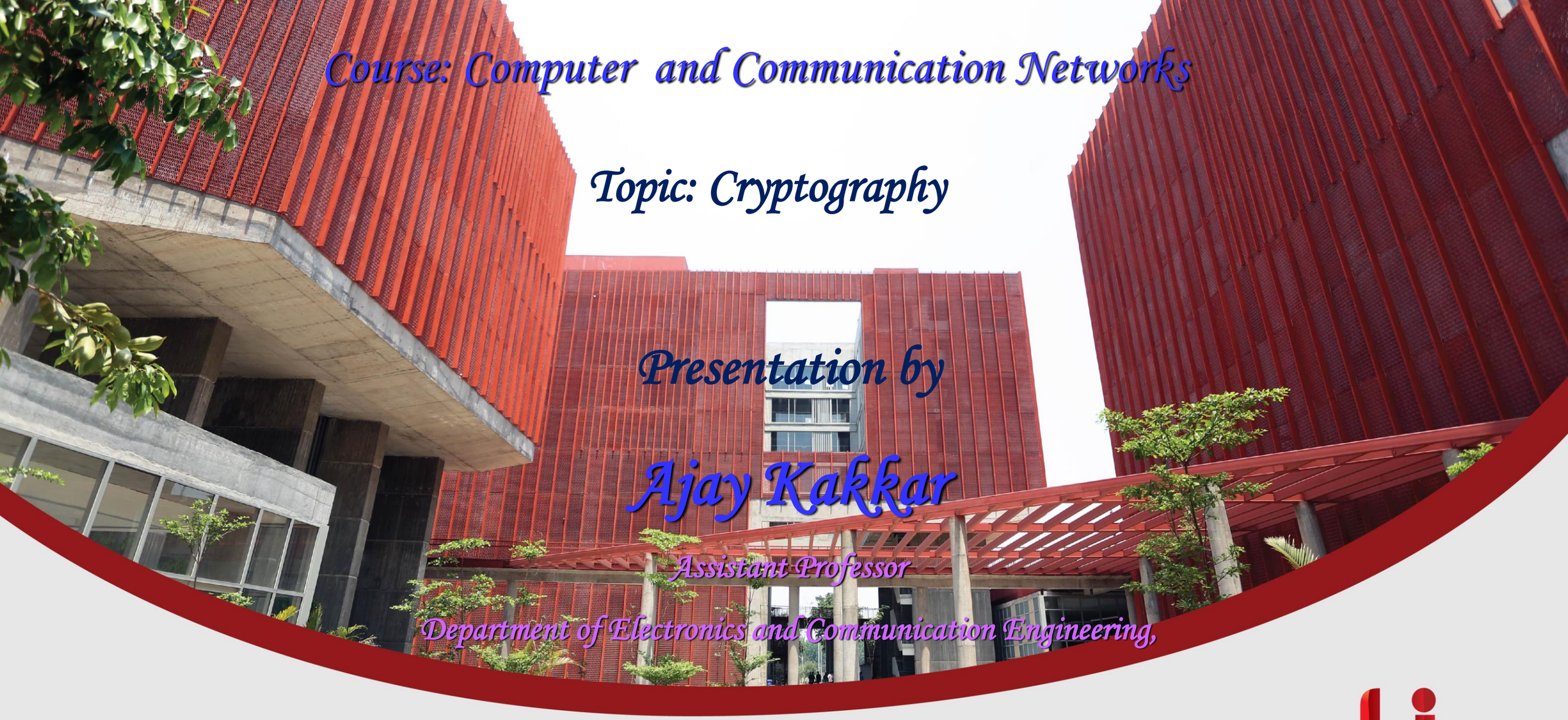


Course: Computer and Communication Networks

Topic: Cryptography

Presentation by

Ajay Kakkar

Assistant Professor

Department of Electronics and Communication Engineering,

Thapar Institute of Engineering & Technology
(Deemed to be University)
Bhadson Road, Patiala, Punjab, Pin-147004
Contact No. : +91-175-2393201
Email : info@thapar.edu

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

Cryptography

Data security is an essential component of an organization, industries and governments in order to keep their information safe from their competitors. Secured and timely transmission of data is always an important aspect for an organization.

•There is a need of secured data communication in defense, industries, universities, etc.

•Need for secured access to bank accounts and electronic transfers of funds.

•Requirement for secure E-commerce.

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

Methods for Secured Communication

There are various ways to achieve the secured communication. Such as; passwords, multiple passwords and cryptography.

Passwords:

Passwords are not treated as reliable for this task. It is easy to guess passwords due to its short range. The main difficulty in designing secure password mechanisms arises from the fact that password space is usually small and much easier to attack than random cryptographic keys.

Cryptography:

It is the best method of saving our documents from the competitor in business.

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

Introduction

Cryptography is a technique used to avoid unauthorized access of data.

Plaintext:

It is the original text before it is encrypted.

Cipher text:

It is the encrypted text. The text obtain after encoding the data with the help of a key is known as cipher text.

Key:

It is a word or value that is used to encrypt the plain text or decrypt the cipher text.

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

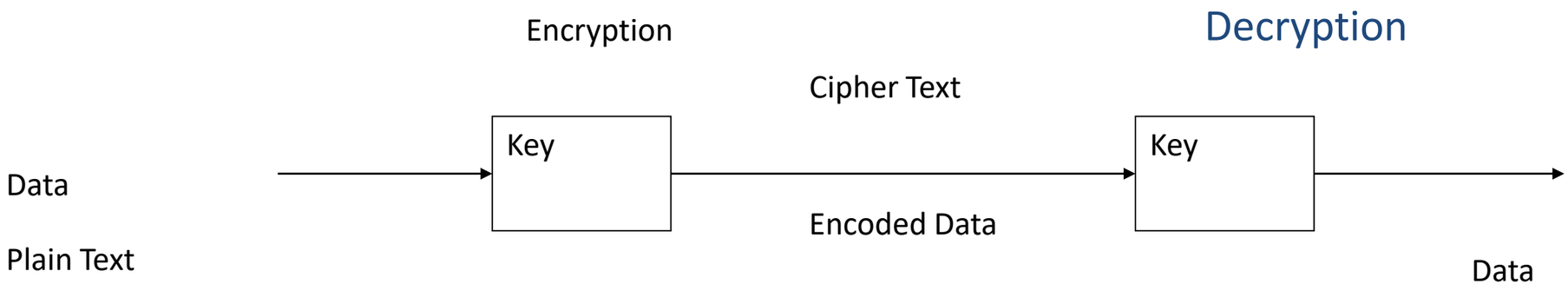
Introduction (Contd.)

Encryption:

The method of converting the data into coded form with the help of key is called encryption.

Decryption:

The method of converting the encoded data to the original form is called decryption.



Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

Type of Cryptography

Symmetric (Private) Cryptography:

•When **same** key is used to encrypt and decrypt the message then it is known as symmetrical key cryptography.

•It is effective and much **faster** as compared to asymmetrical key cryptography.

Asymmetric (Public) Cryptography:

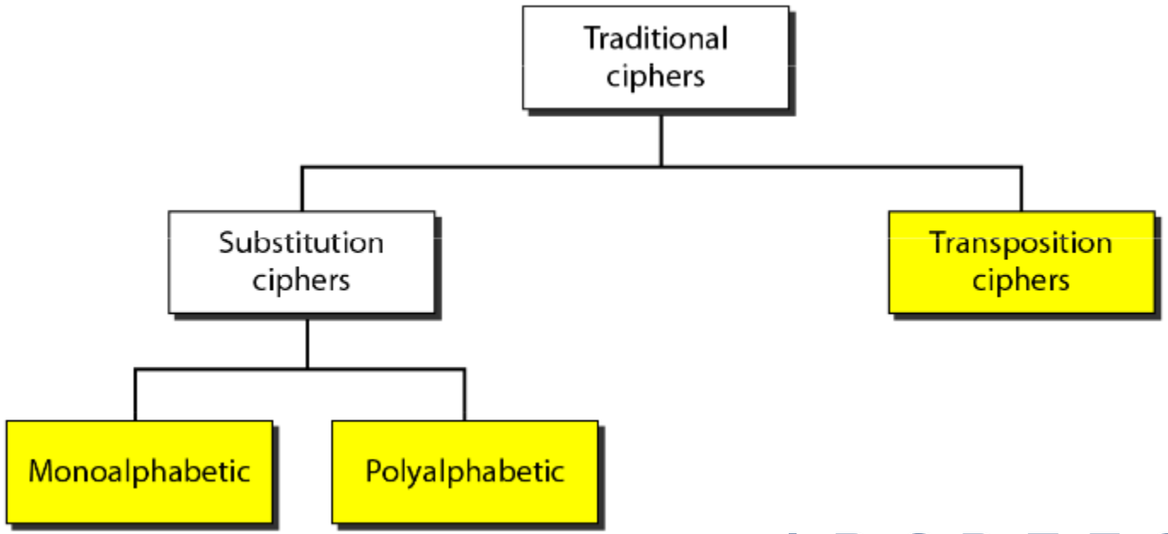
•Whitfield Diffie, Martin Hellman, and Ralph Merkle laid public key cryptography in June 1976.

•It uses different keys for encryption and decryption.

•It is more secure and at the same time consumes more time.

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

Symmetrical Cryptography



The shift cipher is sometimes referred as the has the **Caesar cipher.**

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

BOOK
FSSO

This type of arrangement is known as *substitution ciphers*.

monoalphabetic

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

Symmetrical Cryptography

In **monoalphabetic Cipher**, the relationship between a character in the plaintext and the characters in the ciphertext is **one-to-one**, whereas in **Polyalphabetic Cipher**, the relationship between a character in the plaintext and the characters in the ciphertext is **one-to-many.**

A	B	C	D	E
F	G	H	J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Plaintext:

MUST COME NOW

MU ST CO ME NO WX

Ciphertext:

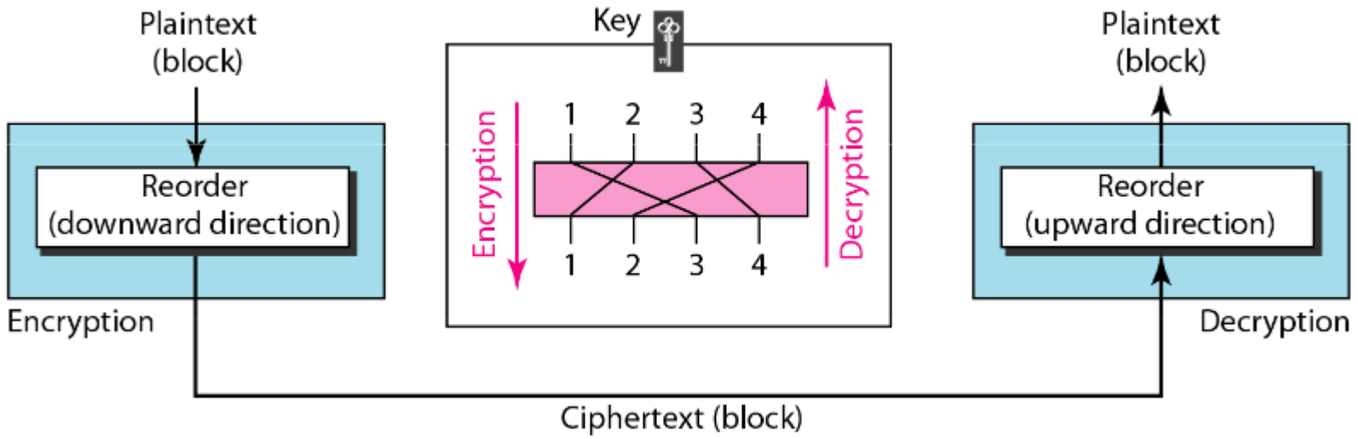
RP XY ND BP ST BC

RPXYN DBPST BC

Polyalphabetic cipher are based on substitution

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

Transposition cipher

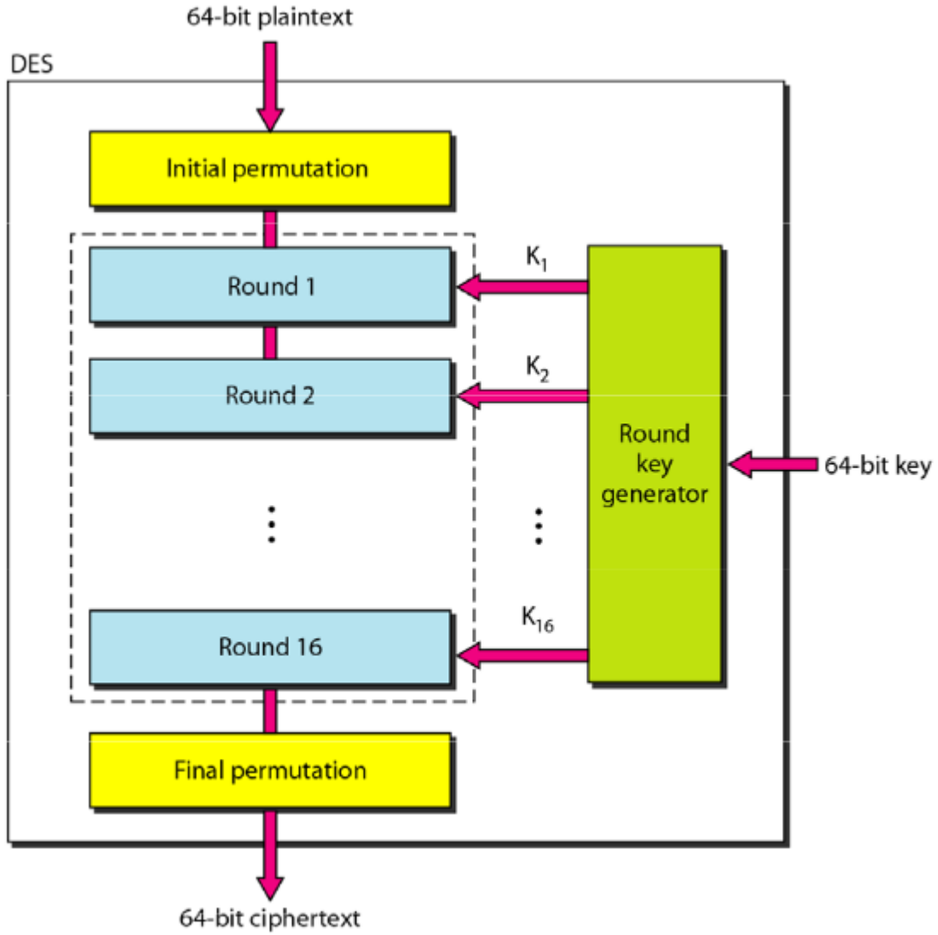


HELLO MY DEAR

We first remove the spaces in the message. We then divide the text into blocks of four characters. We add a bogus character Z at the end of the third block. The result is HELL OMYD EARZ. We create a three-block ciphertext ELHLMDOYAZER.

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

Data Encryption Standard



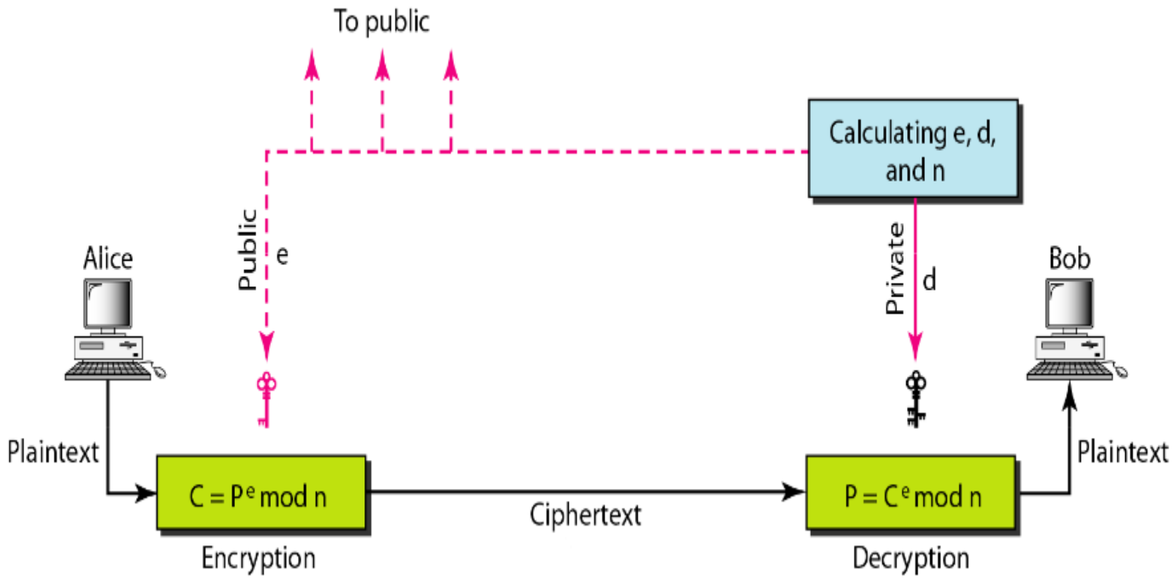
Data Encryption Standard (DES):

- It is one of the most widely accepted, publicly available cryptographic systems today.
- It was developed by IBM in the 1970s but was later adopted by the US government as a national standard.
- It uses a 56-bit key and it processes 64-bit inputs into 64-bit cipher-text.
- Algorithm goes through 16 iteration.

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org

RSA

•RSA is a public key system designed by **Ron Rivest, Adi Shamir, and Leonard Adleman** in 1978.
•The RSA operations can be decomposed in three broad steps; Key Generation, Encryption and Decryption.
•The private key is used to encrypt the data and decryption is done by using public key.
•RSA has many flaws in its design; therefore, not preferred for the commercial use.
•When the small values of are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks.
•On the other hand if large lengths are selected then it consumes more time in designing process of key, hence the performance of RSA is degraded in comparison with DES.
•Further, the algorithm also requires nearly equal lengths for ; practically this is very tough condition to satisfy. If this condition is not satisfied then padding techniques are used which increases the system's overheads by taking more processing time in encryption.



In RSA, *e* and *n* are announced to the public; *d* and Φ are kept secret.

Reference: 1. Ferouzan, Behrouz A., Data Communications and Networking, 2. Stallings William, Data and Computer Communication. 3. https://ieeexplore.ieee.org