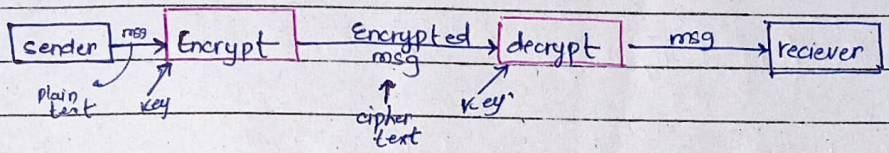
Introduction: The art of protecting information by transforming it into an unreadable format is known as cryptography.

OR

It is a method of protecting information through the use of codes so that only those for whom the information is intended can read & process it.

More generally, cryptography is about constructing & analyzing protocols that prevent 3rd parties or public from reading private message.

- Thus to provide security & protect the valuable info, we use cryptography.



Encryption: Process of transforming information from readable to unreadable format.

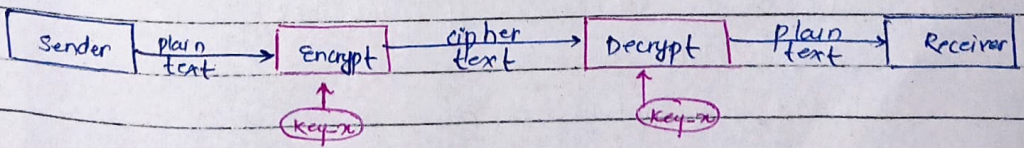
Decryption: Process of transforming information from unreadable to readable format.

Key: string of bits used by cryptographic algo. to transform plaintext to cipher text or vice versa.

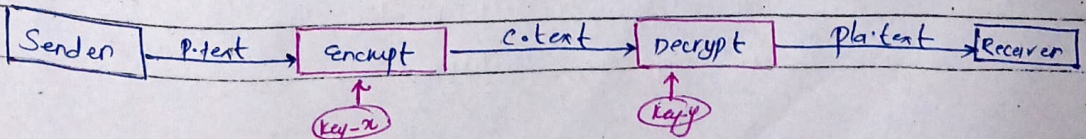
- There are 2 types of cryptography.

(i) **Symmetric Cryptography:** It is the simplest kind of encryption technique that involves only 1 key to encrypt & decrypt the information. It is also known as secret key cryptography.

(ii) **Asymmetric Cryptography:** It is a kind of encryption technique that uses 2 keys (or a pair of keys) for encryption & decryption of the information. It is also known as public key cryptography.



(i)



(ii)

Symmetric Crypto...	Assymetric crypto...
• Also called private or secret key cryptography	• Also called public key cryptography.
• Only 1 key is used for encryption & decryption	• 2 keys are used for encryption & decryption
• Faster in execution	• Slower in execution.
• Less complex	• More complex
• Less computational power req.	• More computational power req.

Security Goals: In cryp... security goals are designed to ensure that data is protected from unauthorized access, tampering & misuse. Main security goals are:

- Confidentiality: It ensures that info... is accessible only to authorized users.
- Integrity: It ensures that the data has not been altered during transmission
- Authentication: It confirms the identity of the sender
- Availability: It ensures that data & services are accessible when needed.

Attacks on Computer & Computer Security

A computer attack is when someone tries to break into a computer or harm it. These attackers may want to:

- Steal your data
- Damage your system

So, these attacks can result in the loss of data, financial damage & even system failure.

Computer security is about protecting your computer & data from these attacks with the help of

- Strong passwords.
- Firewall
- antivirus software
- And encryption

Need For Security:

In today's digital world, the use of computers, mobiles & internet has grown rapidly. As a result a large amount of sensitive inform- is stored & transmitted electronically over internet. This creates a strong need for security to protect this info- from misuse.

Security Approaches.

SA refers to the methods & strategies used to protect computer systems, networks & data from unauthorized access.

Below are main security approaches:

- Preventive Approach: This approach focuses on stopping attacks before they happen. It includes using firewalls, antivirus s/w etc
- Detective Approach: This approach aims to detect attacks when they occur. It uses tools like intrusion detection technique, monitoring s/w etc
- Corrective Approach: This approach deals with fixing problems after an attack or failure has occured. It includes restoring data from backups.

Attack & Types of Attack.

An attack is any attempt to damage, steal or gain unauthorized access to data or systems.

There are 2 different types of attacks.

1. Passive Attack: These attacks try to monitor or steal data without altering it. The goal is to all gather sensitive information secretly.

We can prevent it using better encryption techniques

Types of passive attacks.

- Eavesdropping: Listening to private communication like emails or messages.
- Traffic analysis: Studying the pattern of communication to guess sensitive info.

2. Active Attacks: Active attacks try to modify, delete or disrupt data or systems. They are more dangerous than passive attacks

Types of AA.

- Masquerade Attack: Attacker pretends to be someone else identity
- Replay Attack: A valid message is captured & sent again to trick the system.
- Modification Attack: Altering data in transit to mislead or harm the receiver.

Principles of Security

The principles of security refer to the fundamental concepts used to protect data & computer system from threats such as unauthorized access.

Following are principles of security

- confidentiality
- Integrity
- Availability
- Authentication

} Already Defined.

- Non Repudiation: Ensures that a sender can't deny sending a message or performing an action

* Rail Fence Cey Cipher: It is a type of transposition cipher. It works by writing the message in a zigzag pattern across multiple "rails" (rows) & then reading the message row by row to create cipher text

eg ~~Rail~~ Plaintext → 'All the best'

Row 1 : A - l - h - b - s
Row 2 : - l - t - e - e - t

] encrypted msg = Alhbslteet

..

Symmetric key Algo.

Intro: Symmetric key crypto.. is a method of encryption in which the same key is used for both encrypting & decrypting data. It is also called secret key cryptography. This type of encryption is very fast & efficient.

Symmetric key Algo. are mainly classified into 2 types

- Block ciphers: It encrypt data in fixed size blocks such as 64 or 128 bits

- Stream ciphers: It encrypt data bit by bit or byte by byte in a continuous stream

Symmetric key crypto.. is widely used in various security applications like file encryption, decryption & secure communication.

Data Encryption Standard (DES)

DES is one of the earliest symmetric key algo. It is a block cipher that encrypts data in 64 bit blocks using a 56 bit key. The algo follows a structure known as the Feistal network, where data is divided into 2 halves & passed through multiple round of processing.

- DES performs 16 rounds of encryption and in each round, complex operation such as permutation, substitution & bitwise operations are applied
- Initially the 64 bit plaintext undergoes an initial permutation, & then it is divided into left and right halves

- These halves are processed through 16 rounds where a unique 48 bit subkey is used in each round.

- After 16 rounds, the two halves are combined & passed through a final permutation to produce 64 bit ciphertext.

International Data Encryption Algorithm (IDEA).

IDEA is a symmetric key block cipher algo. IDEA operates on 64 bit blocks of plaintext and uses a 128 bit key for both encryption & decryption, providing much stronger security.

- IDEA encryption involves 8.5 rounds.
- Each of first 8 round consists of modular addition, multiplication and xor operations
- These operations are performed on 16 bit sub-blocks of 64 bit input blocks.
- The final half round performs only a few operations to complete encryption process

One of the key features of IDEA is that it uses 52 sub keys derived from 128 bit original key. These subkeys are generated and applied at diff. stages of encryption & decryption processes.

IDEA a powerful & secure symmetric encryption algo, that played a significant role in the evaluation of modern cryptographic systems.

Rivest Cipher 5 Algo (RC5)

RC5 is a fast and flexible symmetric key block cipher. It is known for its simplicity, speed and configurability. RC5 allow users to choose parameters such as blocksize, key size, and number of rounds, which makes highly adaptable to diff. level of security requirements.

- RC5 operates on data blocks of variable size commonly 32, 64 or 128 bits with 64 bit being the most frequently used.

- It supports key sizes ranging from ~~0 to 200~~. 0 - 2040 bits.
- In this algo no. of rounds can be varied from 12 - 16
- The algo uses 3 simple operations: modular addition, bitwise XOR and data dependent rotations.

The structure of RC5 is based on a Feistel like network, and it consists of 3 main stages: key expansion, encryption & decryption.

- In key expansion phase, the input key is expanded into a set of subkeys using a key schedule algo.

During encryption the plaintext is divided into 2 halves, and each round transforms the data using subkeys & basic operations.

The decryption process simply reverses the encryption using same set of keys.

Digital Signature.

A DS is a cryptographic technique used to validate the authenticity and integrity of message, s/w or document. It works like a handwritten signature, but it is much more secure & based on mathematical algo.

A DS sign.. uses assymetric crypto.. which involves a pair of keys: a private key and a public key. The sender signs the msg using their private key, and receiver varifies the sign.. using the sender's public key.

DS are often generated by first creating a message digest which is then encrypted with the sender's private key to form the signature.

DS provides authentication, integrity & non-repudiation meaning the sender can't deny sending the msgs.

Internet Security Protocol are a set of rules and standards design to protect data during transmission over the internet. They ensure confidentiality, integrity & authentication of data.

common protocols include

- SSL / TLS : (Secure Socket Layer / Transport layer Security) Ensures secure communication b/w web browsers & servers by encrypting data.

- HTTPS : A secure version of HTTP that uses SSL/TLS to protect website data.

- SSH : Provide secure access to remote computers by encrypting login and file transfer sessions.

User Authentication is the process of verifying the identity of a user before granting access to a system or service. It ensures that only authorized users can access sensitive info.

common authentication methods are:

- Password based authentication : In this the user enters a secret password to gain access.

- Biometric auth-- : Uses physical traits like fingerprints, face or iris to verify identity.

- 2FA : Combines 2 methods such as a password & a mobile OTP for security.

- Token based auth-- : Uses digital tokens or smart cards for access.

Firewall : It is a network security device or s/w that monitors and controls incoming & outgoing n/w traffic based on predetermined security rules. It acts as a barrier b/w a trusted internal network and an untrusted external network.

The primary goal of a firewall is to prevent unau---. access to or from a private network.

Types

Packet Filtering Firewall : It checks data packets against a set of filters such as IP addresses, port no. & protocols. It is fast but offers limited protection.

Stateful Inspection Firewall : It monitors the state of active connections and makes decision based on content of traffic.

Application Level Gateway : (Proxy Firewall).
It works at application layer & filters traffic for specific applications like HTTP or FTP. It provides strong security but may reduce speed.

Firewall Configurations define how a firewall operates in a n/w
The main configurations include:

- Screened Host Firewall Uses a bastion host & a screening router to separate the internal n/w from internet
- Dual-Homed Host Firewall: The firewall has 2 network interfaces, one for the internal n/w & one for external creating a physical separation.
- DMZ : Introduces an extra n/w b/w internal & external n/w to host public-facing services, increasing overall security.

Pretty Good Privacy is a data encryption and decryption ~~and decryption~~ sw used to provide privacy, security and authentication for digital communication. PGP uses a combination of symmetric key encryption for speed and assymetric encryption for secure key exchange. It also uses hash functions to create digital signatures.

Diffie-Hellman Algo.

The DH algo is a method of securely exchanging cryptographic keys over a public communication channel. DH is used in assymetric cryptography, but it doesn't provide encryption or authentication on its own. Instead it allows two users to agree on a shared secret key that can later be used for symmetric encryption.

→ working.

~~Publicly shared information~~

Let assume two users A & B.

S1. Both publicly shared parameters. They both agree on a no, a large prime no p and a primitive root g of p.

S2. Each users select a private key.

User A selects a private key 'a'

—— B —————— 'b'

S3. Each user computes their public key using formula.

User A computes : $A = g^a \bmod p$

—— B —— : $B = g^b \bmod p$

S4. Each user uses the others public key to compute the shared secret

User A computes : $K = B^a \bmod p$.

—— B —— : $K = A^b \bmod p$.

Mathematically both values will be equal.

Kerberos Protocol

Kerberos is a network authentication protocol designed to provide secure authentication b/w users & services over an insecure network. The main goal of kerberos is to ensure that passwords are never transmitted over network & both users & servers can verify each other's identity.

Kerberos is based on symmetric key cryptography & uses a trusted 3rd party called key Distribution Centre. The KDC consist of 2 parts: Authentication Server (AS) & Ticket Gathering server (TGS).

→ Working

S1 The user logs in & sends a request to AS

S2 The AS verifies credentials & sends back a TGT

S3 The user sends the TGT to TGS & request access.

S4 If TGT is valid, TGS send back a ST (service Ticket).

S5 The user presents the ST to server.

S6 The server decrypts it & allow access

Vigenere Cipher

It is a polyalphabetic substitution cipher. The encryption is done using a (26x26) matrix or table.

ML Vigenere Table.

Plain Text = GIVE MONEY

key = LOCK.

sol"

P G I V E M O N E Y

K L O C K L O C K L

→ Repeat letters of key so that no. of letters in P & K becomes equal

Now cipher is RWXOXCPOJ → This is obtained using vigenere table that will be given in Q.

For decryption.

cipher → R W X O X C P O J.

keys → L O C K L O C K L

Plain → G I V E M O N E Y

Caesar Cipher

It is also called shift cipher / additive cipher. Each letter in the text is replaced by a letter corresponding to a no of shifts in the alphabet.

eg. Plain = MEAT , key = 3

→ cipher = PHDW

where,

ciphertext, $C = E(K,P) = (P+K) \bmod 26$ // for encryption

$P = D(K,C) = (C-K) \bmod 26$ // for decryption

Note: Plain = M, key = 3, cipher = M+3 = P

cipher = P, key = 3, plain = P-3 = M.

How to write in exam.

Plain text = "HELLO" , key = 4.

C(H) = (P+K) mod 26 = (7+4) mod 26 = 11 = L

C(E) = (P+K) mod 26 = (4+4) mod 26 = 8 = I.

C(L) = ——— = (11+4) mod 26 = 15 = P

C(O) = ——— = (14+4) mod 26 = 18 = S

∴ cipher = LIPPS

→ Now, decryption. P = (C-K) mod 26

P(L) = (L-4) mod 26 = (11-4) mod 26 = 7 = H

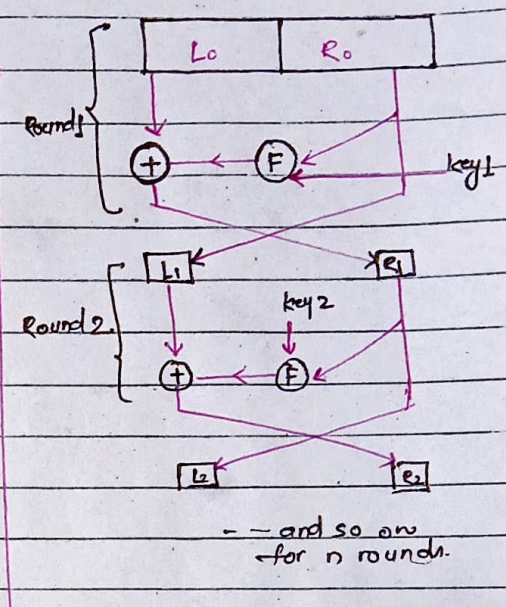
→ and so on

∴ plaintext = HELLO

Fiestel Cipher Structure

Most of the block cipher structure technique follow this structure. The plain text is divided into 2 equal halves L_0 & R_0. The halves of data pass through n rounds of processing & then combine to produce the cipher text.

On the right half we apply a fn & is the fn we will use a subkey generated from master key. The o/p of this is xored with the left half & then their o/p will be swapped.



Authentication : // Define //

Types of Authentication

- Message Encryption
- MAC (Message Authentication Code)
- Hash Functions.

MAC

A MAC is a short piece of info... used to verify the integrity & authenticity of a message. It ensures that the message has not been altered & that it comes from the claimed sender.

→ working

S1. Sender computes the MAC using the message & secret key.
S2. Sender sends both the msg & MAC to the receiver.
S3. Receiver recomputes the MAC using the received msg & same key.
S4. If computed MAC matches the received MAC, the msg is authentic & unaltered.