Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado monoalfabéticos

- Sustituyen cada letra por otra que ocupa la misma posición en un alfabeto desordenado y esta correspondencia se mantiene a lo largo de todo el mensaje. Así se consiguen tantas claves como posibilidades de alfabetos hay.
- El problema está en cómo recordar la clave (el alfabeto desordenado).
- El mejor sistema de criptoanálisis para romper el algoritmo es el estadístico. Se puede romper vía análisis de frecuencia de letras

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado monoalfabéticos …

- El procedimiento es el siguiente:
- Se busca una palabra (clave) fácil de recordar y se le quitan las letras duplicadas.

SEGURIDAD ➔ SEGURIDA

- Se añaden al final de la palabra las restantes letras del alfabeto (sin duplicar letras).

SEGURIDABCFHJKLMNOPQTVWXYZ

Criptografía clásica …

- Cifrados por sustitución …
- Métodos de cifrado monoalfabéticos …
  - Se ordenan en una matriz cuya primera fila es la palabra clave

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

  - El nuevo alfabeto (alfabeto modificado) se lee por columnas y se alinea con el original:

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
s	b	n	y	e	c	o	z	g	f	p	u	h	q	r	j	t	i	k	v	d	l	w	a	m	x

  - Ejemplo: el mensaje *ataque* se convertiría en SVSTDE
  - Ejemplo: gato → osvq

Criptografía clásica …

- TAREA:

❖ Programa de cifrado monoalfabético

- Debe aceptar llaves de hasta 16 caracteres de longitud
- Igual que los anteriores, debe poder leer archivos tipo texto, o aceptar captura directa por teclado del texto claro.
- Debe mostrar la “construcción” del texto encriptado, es decir:
  - Matriz de construcción del alfabeto modificado
  - Tabla del alfabeto original alineado con el alfabeto modificado
  - Texto claro comparado con texto encriptado

❖ Programa de descifrado monoalfabético

- Debe aceptar llaves de hasta 16 caracteres de longitud
- Igual que los anteriores, debe poder leer archivos tipo texto (Texto encriptado).
- Debe mostrar la “construcción” del texto claro, es decir:
  - Tabla del alfabeto modificado alineado con el alfabeto original
  - Matriz de construcción del alfabeto modificado hacia alfabeto normal
  - Texto encriptado comparado con texto claro

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado polialfabéticos (siglo XV)

- Se usan varios cifradores sustitutivos monoalfabéticos, dependiendo de la posición de la letra en el texto.
- Leon Battista Alberti inventa y publica el primer cifrador polialfabético (1459)
  - Este cifrador no fue roto hasta el siglo XIX.

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado polialfabéticos (siglo XV)

- Un ejemplo típico es el Cifrado de Vigènere:

  - Se basa en una tabla con un alfabeto por cada letra del abecedario

- Método:
  - Se busca una palabra clave fácil de recordar.
  - Se escribe la palabra debajo del texto en claro, repitiéndose tantas veces como sea necesario.
  - Cada letra del texto en claro se codifica con el alfabeto de la tabla marcado por la letra inferior, o sea, la letra de la clave que corresponde.

Criptografía clásica …

- Cifrados por sustitución …
- Métodos de cifrado polialfabéticos (siglo XV)

	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

- Ejemplo:
  - Clave:
    - ADIOS
  - Texto claro :
    - E S T O E S C R I P T O L O G I A
  - Clave sec.:
    - A D I O S A D I O S A D I O S A D
  - Criptograma:
    - E V B C W K F Z E H T R T C Y I D

gato → gdbe

Criptografía clásica …

- TAREA:

❖ Programa de cifrado Vigènere

- Debe aceptar llaves de hasta 8 caracteres de longitud
- Igual que los anteriores, debe poder leer archivos tipo texto, o aceptar captura directa por teclado del texto claro.
- Debe mostrar la “construcción” del texto encriptado, es decir:
  - Tabla polialfabética
  - Texto claro con repetición de palabra clave
  - Texto claro comparado con texto encriptado

❖ Programa de descifrado Vigènere

- Debe aceptar llaves de hasta 8 caracteres de longitud
- Igual que los anteriores, debe poder leer archivos tipo texto (Texto encriptado).
- Debe mostrar la “construcción” del texto claro, es decir:
  - Tabla polialfabética
  - Texto encriptado con repetición de palabra clave
  - Texto claro comparado con texto encriptado