ENCRYPTION AND DECRYPTION

Dr.R.SUGANYA

DEPARTMENT OF COMPUTER SCIENCE WITH CYBER SECURITY

Encryption and Decryption

Encryption and decryption are essential processes in cybersecurity. Encryption converts data into an unreadable format, protecting sensitive information from unauthorized access. Decryption reverses this process, making the data accessible again.

Symmetric-Key Encryption

1 **Single Key**

Both encryption and decryption use the same secret key.

2 **Fast and Efficient**

Suitable for high-volume data encryption.

3 **Key Management**

Securely storing and distributing keys is crucial.

4 **Examples**

AES (Advanced Encryption Standard), DES (Data Encryption Standard).

Asymmetric-Key Encryption

Public Key

Used for encrypting data, freely shared.

Private Key

Used for decrypting data, kept secret.

Digital Signatures

Ensures data integrity and sender authenticity.

Encryption Algorithms

1. **Substitution Ciphers**

   Replace characters with others, Caesar cipher.

2. **Transposition Ciphers**

   Rearrange the order of characters, Rail Fence cipher.

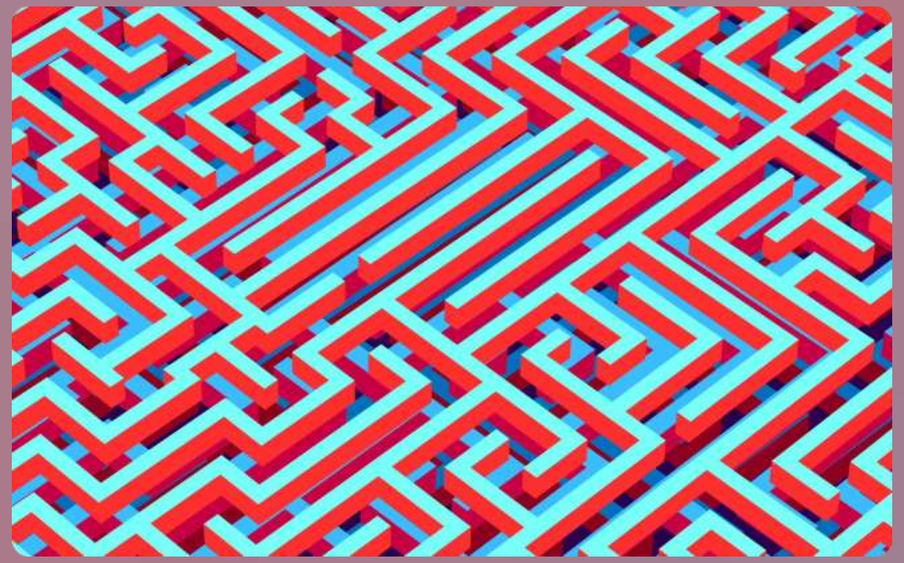
3. **Modern Block Ciphers**

   Operate on fixed-size blocks of data, AES, DES.

4. **Stream Ciphers**

   Encrypt data bit-by-bit, RC4, Salsa20.

Encryption Modes



1. **Electronic Codebook (ECB)**
   Encrypts each block independently, vulnerable to attacks.
2. **Cipher Block Chaining (CBC)**
   Links blocks together, improving security but introducing IV.
3. **Cipher Feedback (CFB)**
   Encrypts data bit-by-bit, suitable for stream encryption.
4. **Output Feedback (OFB)**
   Generates a keystream, suitable for stream encryption.

$$e^{i\pi}+1=0$$

Hashing Algorithms

One-way function	No decryption possible
Fixed-size output	Same input always produces same hash
Collision resistance	Difficult to find two inputs with same hash

Applications of Encryption

Secure Communication

Protects data transmitted over networks.

Data Storage

Secures sensitive information stored on devices.

Financial Transactions

Protects payment information during online transactions.

Email Security

Ensures confidentiality and integrity of emails.

Best Practices for Encryption

Strong Algorithms

Use robust encryption algorithms like AES or RSA.

Secure Key Management

Implement strong key generation, storage, and distribution practices.

Regular Updates

Keep software and algorithms updated to mitigate vulnerabilities.

Awareness and Training

Educate users about encryption best practices and security threats.

Decryption: Unveiling Secrets

The process of transforming encrypted data back into its original form.

by Dr.R.Suganya SNS

Decryption Methods

Symmetric Key

Uses a single key for both encryption and decryption.

Asymmetric Key

Uses separate keys for encryption and decryption.

Hashing

One-way process - irreversible decryption.

Symmetric Key Decryption

1

Key Exchange

Securely sharing the secret key.

2

Decryption Algorithm

Applying the key to the ciphertext.

3

Plaintext

Recovering the original data.

Asymmetric Key Decryption

1 **Public Key**

Used for encryption, widely shared.

2 **Private Key**

Used for decryption, kept secret.

3 **Digital Signatures**

Ensuring data integrity and authenticity.

4 **Key Management**

Managing private key security.

Hashing Decryption

Hashing is a one-way function, meaning decryption is impossible. It's used for data integrity checks and password storage.

Decryption Tools

Software

Dedicated applications for decryption.

Online Services

Web-based platforms for decryption.

Libraries

Code modules for decryption functions.

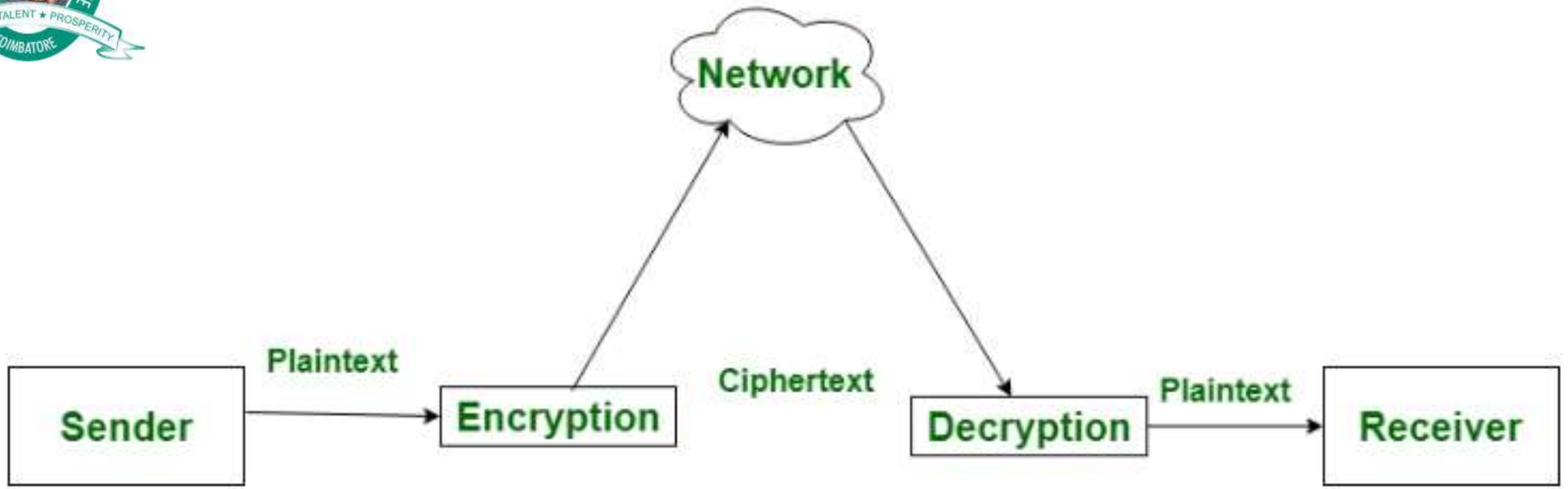
Decryption Challenges

Key Compromise	Unauthorized access to decryption keys.
Algorithm Weakness	Vulnerabilities in the decryption algorithm.
Computational Complexity	Demanding computational resources for decryption.

Difference between Encryption and Decryption

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that's undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.


Network
Plaintext
Sender
Encryption
Ciphertext
Decryption
Plaintext
Receiver

S.NO	Encryption	Decryption
1.	Encryption is the process of converting normal message into meaningless message.	While decryption is the process of converting meaningless message into its original form.
2.	Encryption is the process which take place at sender's end.	While decryption is the process which take place at receiver's end.
3.	Its major task is to convert the plain text into cipher text.	While its main task is to convert the cipher text into plain text.
4.	Any message can be encrypted with either secret key or public key.	Whereas the encrypted message can be decrypted with either secret key or private key.
5.	In encryption process, sender sends the data to receiver after encrypted it.	Whereas in decryption process, receiver receives the information(Cipher text) and convert into plain text.

6.	The same algorithm with the same key is used for the encryption-decryption process.	The only single algorithm is used for encryption-decryption with a pair of keys where each use for encryption and decryption.
	Encryption is used to protect the confidentiality of data by converting it into an unreadable form that can only be read by authorized parties.	Decryption is used to reverse the encryption process and convert the ciphertext back into plaintext.
	The output of encryption is a ciphertext that is unintelligible to anyone who does not have the decryption key.	The output of decryption is the original plaintext message.

1.In cryptography, what is cipher?
a) algorithm for performing encryption and decryption
b) encrypted message
c) both algorithm for performing encryption and decryption and encrypted message
d) decrypted message

2. In asymmetric key cryptography, the private key is kept by _____
a) sender
b) receiver
c) sender and receiver
d) all the connected devices to the network

3. In cryptography, the order of the letters in a message is rearranged by _____
a) transpositional ciphers
b) substitution ciphers
c) both transpositional ciphers and substitution ciphers
d) quadratic ciphers

4.What is data encryption standard (DES)?
a) block cipher
b) stream cipher
c) bit cipher
d) byte cipher

5.Cryptanalysis is used _____

a) to find some insecurity in a cryptographic scheme

b) to increase the speed

c) to encrypt the data

d) to make new ciphers

ANSWERS

1.a.
2b.
3.a.
4.a
5.a

THANK YOU