

# Universidad Tecnológica del Sureste de Veracruz

## Tecnologías de la Información



### Práctica 1

Alumno: **Gómez Solis Jose Alberto**

Asignatura: **Seguridad de la información**

Cuatrimestre: **Séptimo**

Grupo: **701**

Docente: **ING. Jimmy Noe Pacheco Reyes**

Cd. Nanchital de Lázaro Cárdenas del Río, Ver., a **01 de Octubre de 2021**

## LECCIÓN 1: HISTORIA DE LA CRIPTOGRAFÍA Y SU DESARROLLO EN EUROPA EJERCICIOS

### EJERCICIO 1

El descubrimiento de que cada lengua tenía una frecuencia característica de aparición de sus letras, permitió la ruptura de los textos cifrados tipo César y, más general aún, los monoalfabéticos.

Por ello, los criptógrafos se afanaron desde el Renacimiento en encontrar nuevos métodos de cifrado, hallando entre otros los denominados polialfabeto. En éstos, se usan varios alfabetos cifrados, de modo que la letra cifrada de una dada depende de la posición de ésta en el texto en claro. De todos ellos el más sencillo es aquel que usa dos alfabetos de cifrado, uno para las letras que ocupan posiciones pares en el texto en claro y otro para las que se ubican en posiciones impares.

Así, un ejemplo podría ser:

Alfabeto para posiciones impares

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	e	i	m	p	t	x	b	f	j	n	q	u	Y	c	g	k	ñ	r	v	z	d	h	l	o	s	w
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Alfabeto para posiciones pares

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	r	w	b	g	l	p	u	z	e	j	ñ	s	X	c	h	m	q	v	a	f	k	o	t	y	d	i

Suponiendo este método polialfabético cifre el texto en claro:

“SUSTITUCIÓN POLIALFABÉTICA”

### SOLUCIÓN

Procediendo como se ha indicado resulta:

S	U	S	T	I	T	U	C	I	O	N	P	O	L	I	A	L	F	A	B	E	T	I	C	A
V	k	v	f	f	f	d	w	f	h	y	m	g	ñ	f	n	q	l	a	r	p	f	f	w	a

Así pues el resultado será:

v k v f f f d w f h y m g ñ f n q l a r p f j w a

Cifre los siguientes textos:

- 1.- “universidad tecnologica del sureste de veracruz”
- 2.- “tecnologias de la información y comunicacion”

Resultados:

- 1.- dxfovpvzmnmfpwyhghxzinzmgqadvpazgmghgrnivdi
- 2.- zgixgñgpfnvbpñazylgvunizgxswgsdxfwawfhy

### Ejercicio 2

Realice una aplicación de escritorio que permita introducir un texto plano mediante el teclado y cifre dicho texto mediante el método descrito anteriormente, el texto cifrado lo debe mostrar en un cuadro aparte.

