Module- 4 Network Security

Network Security: Providing Security to the stored Data and the data in transit.

Elements of Network Security:There are two security elements

a. **Confidentiality:** Information should be available only to those who have rightful access to it.

b. **Authenticity and integrity:** The sender of a message and the message itself should be verified at the receiving point.

Why do we need to protect information on network?

Threats to Network Security

Internet infrastructure attacks are broadly classified into four categories, as follows:

1. DNS hacking

2. Routing table poisoning

3. Packet mistreatment

4. Denial of service

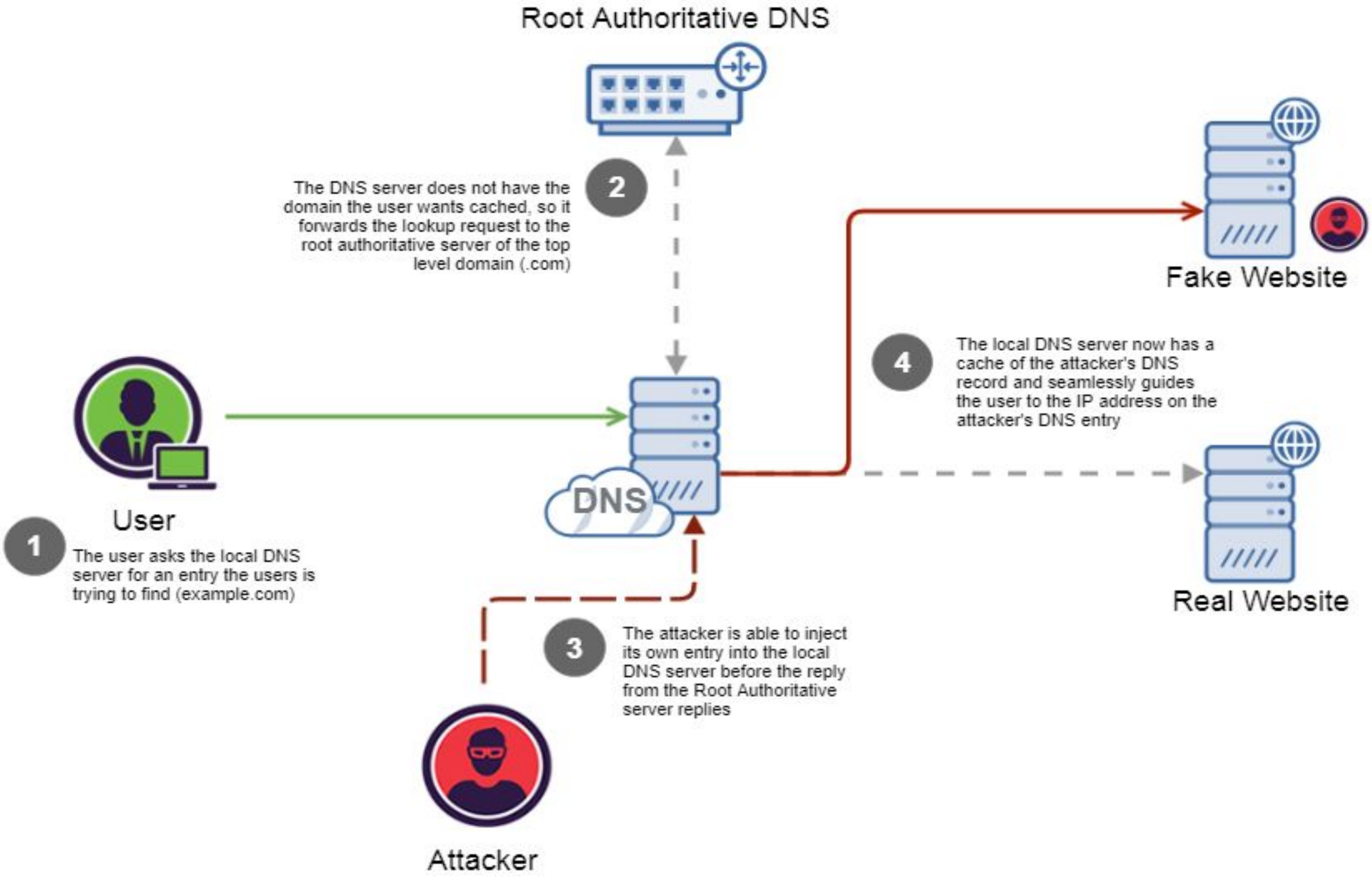
1. DNS hacking: DNS provides address resolution service over Ineternet.(ie, Domain name to IP address conversion)

A DNS hacking attack may result in the lack of data authenticity and integrity and can appear in any of the following forms:

A. DNS cache poisoning:

is a user-end method of DNS spoofing, in which your system logs the fraudulent IP address in your local memory cache. This leads the DNS to recall the bad site specifically for you, even if the issue gets resolved or never existed on the server-end.

With cache poisoning, a hacker tricks a remote name server into caching the answer for a third-party domain by providing malicious information for the domain's authorized servers. Hackers can then redirect traffic to a preselected site.



1 The user asks the local DNS server for an entry the users is trying to find (example.com)

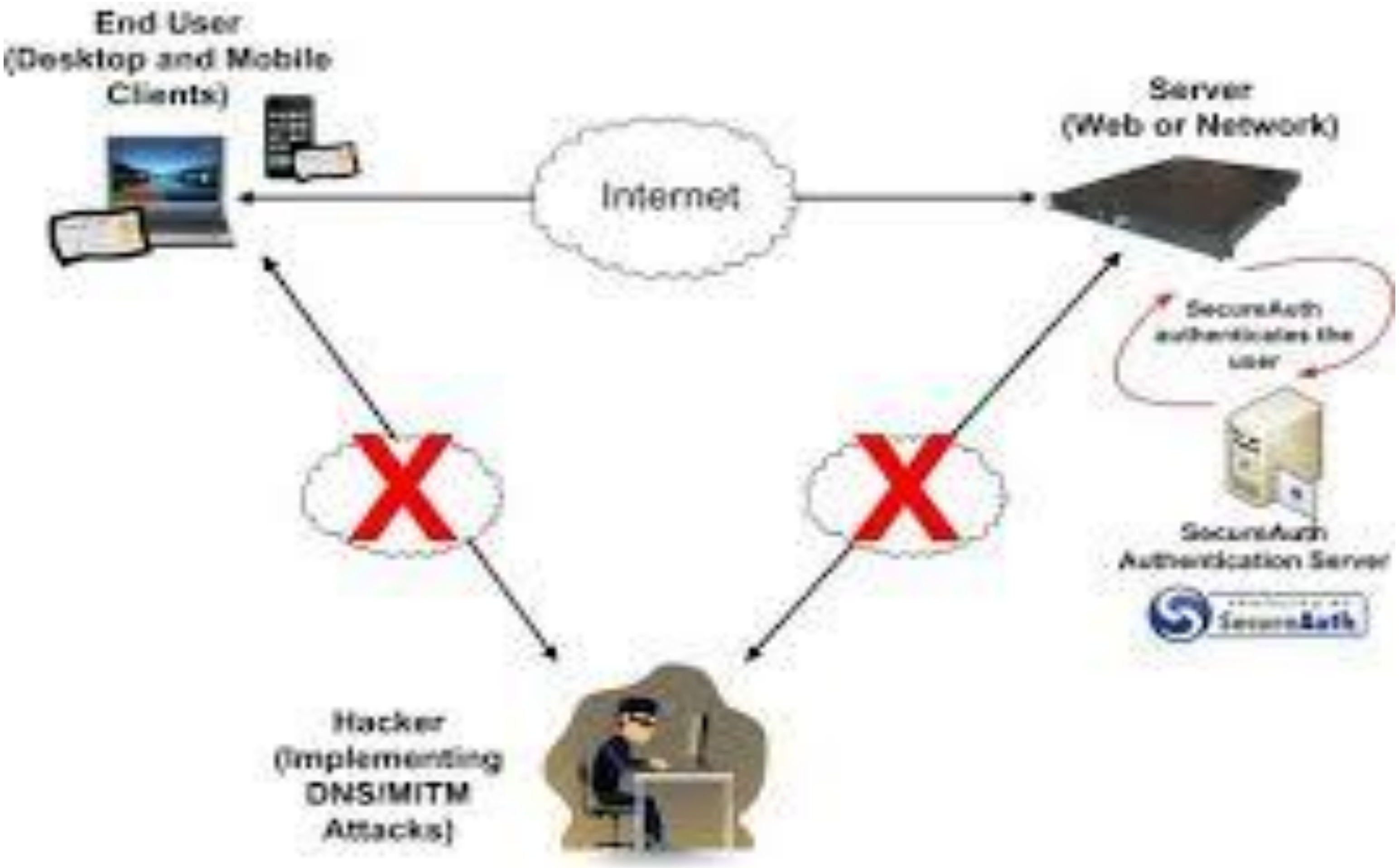
2 The DNS server does not have the domain the user wants cached, so it forwards the lookup request to the root authoritative server of the top level domain (.com)

3 The attacker is able to inject its own entry into the local DNS server before the reply from the Root Authoritative server replies

4 The local DNS server now has a cache of the attacker's DNS record and seamlessly guides the user to the IP address on the attacker's DNS entry

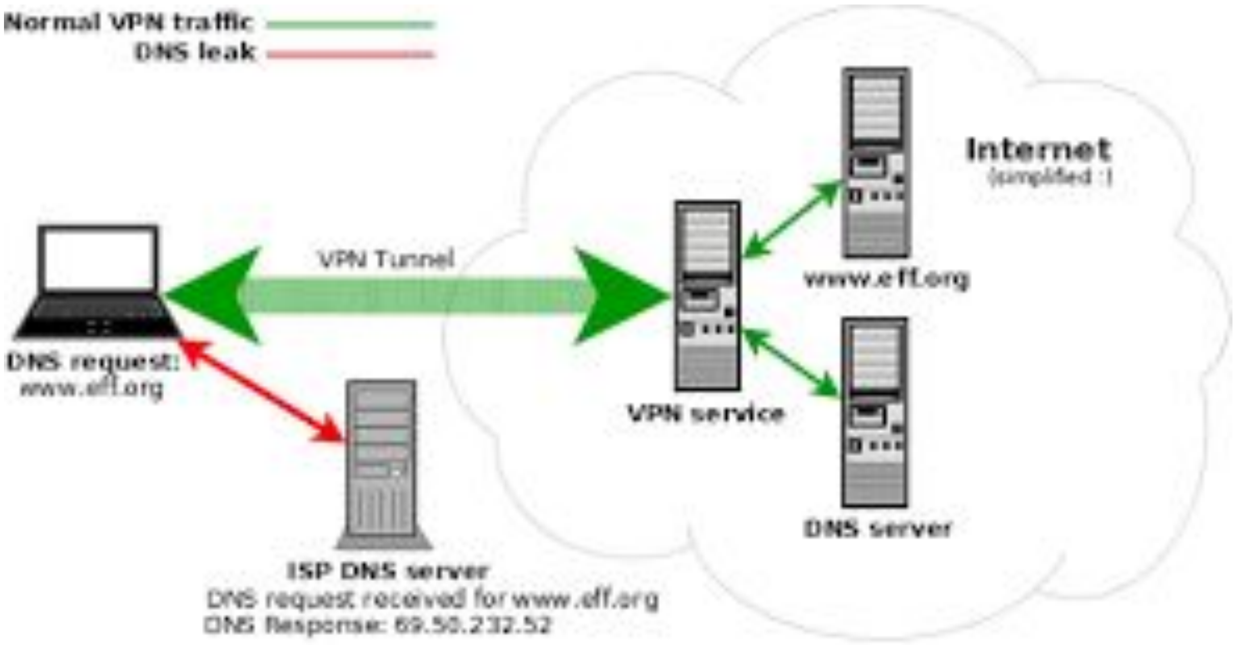
B. Masquerading attack:

- The adversary poses as a trusted entity and obtains all the secret information.
- In this guise, the attacker can stop any message from being transmitted further or can change the content or redirect the packet to bogus servers. This action is also known as a **middle-man attack.**


End User
(Desktop and Mobile Clients)
Internet
Server
(Web or Network)
SecureAuth authenticates the user
SecureAuth Authentication Server
SecureAuth
Hacker
(Implementing DNS/MITM Attacks)

C. information leakage attack:

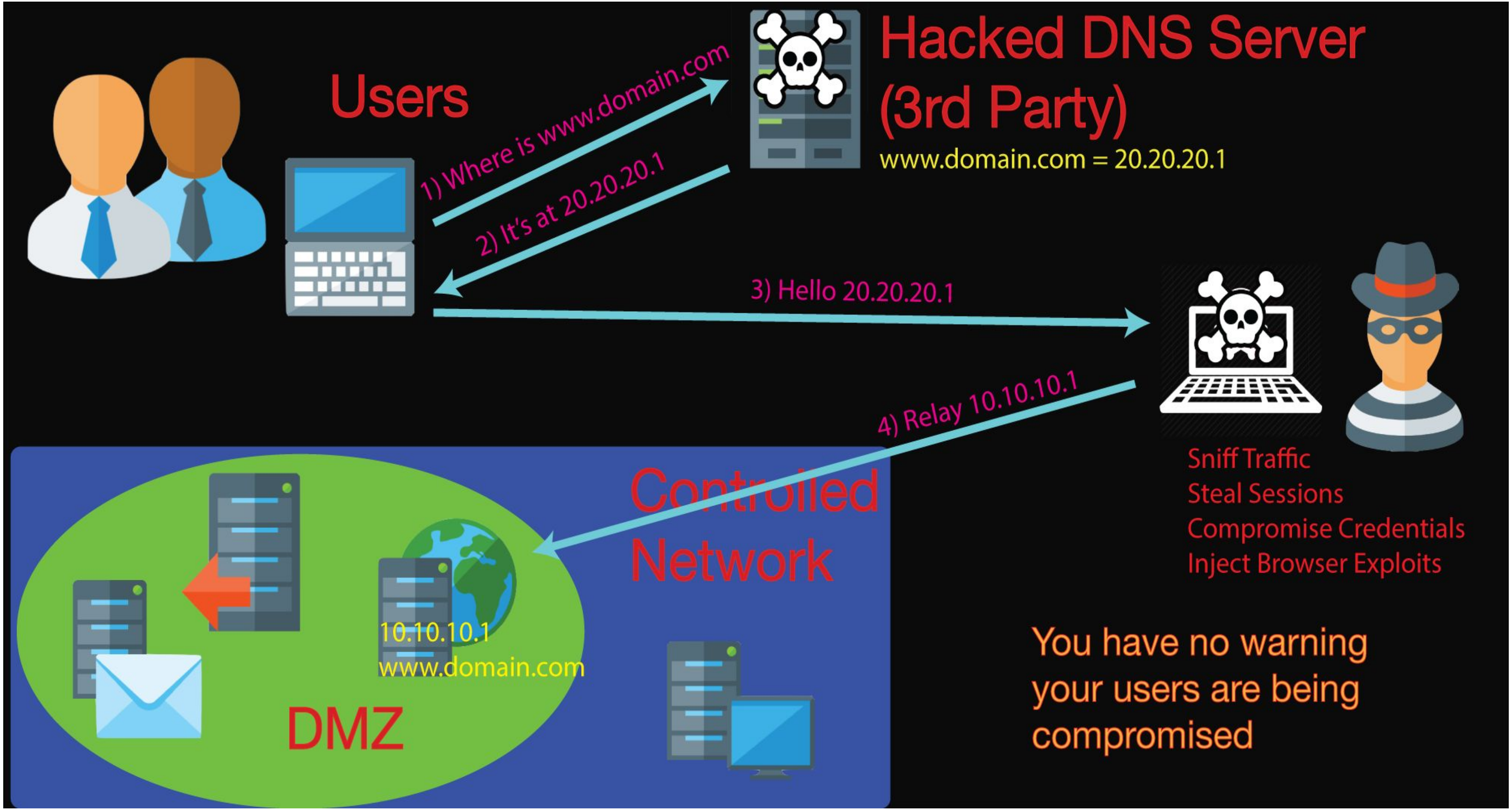
The attacker normally sends queries to each host and receives in reply the DNS host name. In an information leakage attack, the attacker sends queries to all hosts and identifies which IP addresses are not used. Later on, the intruder can use those IP addresses to make other types of attacks.



www.dnsleaktest.com

D. DNS server hijack:

- The criminal directly reconfigures the server to direct all requesting users to the malicious website.
- Once a fraudulent DNS entry is injected onto the DNS server, any IP request for the spoofed domain will result in the fake site.



Users

Hacked DNS Server (3rd Party)

www.domain.com = 20.20.20.1

1) Where is www.domain.com

2) It's at 20.20.20.1

3) Hello 20.20.20.1

4) Relay 10.10.10.1

Sniff Traffic
Steal Sessions
Compromise Credentials
Inject Browser Exploits

Controlled Network

DMZ

10.10.10.1
www.domain.com

You have no warning your users are being compromised

2.Routing table poisoning attack

- A routing table poisoning attack is the undesired modification of routing tables.
- An attacker can do this by maliciously modifying the routing information update packets sent by routers.
- Any false entry in a routing table could lead to significant consequences, such as congestion, an overwhelmed host, looping, illegal access to data, and network partition.
- Two types of routing table poisoning attacks are the **link attack** and the **router attack.**
- A **link attack** occurs when a hacker gets access to a link and thereby intercepts, interrupts, or modifies routing messages on packets.(Modification in packet info)
- **Router attacks** may affect the link-state protocol or even the distance-vector protocol. If link-state protocol routers are attacked, they become malicious.

3. Packet-Mistreatment Attacks

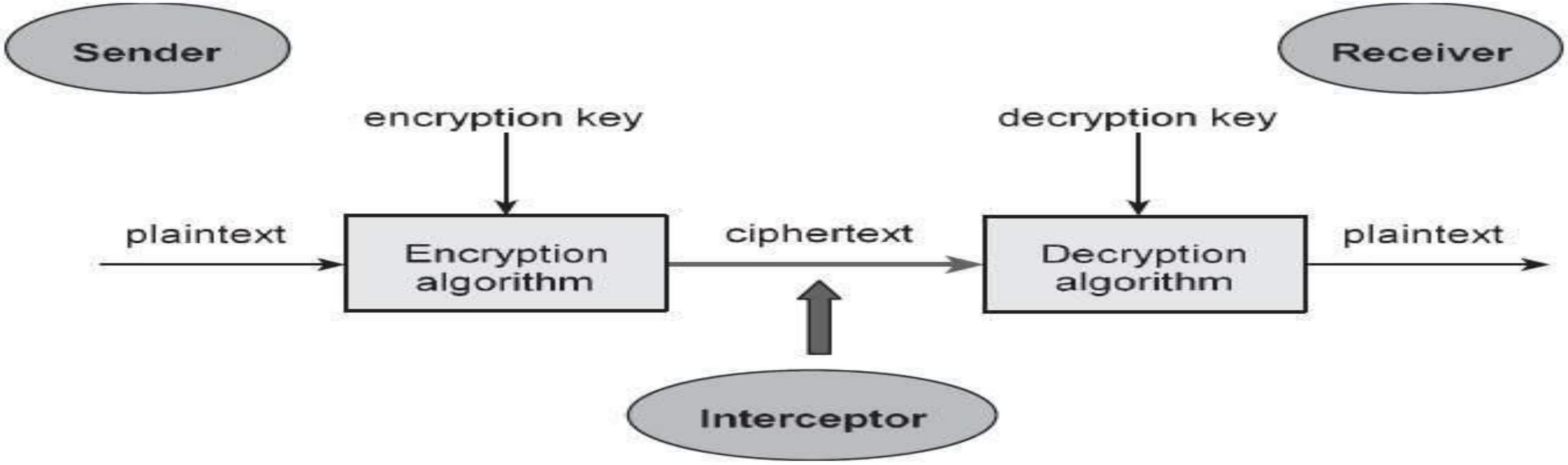
- A packet-mistreatment attack can occur during any data transmission. A hacker may capture certain data packets and mistreat them. This type of attack is very difficult to detect. The attack may result in congestion, lowering throughput, and denial-of-service attacks.
- packet-mistreatment attacks can also be subclassified into link attacks and router attacks.
- The link attack causes interruption, modification, or replication of data packets. A router attack can misroute all packets and may result in congestion or denial of service.

4. Denial-of-Service Attacks

- A denial-of-service attack is a type of security breach that prohibits a user from accessing normally provided services.
- Denial-of-service attacks affect the destination rather than a data packet or router.
- Usually, a denial-of-service attack affects a specific network service, such as e-mail or DNS. For example, such an attack may overwhelm the DNS server in various ways and make it inoperable.
- Denial-of-service attacks are easy to generate but difficult to detect. They take important servers out of action for few hours, thereby denying service to all users.

Overview of Security Methods

Cryptographic Techniques: **Cryptography** is the science of protecting information by transforming it into a secure format. It makes use of Encryption and decryption process.

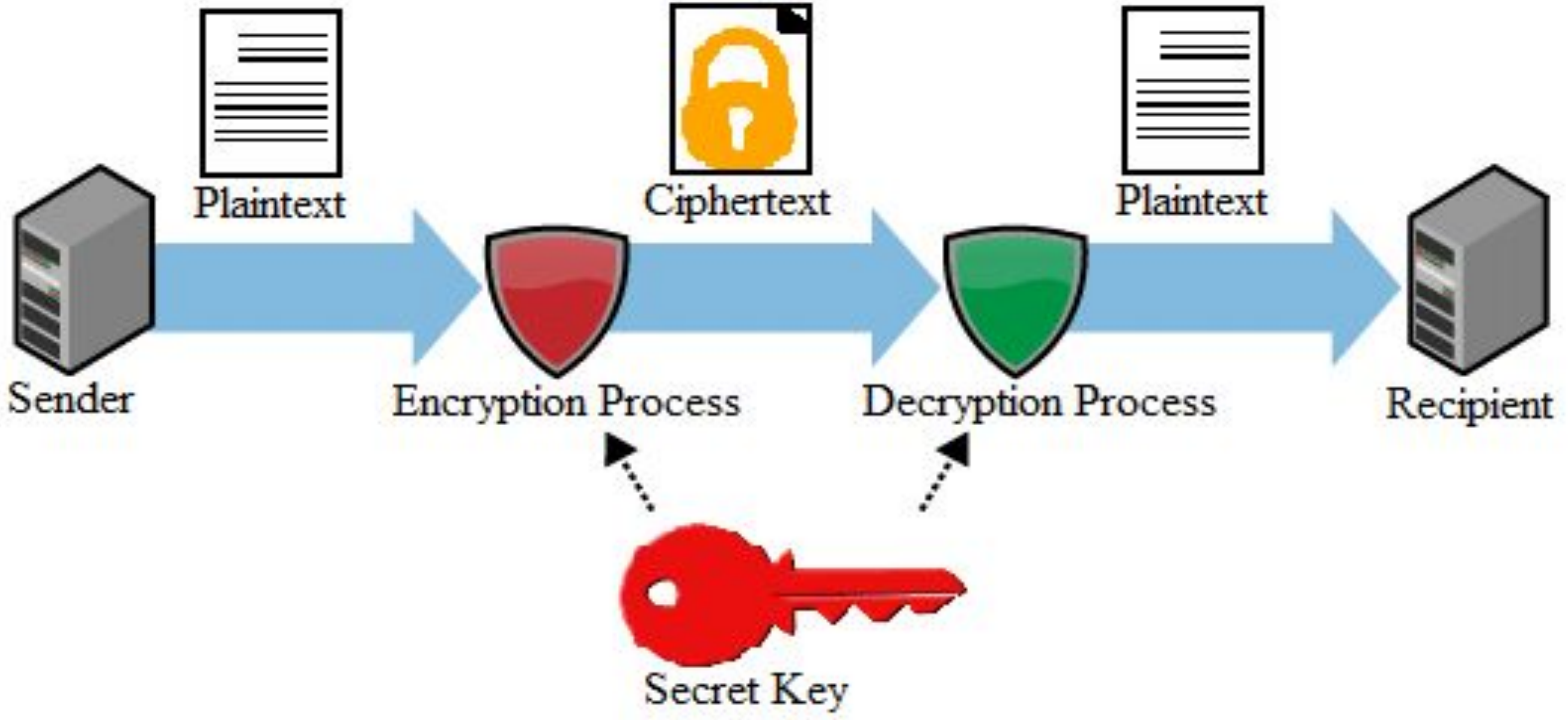


Types of Encryption Techniques in Cryptography

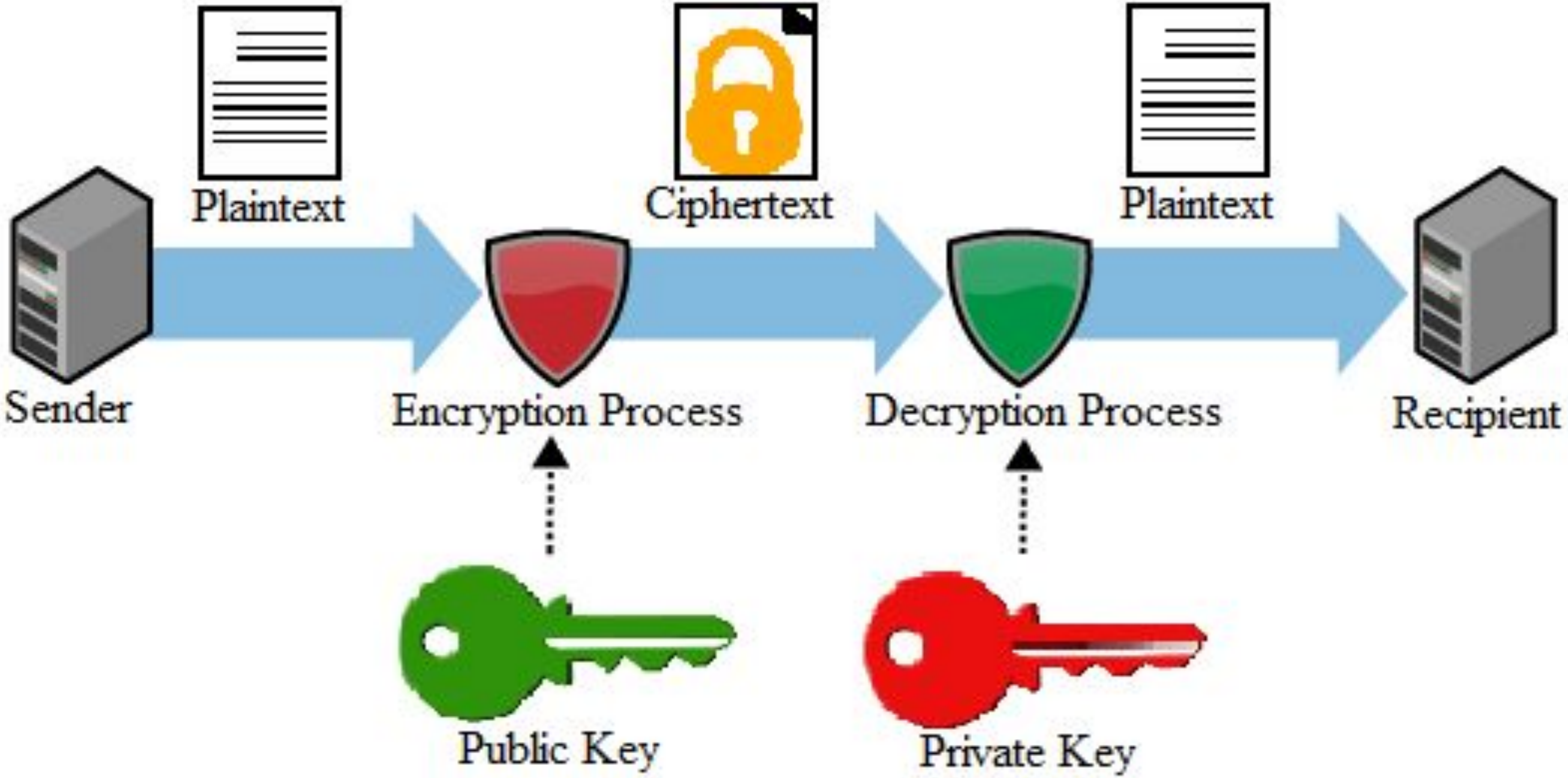
1. **Private Key encryption(Symmetric key encryption, Single key encryption)**

2. **Public Key Encryption(Asymmetric key encryption, 2-key encryption)**

1. Private Key Encryption



2. Public Key encryption



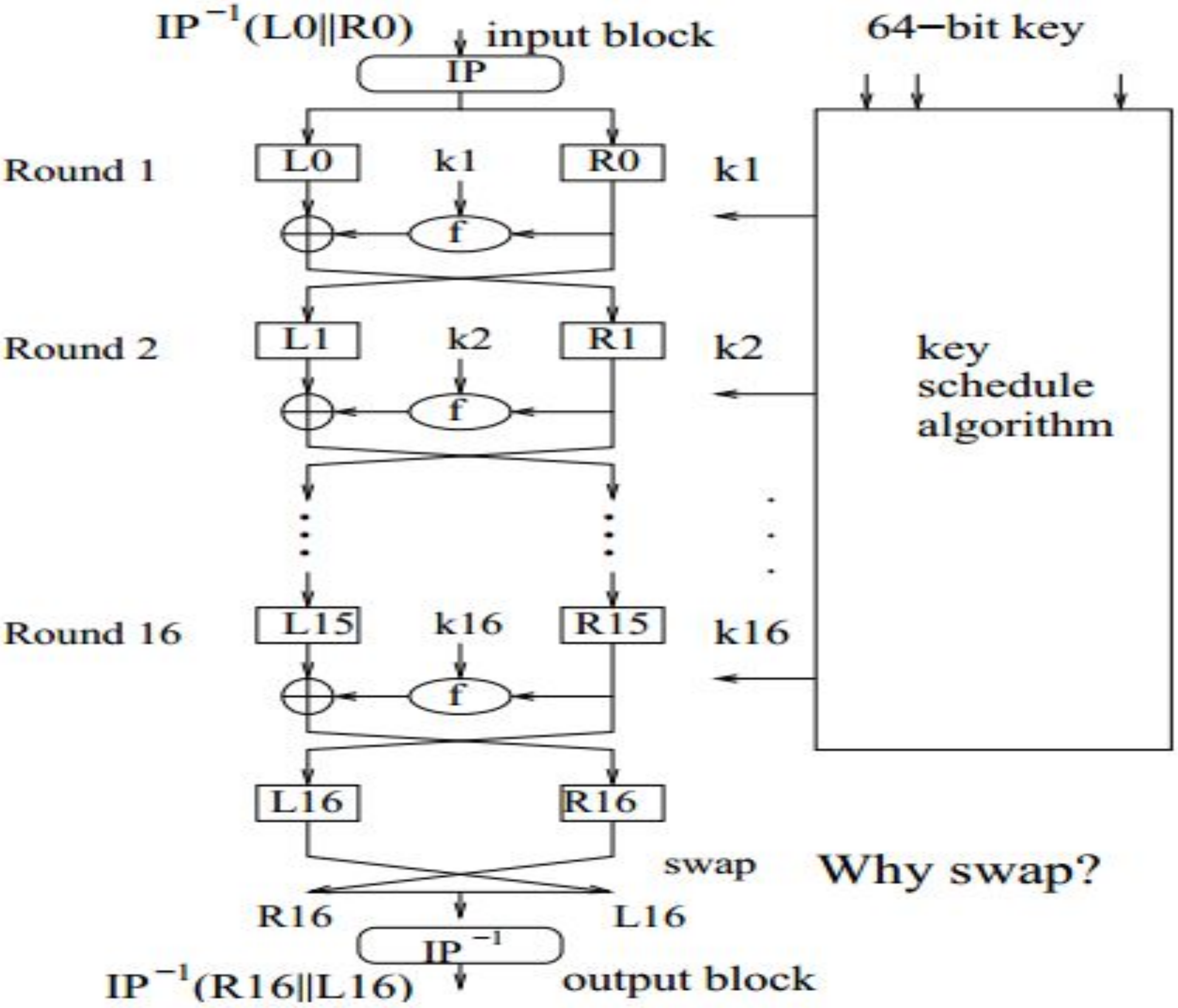
Secret-Key Encryption Protocols

1. Data Encryption Standard (DES)

2. Advanced Encryption Standard (AES)

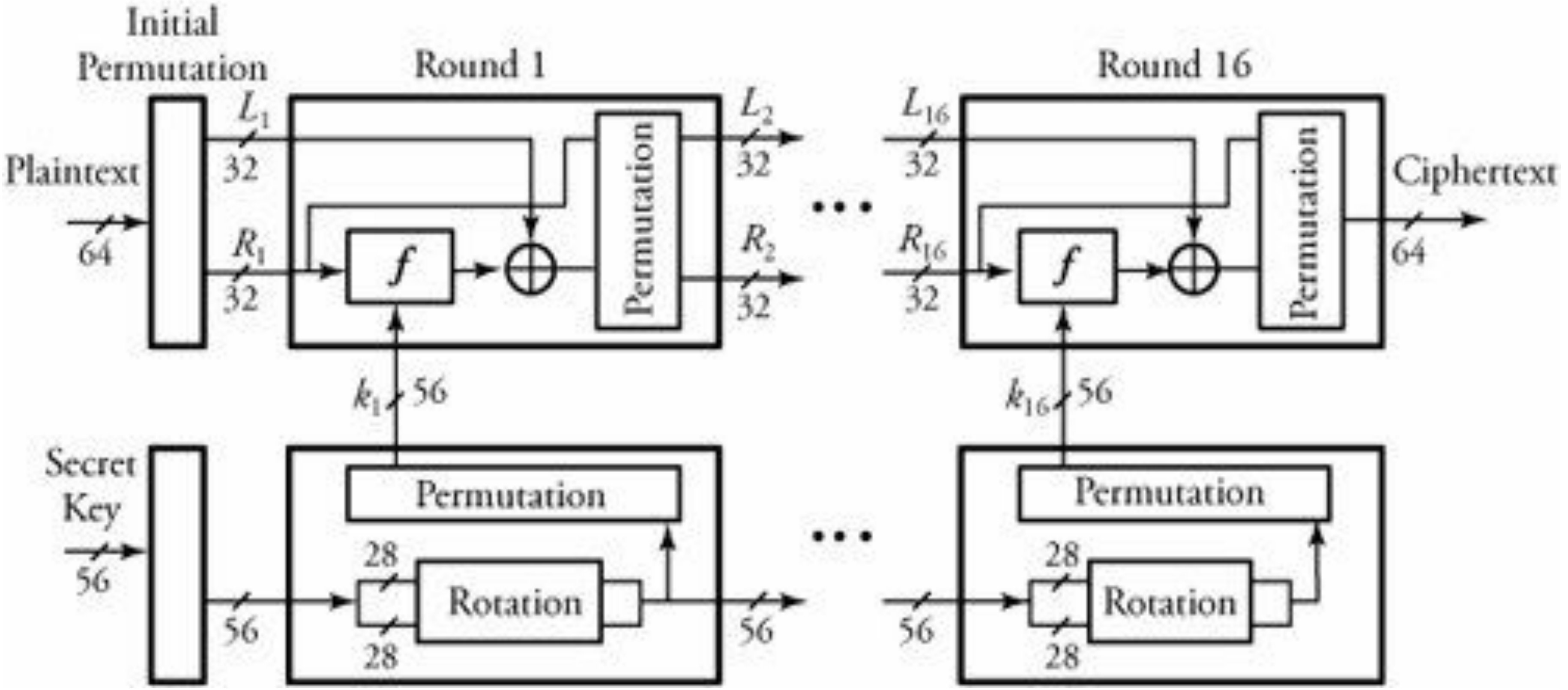
1. Data Encryption Standard (DES) Algorithm:

- Private Key encryption algorithm and hence uses single key for encryption and decryption process
- Block cipher generation method and processes 64 bit block at a time
- Uses 56 bit encryption Key
- Works in 16 rounds
- Applies Permutation and substitution approaches and bit level XOR operation


IP^{-1}(L0||R0)
input block
64−bit key
IP
Round 1
L0
k1
R0
k1
f
Round 2
L1
k2
R1
k2
f
key
schedule
algorithm
Round 16
L15
k16
R15
k16
f
L16
R16
swap
R16
L16
IP^{-1}
IP^{-1}(R16||L16)
output block

Why swap?

Working of DES (As given in the text book)



- Messages are converted into 64-bit blocks, each encrypted using a key.
- Each incoming 64-bit message is broken into two 32-bit halves denoted by Li and Ri, respectively.
- The 56 bits of the key are also broken into two 28-bit halves, and each half is rotated one or two bit positions, depending on the round.
- All 56 bits of the key are permuted, producing version ki of the key on round i.
- The 32-bit Ri-1 is expanded from 32 bits to 48 bits so that it can be combined with 48-bit ki. The expansion of Ri-1 is carried out by first breaking Ri-1 into eight 4-bit chunks and then expanding each chunk by copying the leftmost bit and the rightmost bit from left and right adjacent chunks, respectively.
- Function F() also partitions the 48 bits of ki into eight 6-bit chunks.

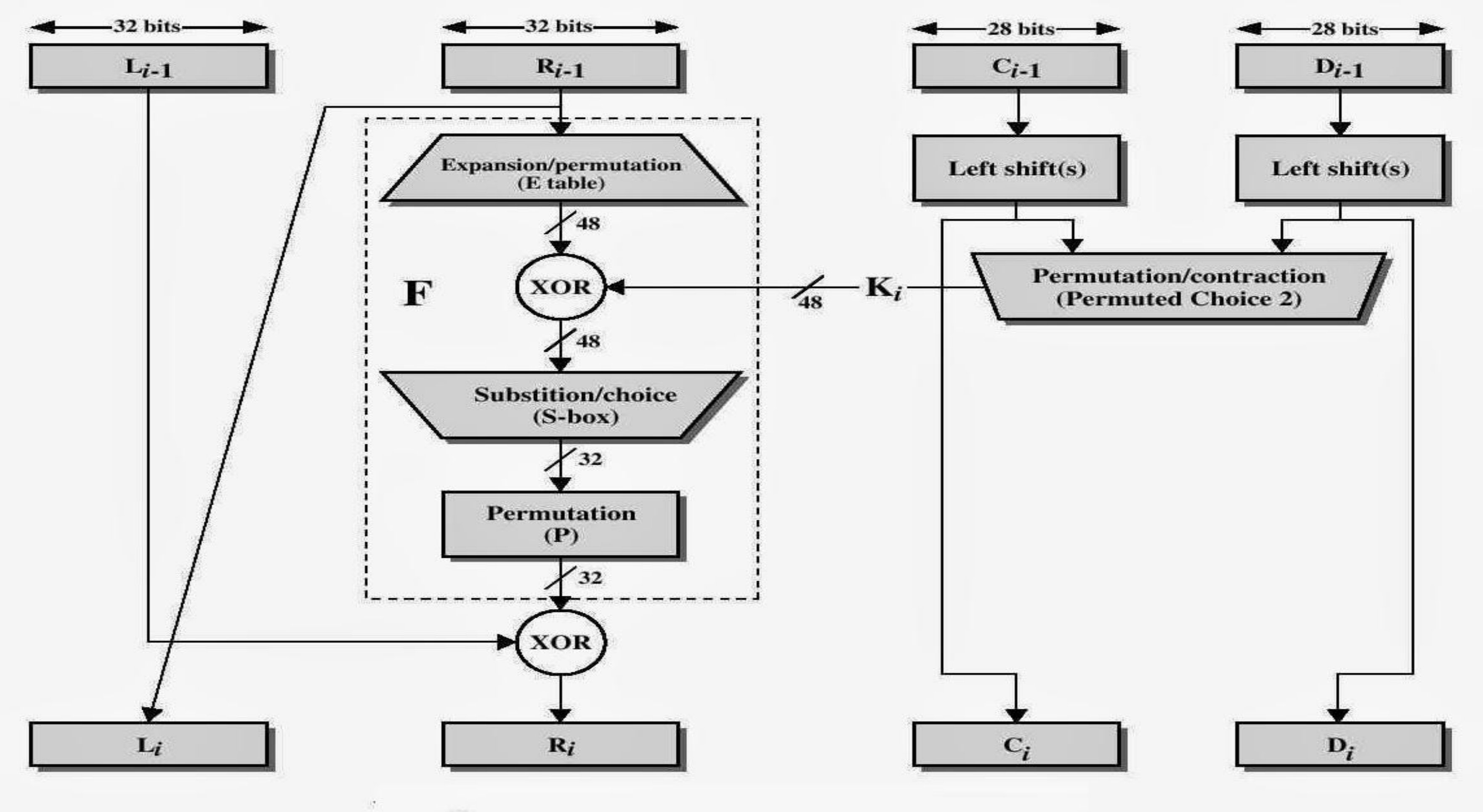
- Function F() also partitions the 48 bits of ki into eight 6-bit chunks.
- Then, Li and Ri are determined by

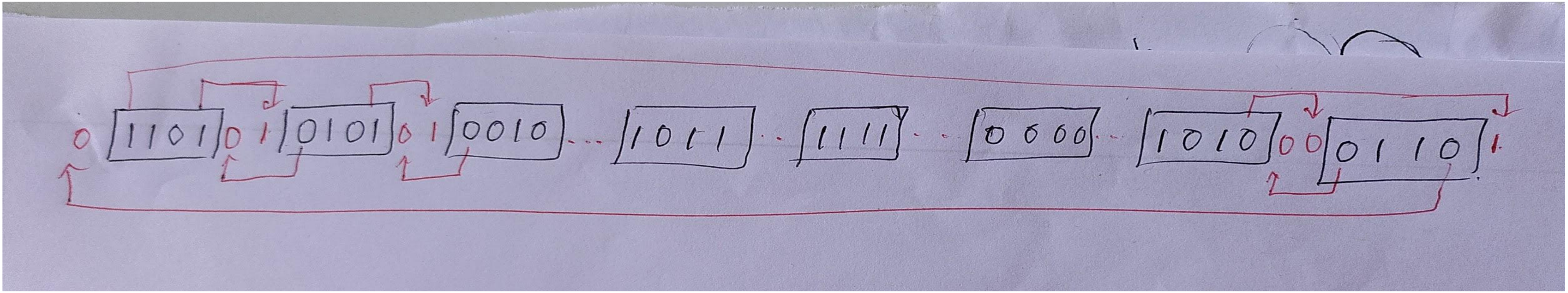
$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i).$$

-
- All 64 bits of a message are permuted.
- Same operation will be repeated for 16 rounds.
- The left and right blocks of 32 bits are swapped to get final cipher text for the block
- At the receiver, the same steps and the same key are used to reverse the encryption (Decryption process).

Working of single round in DES



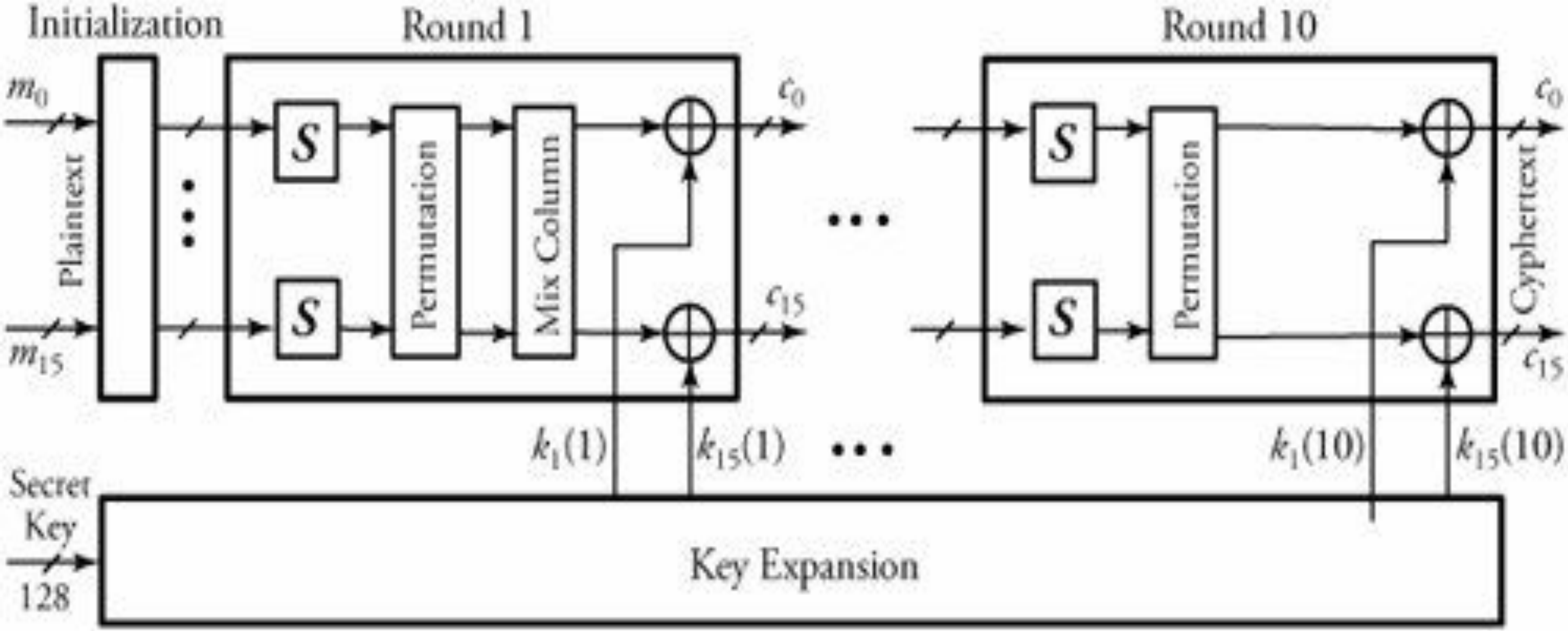


Exam Question:

With a neat diagram, explain the working of DES encryption algorithm [10M]***

Advanced encryption Standard (AES)

- AES is a private key encryption algorithm
- AES supports 128-bit symmetric block messages and uses 128-, 192-, or 256-bit keys.
- The number of rounds in AES is variable from 10 to 14 rounds depending on the key and block sizes.
- Figure given below, illustrates the encryption overview of this protocol,
- using a 128-bit key.


Initialization
Round 1
Round 10
m_0
m_{15}
Plaintext
S
S
Permutation
Mix Column
c_0
c_{15}
S
S
Permutation
Cyphertext
c_0
c_{15}
$k_1(1)$
$k_{15}(1)$
$k_1(10)$
$k_{15}(10)$
Secret Key
128
Key Expansion

Overview of Advanced Encryption Standard (AES) protocol

- There are ten rounds of encryptions for the key size of 128 bits.
- All rounds are identical except for the last round, which has no mix-column stage.
- A single block of 128-bit plaintext (16 bytes) as an input arrives from the left.
- The plaintext is formed as 16 bytes m0 through m15 and is fed into round 1 after an initialization stage.
- In this round, substitute units indicated by S in the figure perform a byte-by-byte substitution of blocks.
- The ciphers, in the form of rows and columns, move through a permutation stage to shift rows to mix columns.

- At the end of this round, all 16 blocks of ciphers are Exclusive-ORed with the 16 bytes of round 1 key k0(1) through k15(1).
- The 128-bit key is expanded for ten rounds.
- The AES decryption
- algorithm is fairly simple and is basically the reverse of the encryption algorithm at each stage of a round.

Exam Question:

Explain how to generate the cipher text using AES encryption algorithm?[10M]***