MANEJO DE FUNCIONES

Equipos de 4 integrantes

El término de criptografía proviene de dos vocablos griegos: *criptos*, que significa oculto o escondido y *grafos*, que significa escrtitura. Es el arte de escribir un mensaje con un significado pleno mediante el uso de claves y cifras que ocultan el verdadero sentido de la informción.

El texto que forma el mensaje original y que se cifra con un algoritmo dado se denomina texto plano o texto claro, mientras que el mensaje ya cifrado recibe el nombre génerico de texto cifrado o criptograma.

Los métodos critpográficos pueden dividirse en dos grandes técnicas de transformación del texto: los métodos de sustitución y los de transposición.

En una sustitución las unidades de texto plano mantienen su orden en el mensaje, pero se sustituye con texto cifrado siguiendo un algoritmo específico.

En una transposición las letras del texto plano se mezclan o desordenan siguiendo un determinado algoritmo para obtener una anagrama.

Los métodos de sustitución son mucho más numerosos e importantes que los de transposición y todos ellos parten del concepto de alfabeto de sustitución.

La cifra ATABASH
ATABASH es un método criptográfico de sustitución monoalfabética muy empleado en el alfabeto hebreo entre los años 600 y 500 a.C.

Alfabeto: 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

Cifrado: 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

Ejemplo: Cifrar el texto plano: *La misión ha sido un éxito*.

Sustituyedo la letra del alfabeto con su correspondiente letra de Cifrado tenemos:

Texto Cifrado: OZ NRHRLM SZ HRWL FM VCRGL

La cifra César
Es una de las técnicas criptográficas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución monoalfabética en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3 la “a” sería sustituida por la “D”. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus genereales.

Alfabeto: 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

Cifrado: 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

Ejemplo: Cifrar el texto plano: *La misión ha sido un éxito*.

Sustituyedo la letra del alfabeto con su correspondiente letra de Cifrado tenemos:

Texto Cifrado: OD PLVLRQ KD VLGR XQ HALWR

Las cifras de Bellaso.
Bellaso nació en Brescia en el seno de una familia acomodada en 1505. En 1538 recibió un título en leyes en la universidad de Padua.

En 1552 entró en contacto con el renombrado escritor Girolano Ruscelli, también experto en criptografía, quien le urigó a publicar sus conocimientos.

Giovano Batista ha pasado a la historia por haber ideado una cifra que marcó una época y que fue considerada irrompible durante más de cuatro siglos.

La cifra es una sustitución polialfabética, con uso de contraseñas largas que la hacían sufientemente segura, incluso aunque la tabla recíproca en la que se basa fuera de dominio público.

Tal como Bellaso describe en su obra de 1564, el mecanismo para cifrar un texto llano consiste en construir una tabla recíproca de cinco alfabetos mezclados. La tabla se genera a partir de una primera palabra que actúa como contraseña del siguiente modo:

- Si el número de letras es par, se distribuye mitad a mitad entre las dos líneas del alfabeto.
- Si es impar, se sitúa en la línea de arriba hasta la letra que se encuentra en la mitad de la palabra y el resto en la de abajo.

Por ejemplo, si la contraseña es IOVE, tendremos la siguiente tabla:

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

La contraseña tiene cuatro letras, así pues de distribuyen dos a dos entre las dos líneas del primer alfabeto. A continuación se acompleta este en orden sin las letras presentes en la contraseña. A partir de aquí, el resto de alfabetos se generan fácilmente: la primera mitad de todos los alfabetos es la misma, la segunda parte se obtiene desplazando un carácter a la derecha la segunda línea del alfabeto anterior.

El alfabeto en mayúsculas de la primera columna también se construye a partir del primero. Toma la primera letra del primer alfabeto y sigue escribiendo en orden y hacia abajo todas las letras. Cada cinco caracteres debes cambiar de columna.

El emisor emplea una contraseña distinta de la que ha empleado para construir la tabla recíproca.De esta contraseña sitúa la primera letra sobre la primera letra de la primera palabra del texto plano y así consecutivamente. A continuación se cifra palabra por palabra comenzando con el alfabeto indcado por la letra de la contraseña y cambiando cíclicamente con cada letra hasta llegar a la primera letra de la palabra siguiente, donde será necesario empezar por el alfabeto indicado por la letra de la contraseña.

Ejemplo: Cifrar el texto plano: *El Papa viajará a Roma pronto*.
Contraseña: AVE MARIA GRATIA PLENA

A	V	E	M	A	R
El	Papa	viajará	a	Roma	pronto

Texto Cifrado: BU FYBE CVETZJN V GYUN FJEBJY

La cifra Playfair
Sir Charles Wheatstone fue un reputado científico e inventor británico de la época victoriana. A él le corresponde por derecho propio el algoritmo de la cifra Playfair.

En la sustitución digrámica de Playfair la clve viene dada por una matriz de cifrado de 5x5 caracteres (las letras I/J son intercambiables y no existe la Ñ).

Se coloca en la primera fila de la matriz la palabra clave sin letras repetidas y eliminando caracteres duplicados. Se combinan las letras I y J en un solo elemento y se rellena a continuación la matriz con las letras del alfabeto que falten en su orden normal.

Por ejemplo, supongamos que usamos como contraseñala propia palabra PLAYFAIR. Entonces la matriz de cifrado/descifrado quedaría así:

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

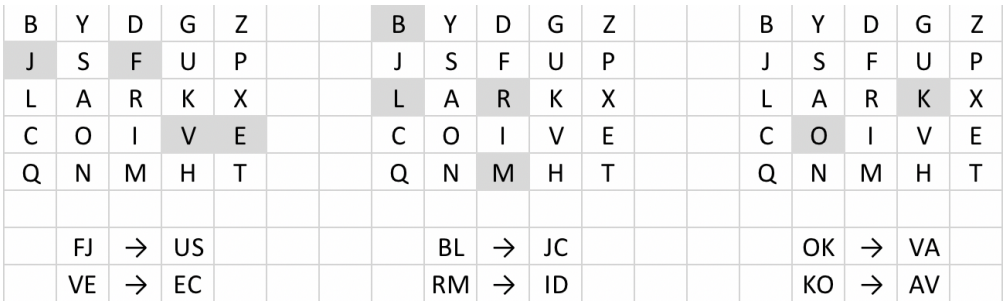
Para cifrar un texto se debe separar en diagramas, de modo que ambas letras sean diferentes. Si no ocurre esto, se inserta una letra X adicional entre las dos idénticas y se añade otra adicional al final para convertir en un dígrafo una letra final que quede aislada.

Para cifrar el mensaje La cifra es vulnerable, la separación en dígrafos quedaría así:

la ci fr ae sv ul ne ra bl ex

Todos los dígrafos poseen en la matriz una de estas tres posiciones: las dos letras caen en la misma línea, en la misma columna o aparecen en distinta fila o columna:

- Si ambas letras están en la misma fila, se reemplazan por la letra que queda a la derecha de cada una de ellas. Si una de las letras está al final de la línea se reemplaza por la letra que haya al principio.
- Si ambas letras están en la misma columna, son reemplazadas por la letra que hay debajo de cada una de ellas. Si una de las letras esta en la parte inferior de la columna se cambia por la que está al principio de la columna.
- Si las letras no están en la misma fila o columna se reemplazan por aquellas que se encuentran en la misma fila pero en el otro par de vértices del rectángulo que define el par original.



Estan en el mismo renglón. Estan en la misma columna. No coinciden

Para descifrar, puesto que es una cifra simétrica, basta con seguir el proceso inverso de las tres reglas antes mencionadas.

Transposición Columnar Simple

Los métodos criptográficos por transposición ya no sustituyen los símbolos de un mensaje por otros, sino que los mezclan en un orden que hacen que el mensaje original ya no sea comprensible.

Una técnica de permutación muy empleada antiguamente es la transposición columnar.

Para emplearlo, se debe escribir el texto de izquierda a derecha y de arriba abajo en una tabla con un número de columnas acordado previamente entre el emisor y el receptor. Cada letra se sitúas en cada celda hasta agotar el texto.

Finalmente, el texto cifrado se obtiene escribiendo las letras por columnas desde la primera, hasta la última.

Ejemplo: Cifrar el texto plano: *El arte de la medicina consiste en entretener al paciente mientras la naturaleza cura la enfermedad*.

E	L	A	R	T	E	D
E	L	A	M	E	D	I
C	I	N	A	C	O	N
S	I	S	T	E	E	N
E	N	T	R	E	T	E
N	E	R	A	L	P	A
C	I	E	N	T	E	M
I	E	N	T	R	A	S
L	A	N	A	T	U	R
A	L	E	Z	A	C	U
R	A	L	A	E	N	F
E	R	M	E	D	A	D

Escribiendo por columnas:

Texto Cifrado: EECSENCILARE LLIINEIEALAR AANSTRENNELM RMATRANTAZAE TECEELTRTAED EDOETPEAUCNA DINNEAMSRUFD

Aplicación a desarrollar
La aplicación debe presentar un menú donde se puedan seleeccionar cada uno de los métodos para cifrar y descifrar un texto plano y un texto cifrado.

La aplicación debe contemplar:

- Uso de funciones: declaración, con y sin argumentos, funciones que reciben y mandan colecciones: listas, tuplas, conjuntos, diccionarios
- Uso de cadenas de caracteres y colecciones en python
- Uso de estructuras de control
- Uso de módulos propios. (Investigar)

NOTA: No utilizar expresiones regulares.

Puntos a considerar para la entrada y salida de datos en la aplicación:

- El texto plano se escribe con mayúsculas y mínusculas según sea el caso: “La Casa Rosa esta en la avenida principal”.
- El alfabeto base se escribe con minúscula.
- El alfabeto cifrado con mayúscula. El texto cifrado se presenta en letras mayúsculas.
- Las matrices se toman tal como se presentan anteriormente.
- Las contraseñas para la cifra César son mayores a 3 y menores a 6.
- El texto original se obtiene del descifrado y debe considerarse con espacios en blanco

Fecha de Entrega: Martes 14 de Septiembre 2021