Security:

Prevention of System Collapse due to intended actions or unintended actions.

Security stages:

- **Identification**: identify username/email.
- **Authentication**: authenticate user accessing tool ex: password, fingerprint etc.
- **Authorization**: authorizing user authority, rights.
- **Auditing/Logging**: recording user since logging in.

Give five computer security Principles.

Default to Access Denial. **Non-Secret Design.** **User Acceptability.**

Least Privilege. **Separation of Privilege.** **Economy of Mechanism.**

Complete Mediation. **Least Common Mechanism.**

Give a logical strategy to crack any system use a password as an authentication method.

Try default password.

Try all short password from 1:3 char long.

Try system one line direction 160000 word.

Collect information about user hobbies, family name, birthday.

Try all legitimate license.

Try etrojon horse.

Sniffer ⟶ Tap

Why logical operation XOR is the only one used throughout all cryptography ?

Imagine you have a string of binary digits 10101 and you XOR the string 10111 with it you get 00010

now your original string is encoded and the second string becomes your key if you XOR your key with your encoded string you get your original string back.

XOR allows you to easily encrypt and decrypt a string, the other logic operations don't.

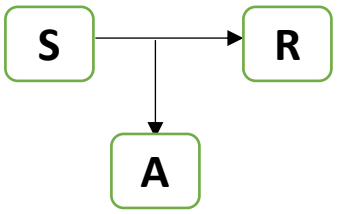
If you have a longer string you can repeat your key until its long enough for example if your string was 1010010011 then you'd simple write your key twice and it would become 1011110111 and XOR it with the new string

Three Classes of Intruders:

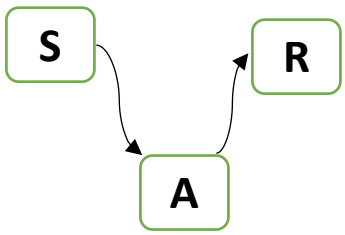
- **Masquerader – unauthorized user who penetrates a system exploiting a legitimate user's account *(outside)***
- **Misfeasor - legitimate user who makes unauthorized accesses or misuses his privileges *(inside)***
- **Clandestine user - seizes supervisory control to evade auditing and access controls or suppress audit collection *(inside|outside)***

Threads of attack between sender and receiver:

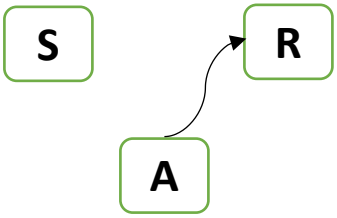
1.Interception: takes a copy from the massages.



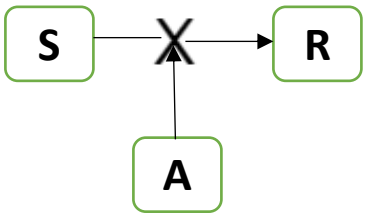
2. **Modification**: makes changes to the original messages.



3.Fabrication: Sending a fabricated message to the receiver.



4.Interruption: Prevents the messages from the sender to the receiver.



K = key **P= plaintext** **C= cyphertext** **N= number of characters**

Caesar encryption:

Encryption: C = (P+ K) Mod N **Decryption: P = (C - K) Mod N**

Transposition Algorithm:

We just create a matrix, the columns in it is the number of characters in the key, and we fill the cells with the key and complete the rest of the cells using the **Plaintext**, and if cells remain in the last row, we complete them in alphabetical order (A, B, C . . ,Z).

PlayFair Algorithm:

We just create a matrix and fill the cells with the key and the remaining cells we fill it using the alphabet as long as no letter is repeated.

Affine Algorithm:

Encryption: C = (Mp+K) Mod N **Decryption:** P = M^{-1}*(C-K) Mod N

Hill cipher:

Encryption:

$$\begin{bmatrix} C1 \\ C2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} P1 \\ P2 \end{bmatrix} \text{ Mod N}$$

Decryption:

$$\begin{bmatrix} P1 \\ P2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} * det^{-1} * \begin{bmatrix} c1 \\ c2 \end{bmatrix} \text{ Mod N}$$

Diffie-Hellman Setup

public key:

$y_A = \alpha^{xA} \bmod q$

Shared key for users A & B is K:

K = y_A^{xB} mod q (which **B** can compute) K = y_B^{xA} mod q (which **A** can compute)

RSA:

- Generate **2** large prime numbers (**P**, **Q**)
- Calculate **(n)** = P*Q
- Calculate **(z)** = (P-1) *(Q-1)
- Assume **(e)** but should be relatively prime (GCD between them = 1) with **(z)**
- Calculate **D =** e^{-1} **Mod z**

Encryption: C = P^e **mod N** **Decryption:** P = C^d **mod N**

What are the main features of Data encryption standard (DES)?

Symmetric key.

Easy to implement.

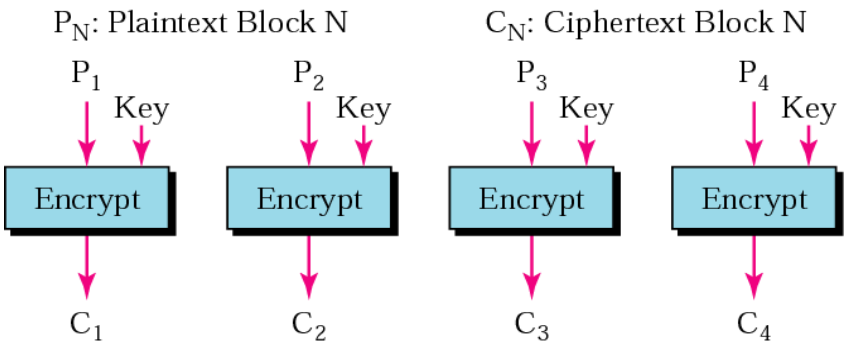
Use storage encryption algorithm.

Block cipher.

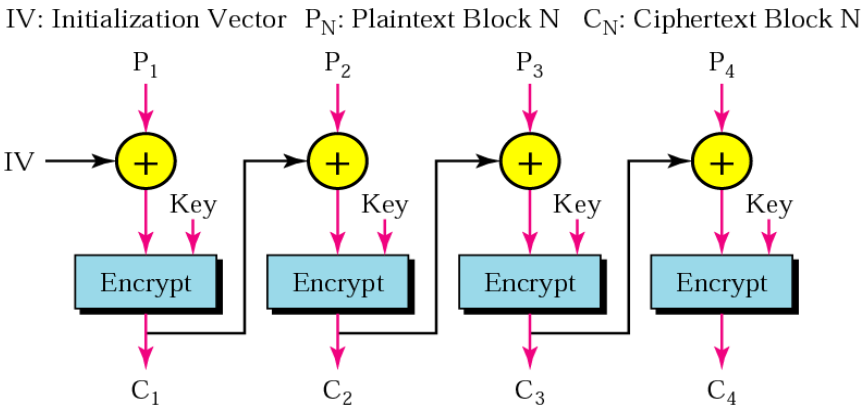
Use X-or operation.

DES Operation Modes:

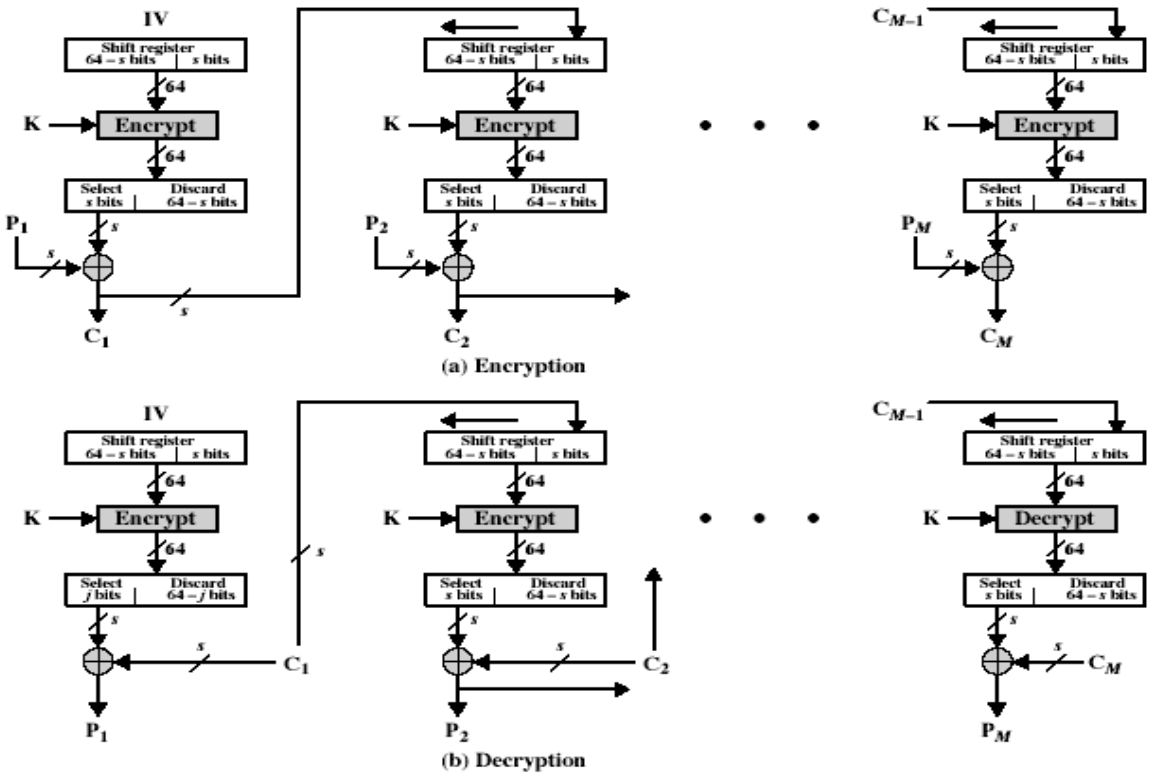
- **ECB**



- **CBC**



- **CFB**



MD2 & MD5 Padding:

MD2 Padding

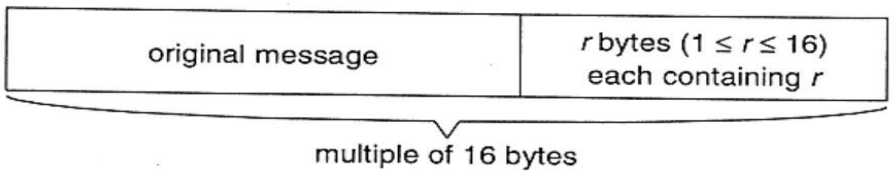
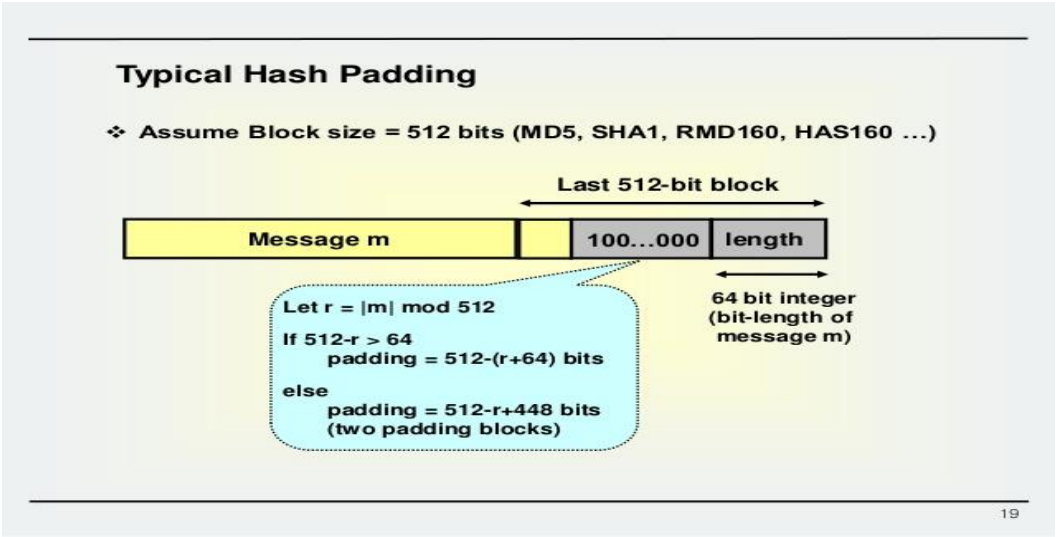


Figure 5-3. MD2 Padded Message

21



Types of firewall:

Packet Filters –

It works in the **network layer** of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.

For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to 'discard all packets' or to 'accept all packets.

Application Gateways –

It is also known as **Proxy server**. It works as follows:

Step-1: User contacts the application gateway using a TCP/IP application such as HTTP.

Step-2: The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.

Step-3: After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

Stateful Inspection Firewalls –

It is also known as ‘Dynamic Packet Filters’. It keeps track of the state of active connections and uses this information to decide which packets to allow through it, i.e., it adapts itself to the current exchange of information, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.

Circuit-Level Gateways –

It works at the **session layer** of the OSI Model. It is the advanced variation of *Application Gateway*. It acts as a virtual connection between the remote host and the internal users by creating a new connection between itself and the remote host. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world.