INTRODUCTION TO CRYPTOGRAPHY

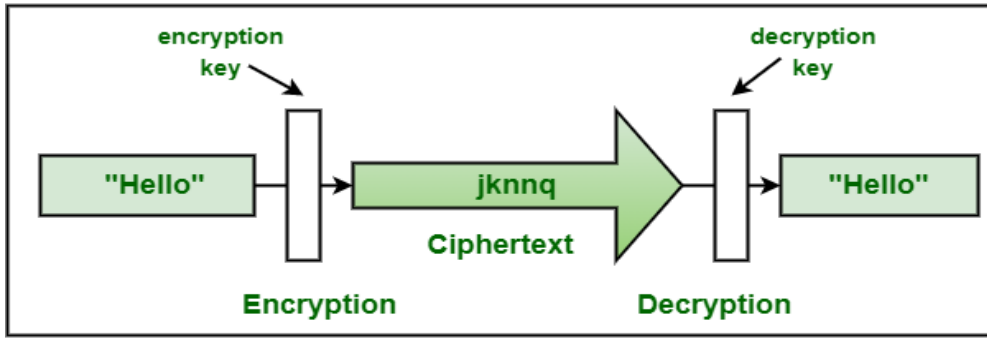
ECE 422 – DATA COMMUNICATIONS & COMPUTER NETWORKS

Monday, April 13, 2026

WHAT IS CRYPTOGRAPHY?

Origin of Word

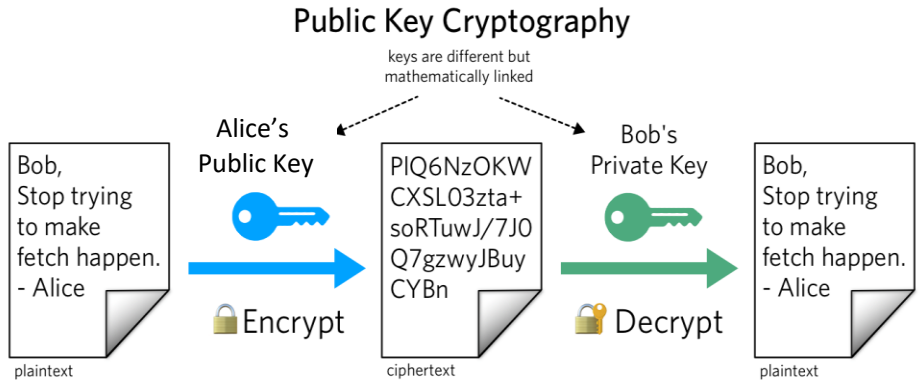
- The word cryptography was derived from the Greek word *Kryptos*, which is used to define anything that is *hidden, obscure, secret or mysterious*.



Cryptography

Modern Definition

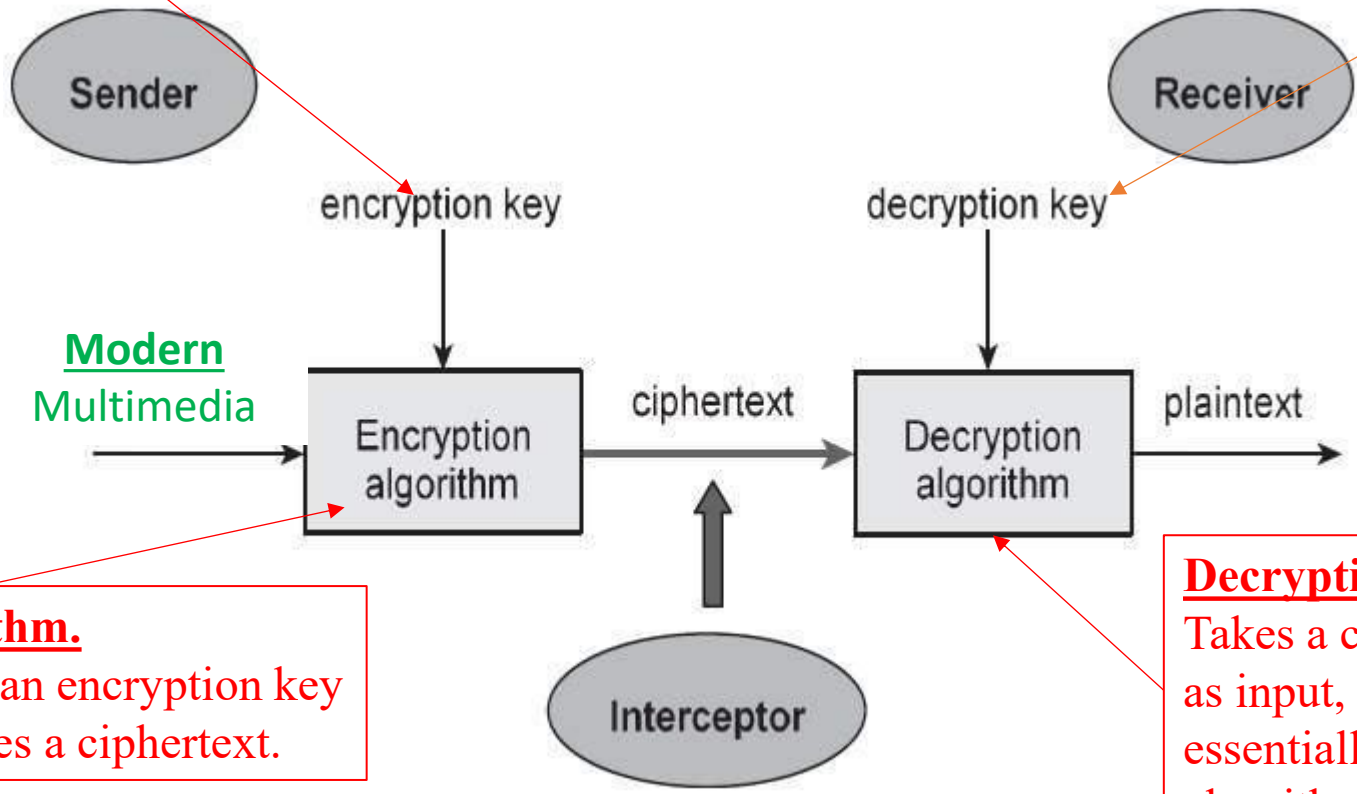
1. **Cryptography** is the science and art of transforming messages to make them secure and immune to attacks.
2. **Cryptography** is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.



COMPONENTS OF A CRYPTOSYSTEM

Encryption Key:
Sender inputs the encryption key into the encryption algorithm along with the plaintext in order to generate the ciphertext.

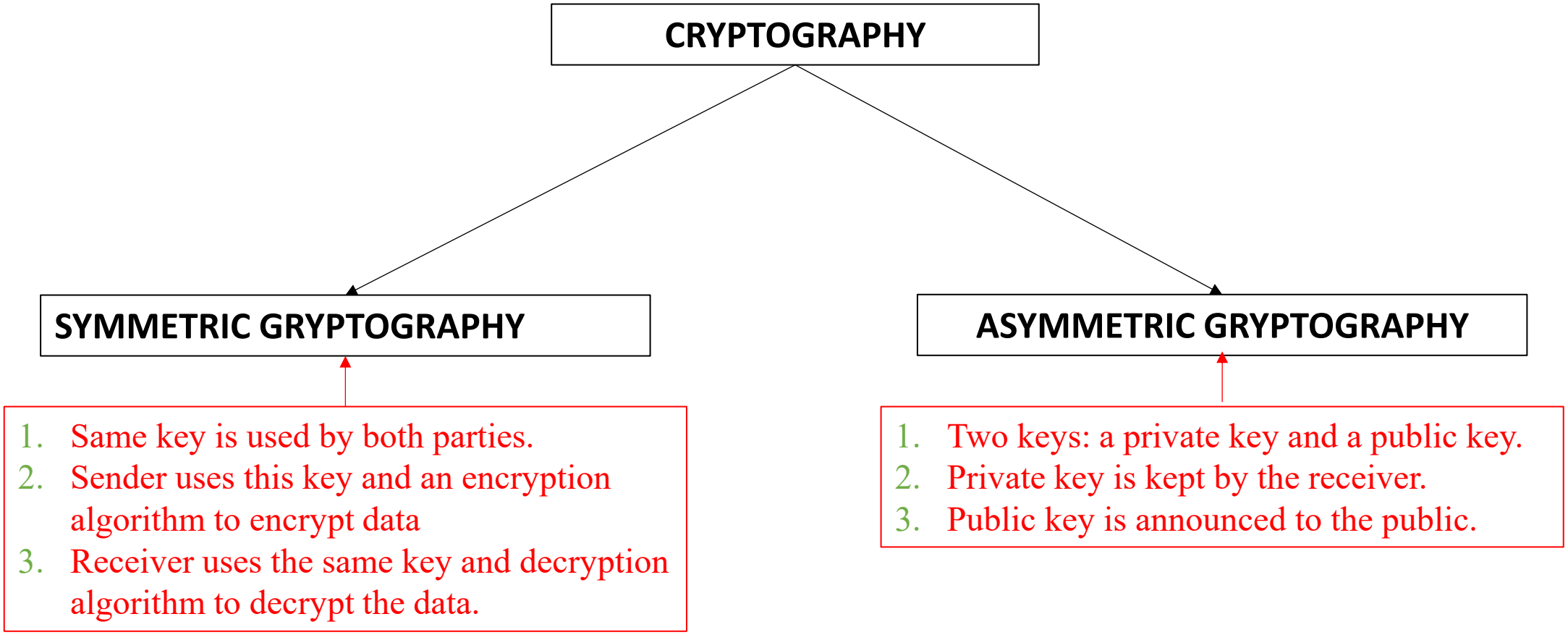
Decryption Key:
Receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.



Encryption Algorithm.
Takes plaintext and an encryption key as input and produces a ciphertext.

Decryption Algorithm:
Takes a ciphertext and a decryption key as input, and outputs a plaintext. It essentially reverses the encryption algorithm and is thus closely related to it.

CATEGORIES OF CRYPTOGRAPHY



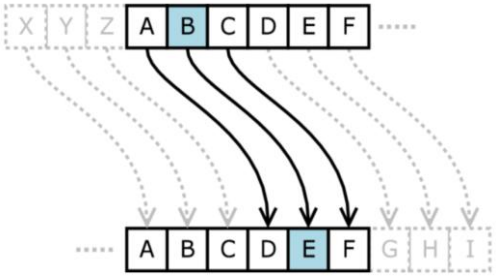
TRADITIONAL CIPHERS

TRADITIONAL CRYPTOGRAPHY

TRANSLATION CIPHERS

SUBSTITUTION CIPHERS

Substitution cipher (Ceasar cipher) substitutes one symbol with another.



Transposition Cipher
A cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text.

MONOALPHABETIC CIPHERS

POLYALPHABETIC CIPHERS

Monoalphabetic cipher
Character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text.

Polyalphabetic cipher
The relationship between a character in the plaintext to a character in the ciphertext is a one-to-many relationship.

WORKED EXAMPLE

Create a code a secret message using a Caesar cypher with a shift of 7 to the right to send the message “THIS IS A SECRET MESSAGE BURN AFTER READING”

SOLUTION

1. Create the substitution table having the alphabet and the same alphabet shifted 7 places to the right as follows.

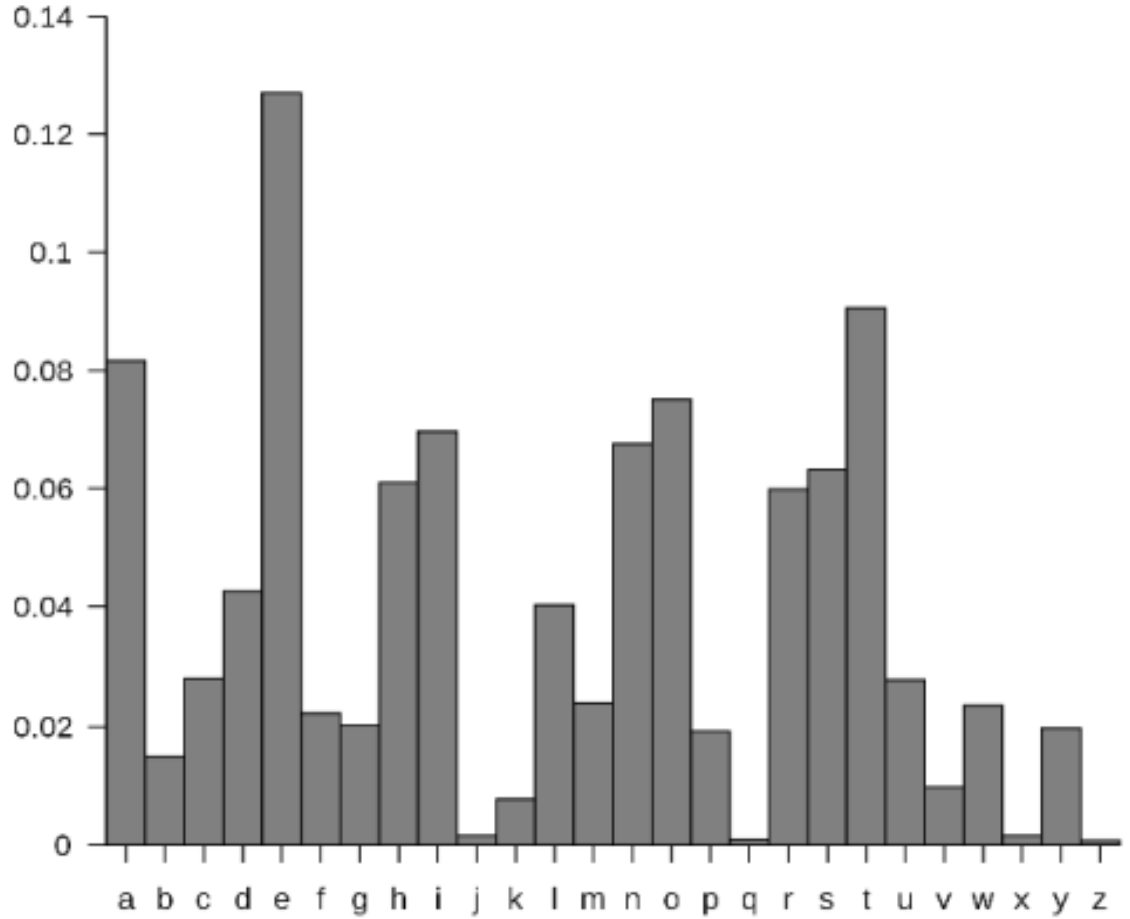
	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T

2. Write the message and the corresponding symbols as shown below.

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

PROBLEM WITH CAESAR CYPHER

1. **Caesar cipher** can easily be broken, even in cipher-text only scenario using frequency analysis.
2. **Frequency analysis** uses the frequency distribution of letters in a language to guess original letters. The distribution of letters in a typical sample of English language text has a very distinct and predictable shape.
3. **A Caesar shift** "rotates" this frequency distribution, and it is possible to determine the shift by examining the resultant frequency graph.



TRANSPOSITION/COLUMNAR CIPHER

In transformation cypher is created using the following steps.

1. Plain text is written out in fixed length rows in a table.
2. Columns are rearranged based on the password.
3. The message is read out column by column.
4. If the matrix is not completely filled, it is padded with null characters or some other character.

WORKED EXAMPLE – TRANSPOSITION CIPHER

Write the transposition cypher code of the message “enemyattackstonight” with a Key:31452. Use z to pad any empty spaces.

SOLUTION

Step 1: Write the plain text column by column.

1	2	3	4	5
e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

Step 2: Rearrange the columns

3	1	4	5	2
e	e	m	y	n
t	a	a	c	t
t	k	o	n	s
h	i	t	z	g

Step 3: Read the matrix column by column

Cipher text: ettheakimaotycnzntsg

MODERN CIPHERS

1. Traditional ciphers were character-oriented.
2. With the advent of the computer, ciphers need to be bit-oriented. This is so because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data.
3. It is convenient to convert these types of data into a stream of bits, encrypt the stream, and then send the encrypted stream.
4. When text is treated at the bit level, each character is replaced by 8 (or 16) bits, which means the number of symbols becomes 8 (or 16).
5. Mingling and mangling bits provides more security than mingling and mangling characters.

MODERN CIPHERS /02

Modern ciphers are normally made of a set of simple ciphers, which are simple predefined functions in mathematics or computer science and include:

1. XOR cipher:
2. Rotation cipher:
3. Substitution Cipher (S-box):
4. Transposition Cipher (P- box):