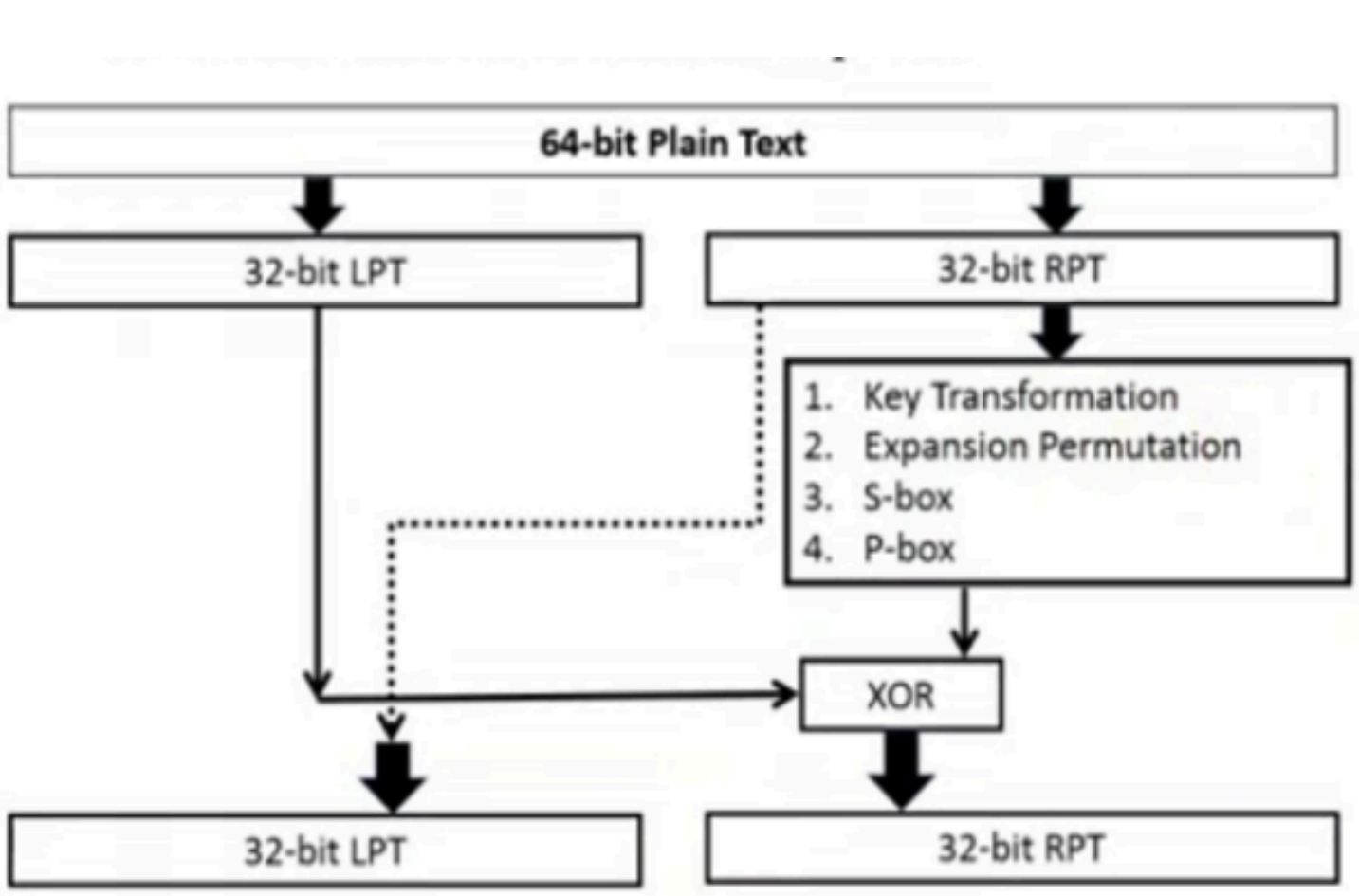
P-BOX permutation

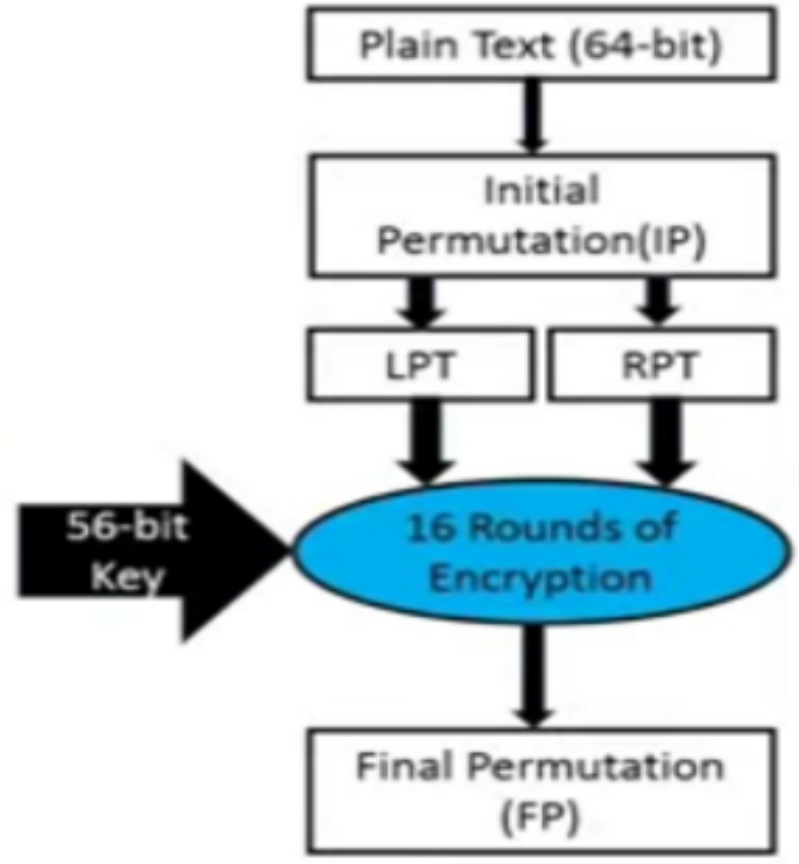
- Output of s-box is given to p-box
- 32-bit is permuted with 16*2 permutation table
- For Example:
- 16th bit of S-box take 1st position as per below permutation table.

P – Box Table															
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

XOR and SWAP

- 32-bit LPT is XOR ed with 32-bit p-box
- 1st round of encryption is completed. Now remaining 15 rounds will be performed same as 1st round.

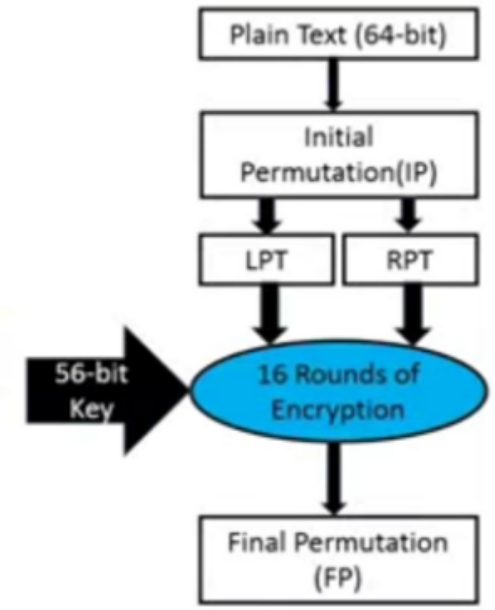




Final Permutation

- At the end of the 16 rounds, the final permutation is performed(only once).
- For example:
- 40^{th} bit of input take 1^{st} Position as per below permutation table.

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25



- The output of the final permutation is the 64-bit encrypted block(64-bit cipher text block).

Hacking

- Act of illegally entering a computer system , and making unauthorized changes to the files and data contain within.
- The process of attempting to gain or successfully gaining, unauthorized access to computer resources is called hacking.

Types of hacking

- Website Hacking
- Network Hacking
- Ethical Hacking
- Email Hacking
- Password Hacking
- Online Banking Hacking
- Computer Hacking

Who is Hacker

- In the Computer Security context, a hacker is someone who seeks and exploits weakness in a computer system or computer network.
- Any programming specialist who has expertise to enter computer network unauthorized.

- Hacker: A person who enjoys learning the details of computer systems and how to stretch their capabilities- as opposed to most users of computers, who prefer to learn only the minimum amount necessary.
- One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.

Types of Hacker

- White Hats
- Black Hats
- Gray Hats

White hats Hackers

- Ethical hackers usually fall into the white-hat category
- White hats are the good guys, the ethical hackers who use their hacking skills for defensive purpose.
- White hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weakness and implement countmeasures.
- White hats are those with permission from the data owner.

Black Hats Hackers

- Black hats are the bad guys ,the malicious hackers or crackers who use their skills for illegal or malicious purpose.
- The break System otherwise violate the system integrity of remote systems, with malicious internet.
- Having gained unauthorized access, black hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets.

Grey Hats Hackers

- Grey hats hackers who may work offensively or defensively, depending on the situation.
- Grey hat hackers may just be interested in hacker tools mostly from a curiosity standpoint.
- They may want to highlight security problems in a systems or educate victims so they secure their systems properly.
- These hackers are doing their “victims” a favour.

Ethical Hacking

- Using the same software tools & techniques as malicious hackers to find the security weakness in computer networks & systems.
- Ethical Hackers must always act in a professional manner to differentiate themselves from malicious hackers.
- Ethical hacker always gain permission from the data owner prior to accessing the computer system.

Goals of Ethical Hacking

- Hack your systems in non destructive fashion
- Enumerate vulnerabilities and if necessary prove to upper management that vulnerabilities exists.
- Apply results to remove vulnerabilities & better secure your systems.

Digital Signature

A digital signature is a mathematical technique which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author name, date and time of signatures, and authenticate the message contents. The digital signature offers far more inherent security and intended to solve the problem of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.

Application of Digital Signature

- The important reason to implement digital signature to communication is:

1. Authentication
2. Non-repudiation
3. Integrity

- Authentication

  Authentication is a process which verifies the identity of a user who wants to access the system. In the digital signature, authentication helps to authenticate the sources of messages.

- Non-repudiation

  Non-repudiation means assurance of something that cannot be denied. It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or in a file or the sending of a message that they originated.

- Integrity

  Integrity ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.

Algorithms in Digital Signature

A digital signature consists of three algorithms:

1. **Key generation algorithm**

- The key generation algorithm selects private key randomly from a set of possible private keys. This algorithm provides the private key and its corresponding public key.

2. **Signing algorithm**

- A signing algorithm produces a signature for the document.

3. **Signature verifying algorithm**

A signature verifying algorithm either accepts or rejects the document's authenticity.

How digital signatures work

- Digital signatures are created and verified by using public key cryptography, also known as **assymmetric** cryptography. By the use of a public key algorithm, such as RSA, one can generate two keys that are mathematically linked- one is a private key, and another is a public key.
- The user who is creating the digital signature uses their own private key to encrypt the signature-related document. There is only one way to decrypt that document is with the use of signer's public key.
- This technology requires all the parties to trust that the individual who creates the signature has been able to keep their private key secret. If someone has access the signer's private key, there is a possibility that they could create fraudulent signatures in the name of the private key holder.

Network layer Security

1. Application Layer –
Communication Protocols- HTTP,FTP,SMTP
Security Protocols- PGP,S/MIME, HTTPS
2. Transport Layer-
Communication Protocols- TCP /UDP
Security Protocols- SSL, TLS, SSH
3. Network Layer-
Communication Protocols- IP
Security Protocols- IPsec

Transport Layer Security

- Bob visits Alice’s website for selling goods. In a form on the website, Bob enters the type of good and quantity desired, his address and payment card details. Bob clicks on Submit and waits for delivery of goods with debit of price amount from his account. All this sounds good, but in absence of network security, Bob could be in for a few surprises.
- If transactions did not use confidentiality (encryption), an attacker could obtain his payment card information. The attacker can then make purchases at Bob's expense.
- If no data integrity measure is used, an attacker could modify Bob's order in terms of type or quantity of goods.
- Lastly, if no server authentication is used, a server could display Alice's famous logo but the site could be a malicious site maintained by an attacker, who is masquerading as Alice. After receiving Bob's order, he could take Bob's money and flee. Or he could carry out an identity theft by collecting Bob's name and credit card details.
- Transport layer security schemes can address these problems by enhancing TCP/IP based network communication with confidentiality, data integrity, server authentication, and client authentication.

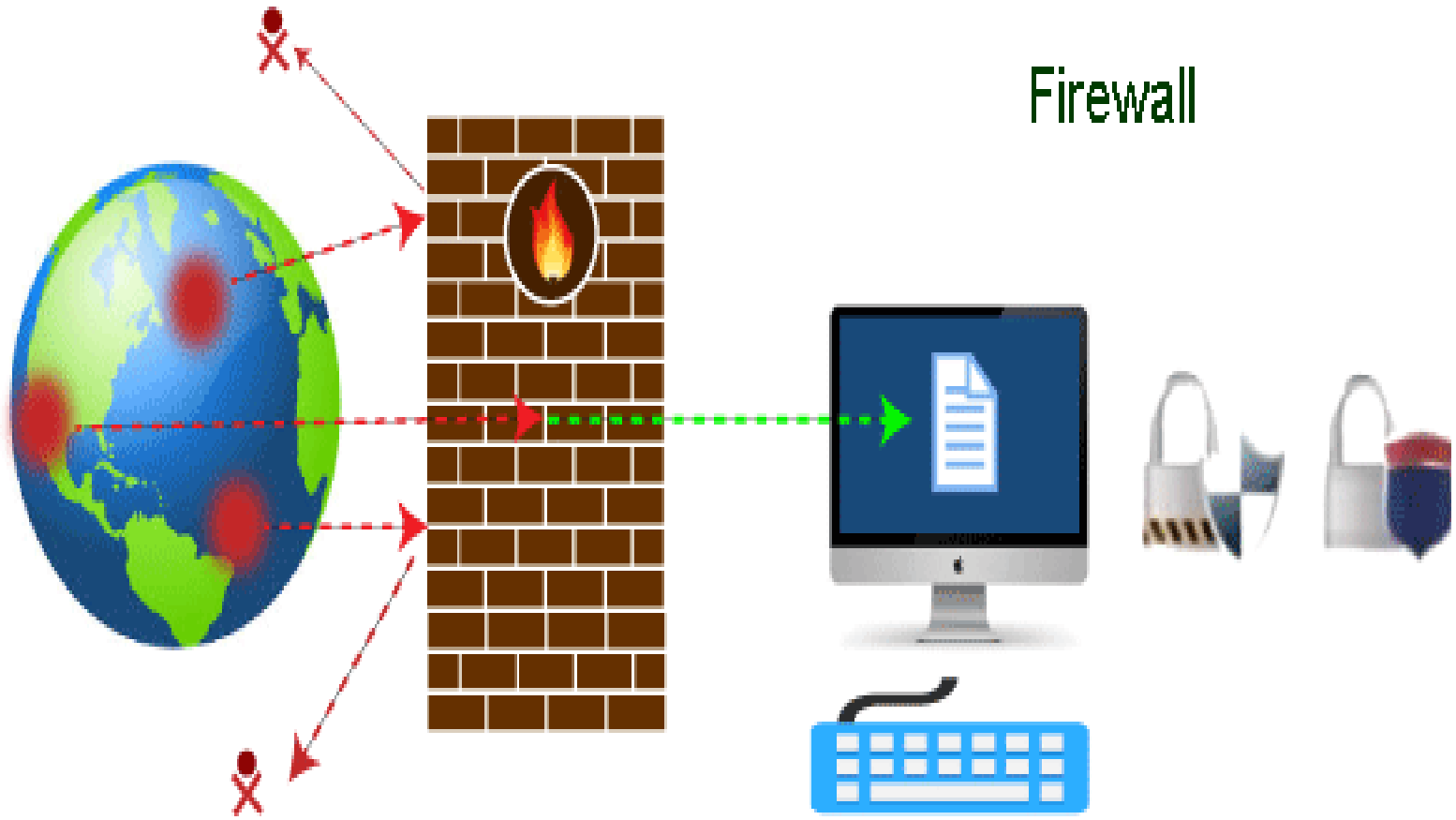
Application Layer Security

- Application layer security refers to ways of protecting web applications at the application layer (layer 7 of the OSI model) from malicious attacks.
- E-mail Security

  Nowadays, e-mail has become very widely used network application. Let’s briefly discuss the e-mail infrastructure before proceeding to know about e-mail security protocols.
- The protocols used for e-mail are as follows –
- Simple mail Transfer Protocol (SMTP) used for forwarding e-mail messages.
- Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) are used to retrieve the messages by recipient from the server.

Firewall

- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.


Firewall

Why Firewall

- Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

Intrusion Detection Systems(IDS)

- An intrusion detection system (IDS) is an app or device that monitors inbound and outbound network traffic, continuously analyzing activity for changes in patterns, and alerts an administrator when it detects unusual behavior. An administrator then reviews alarms and takes actions to remove the threat.
- For example, an IDS might inspect the data carried by network traffic to see if it contains known malware or other malicious content. If it detects this type of threat, it sends an alert to your security team so they can investigate and remediate it. Once your team receives the alert, they must act quickly to prevent an attack from taking over the system.

Goals of Intrusion Detection Systems

- A firewall alone doesn’t provi de adequate protection against modern cyber threats. Malware and other malicious content are often delivered using legitimate types of traffic, such as email, or web traffic. An IDS provides the ability to inspect the contents of these communications and identify any malware that they might contain.
- The main goal of an IDS is to detect anomalies before hackers complete their objective. Once the system detects a threat, the IDS informs the IT staff and provides the following info about the danger:
- The source address of the intrusion.
- Target and victim addresses.
- The type of threat.

Assignment

Thank You