

The logo of Galgotias University is a stylized circular emblem with three curved, overlapping bands in shades of yellow, blue, and red, resembling a globe or a dynamic swirl.

## UNIT I

### Introduction: Basic Terminology

GALGOTIAS  
UNIVERSITY

# CLASSICAL ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques: substitution and transposition.

## SUBSTITUTION TECHNIQUES



A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

## Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet. e.g., plain text : pay more money Cipher text: SDB PRUH PRQHB Note that the alphabet is wrapped around, so that letter following „z“ is „a“.

GALGOTIAS  
UNIVERSITY

## Example

For each plaintext letter  $p$ , substitute the cipher text letter  $c$  such that

$$C = E(p) = (p+3) \bmod 26$$

A shift may be any amount, so that general Caesar algorithm is

$$C = E(p) = (p+k) \bmod 26$$

Where  $k$  takes on a value in the range 1 to 25. The decryption algorithm is simply

$$P = D(C) = (C-k) \bmod 26$$

GALGOTIAS  
UNIVERSITY

## Playfair cipher

The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy“ . The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.

## Example

The letter „i“ and „j“ count as one letter. Plaintext is encrypted two letters at a time According to the following rules:

- ❑ Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x“. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last.
- ❑ Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.

Otherwise, each plaintext letter is replaced by the letter that lies in its own row And the column occupied by the other plaintext letter.

## Example

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

Plaintext = meet me at the school house  
Splitting two letters as a unit => me et me at th es ch ox ol ho us  
ex Corresponding cipher text => CL KL CL RS PD IL  
HY AV MP HF XL IU

# Playfair Cipher Encryption Algorithm

The Algorithm consists of 2 steps:

## **Generate the key Square(5×5):**

- ❑ The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
- ❑ The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.



# Example

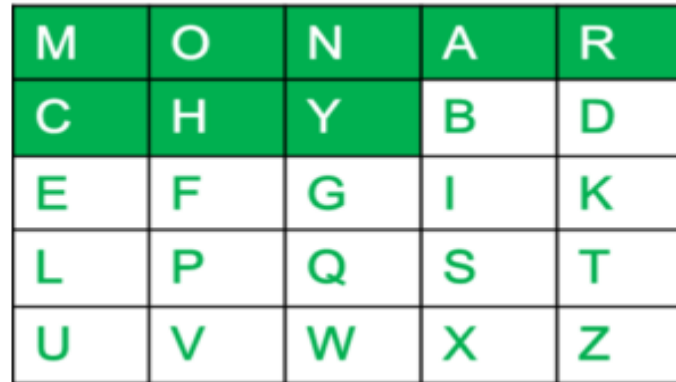
**For example: Keyword:MONARCHY**

**Plaintext:INSTRUMENTS**

The key is "monarchy" Thus the initial entieres are 'm', 'o', 'n', 'a', 'r', 'c', 'h', 'y' followed by remaining characters of a-z(except 'j') in that order.

GALGOTIAS  
UNIVERSITY

# Example



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

GALGOTIAS  
UNIVERSITY

## Algorithm to encrypt the plain text

The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. **For example:**

❑ **PlainText:** "instruments"

❑ **After Split:** 'in' 'st' 'ru' 'me' 'nt' 'sz'

❑ **Rules for Encryption:**

❑ **If both the letters are in the same column:** Take the letter below each one (going back to the top if at the bottom).

**For example:**

**Diagraph:** "me"

**Encrypted Text:** cl

**Encryption:** m -> c e -> l

# Example

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

GALGOTIAS  
UNIVERSITY

## Example

- **If both the letters are in the same row:** Take the letter to the right of each one (going back to the leftmost if at the rightmost position). **For example:**
- **Diagraph:** "st"
- **Encrypted Text:** tl
- **Encryption:** s -> t t -> l

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

## Example

- **If neither of the above rules is true:** Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
- **For example:**
- **Diagraph:** "nt"
- **Encrypted Text:** rq
- **Encryption:** n -> r t -> q

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

# Example

**For example: Plain Text:** "instrumentsz" **Encrypted Text:** gatlmzclrqtz

**Encryption:**

i -> g  
n -> a  
s -> t  
t -> l  
r -> m  
u -> z  
m -> c  
e -> l  
n -> r  
t -> q  
s -> t  
z -> x



GALGOTIAS  
UNIVERSITY

# Example

in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

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



## Strength of playfair cipher

Playfair cipher is a great advance over simple mono alphabetic ciphers. Since there are 26 letters,  $26 \times 26 = 676$  diagrams are possible, so identification of individual diagram is more difficult

GALGOTIAS  
UNIVERSITY

## Polyalphabetic ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.

The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common.

- A set of related monoalphabetic substitution rules are used

- A key determines which particular rule is chosen for a given transformation

GALGOTIAS  
UNIVERSITY

## Vigenere cipher

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 caesar ciphers with shifts of 0 through 25.

Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd' (since a=0, b=1, c=2 and so on).

To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed .

Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left.

A normal alphabet for the plaintext runs across the top. The process of Encryption is simple:

Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

## Vigenere cipher

- ❑ Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square* or *Vigenère table*.
- ❑ The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- ❑ At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- ❑ The alphabet used at each point depends on a repeating keyword.

## Example

Input : Plaintext : GEEKSFORGEEKS

Keyword : AYUSH

Output : Ciphertext : GCYCZFMLEIM

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text. The keyword "AYUSH" generates the key "AYUSHAYUSHAYU" The plain text is then encrypted using the process explained below.

### Encryption

The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column Y is C. The rest of the plaintext is enciphered in a similar fashion.

# Example

	PLAIN TEXT															
K		a	b	c	d	e	f	g	h	i	j	k	...	x	y	z
E	a	A	B	C	D	E	F	G	H	I	J	K	...	X	Y	Z
Y	b	B	C	D	E	F	G	H	I	J	K	L	...	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	...	Z	A	B
L	d	D	E	F	G	H	I	J	K	L	M	N	...	A	B	C
E	e	E	F	G	H	I	J	K	L	M	N	O	...	B	C	D
T	f	F	G	H	I	J	K	L	M	N	O	P	...	C	D	E
T	g	G	H	I	J	K	L	M	N	O	P	Q	...	D	E	F
E	:	:	:	:	:	:	:	:	:	:	:	:	...	:	:	:
R	:	:	:	:	:	:	:	:	:	:	:	:	...	:	:	:
S	x	X	Y	Z	A	B	C	D	E	F	G	H	...			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	...			X
	z	Z	A	B	C	D	E	F	G	H	I	J	...			Y

# Table to encrypt-Geeks

## Table to encrypt – Geeks

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



## Decryption

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

- ❑ A more **easy implementation** could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].
- ❑ **Encryption** The plaintext(P) and key(K) are added modulo 26.  $E_i = (P_i + K_i) \bmod 26$
- ❑ **Decryption**  $D_i = (E_i - K_i + 26) \bmod 26$
- ❑ **Note:**  $D_i$  denotes the offset of the i-th character of the plaintext. Like offset of **A** is 0 and of **B** is 1 and so on.



## Example

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g.,

key = d e c e p t i v e d e c e p t i v e d e c e p t i v e

PT = w e a r e d i s c o v e r e d s a v e y o u r s e l f

CT = Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Strength of Vigenere cipher

- o There are multiple cipher text letters for each plaintext letter.
- o Letter frequency information is obscured.

# One Time Pad Cipher

It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s. this can be accomplished by writing all numbers in binary, for example, or by using ASCII.

The key is a random sequence of 0's and 1's of same length as the message. Once a key is used, it is discarded and never used again. The system can be expressed as Follows:

$$C_i = P_i \oplus K_i$$

$C_i$  -  $i^{\text{th}}$  binary digit of cipher text  $P_i$  -  $i^{\text{th}}$  binary digit of

plaintext  $K_i$  -  $i^{\text{th}}$  binary digit of key

Exclusive OR operation

Thus the cipher text is generated by performing the bitwise XOR of the plaintext and the key.

Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation:

$$P_i = C_i \oplus K_i$$

e.g., plaintext = 0 0 1 0 1 0 0 1

Key = 1 0 1 0 1 1 0 0

## Example

- ----- ciphertext = 1 0 0 0 0 1 0 1
- Advantage: Encryption method is completely unbreakable for a ciphertext only attack.  
Disadvantages It requires a very long key which is expensive to produce and expensive to transmit. Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.f

GALGOTIAS  
UNIVERSITY



Thank You