Universidad Internacional de La Rioja (UNIR)

Escuela de Ingeniería

Grado en Ingeniería Informática

Sistemas Encriptadores para Seguridad de Propósito General

Ubicación del código fuente:

https://github.com/Raycosegura/TFG-UNIR

https://drive.google.com/drive/folders/1xwxOSKvpn1mQpcnQX1FjqPHZr9gZOhpT?usp=sharing

Trabajo Fin de Grado
presentado por: SEGURA TAVÍO, RAYCO JAVIER
Director/a: PEÑA SÁNCHEZ, LUIS

Ciudad: Madrid
Fecha: 18/07/2018

ÍNDICE

1. INTRODUCCIÓN

1.1 MOTIVACIÓN

Hoy en día la gran mayoría de nosotros usamos una computadora ya sea de tu trabajo o propia para uso personal. Poco a poco vamos llenando el disco duro de nuestra computadora de información, tanto de forma voluntaria como involuntaria. Por eso es muy importante que aprendamos a proteger esta información que, de caer en manos equivocadas, puede resultar muy peligroso.

Muchas personas consideran que la información que guardan en sus dispositivos, ya sea computadoras, teléfonos o tabletas no es tan importante ni dice tanto de ellos como para tener que salvaguardarla. Cuando alguien experto en extraer información pone sus manos en un dispositivo de otra persona, es capaz de obtener mucha más información de la que creemos, desde teléfonos y correos electrónicos hasta cuentas bancarias, o información confidencial de tu negocio o compañía que sin duda nadie más debería de ver.

Al encriptar la información la estamos protegiendo de tres cosas, un robo, un *hacker* o un *malware*, término anglosajón para referirse a *malicious software* o software malicioso que extrae la información de los dispositivos o bien envía virus a través de tus cuentas de correo y redes sociales. La encriptación de la información te da una última oportunidad de salvar tus datos, si no están en tus manos, al menos tampoco estarán en manos de nadie más, especialmente quien pueda darle un mal uso.

En tiempos digitales, la información que almacenamos en nuestros dispositivos dice mucho más de nosotros que lo que quisiéramos y hay cosas confidenciales que ciertamente no tienen por qué estar en manos que no debieran.

Por eso siendo un tema tan importante en la actualidad y fundamental para nuestra seguridad es lo que me ha motivado a realizar este Trabajo Fin de Grado.

1.2 OBJETIVOS

Con el presente Trabajo Fin de Grado se pretende desarrollar una aplicación informática de algoritmos de criptografía y seguridad en ordenadores, en la cual un usuario encripta y desencripta un texto o documento en base a los algoritmos de sustitución y será el usuario quien elija el algoritmo deseado.

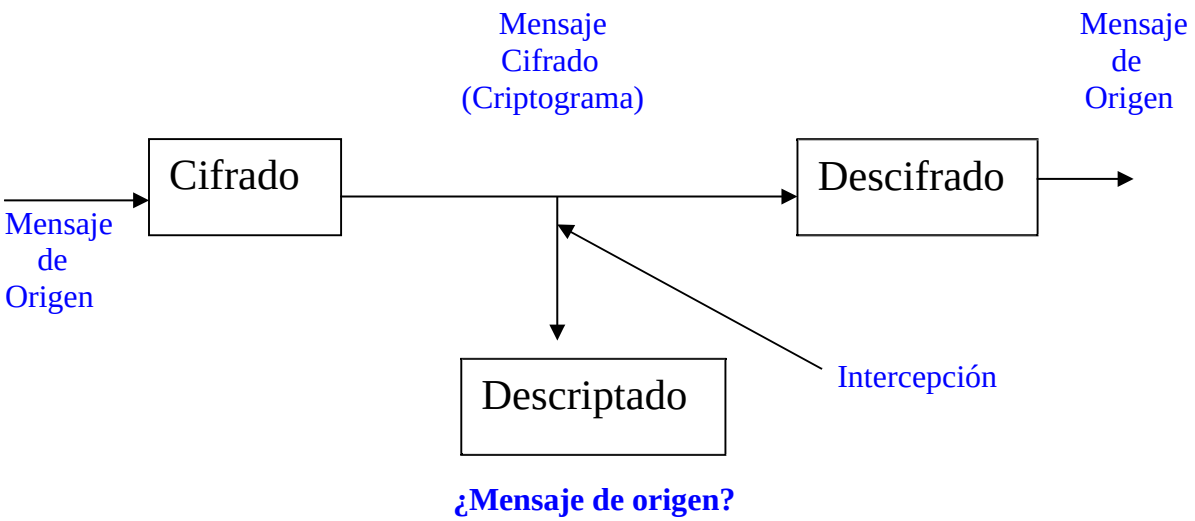
En este Trabajo Fin de Grado se pretende alcanzar los objetivos de tener nuestra información protegida con los diversos algoritmos implementados, proporcionando la seguridad que dicha información requiere, ya que la misma es de vital importancia.

1.3 METODOLOGÍA

--Los métodos implementados en este Trabajo Fin de Grado son los cifrados por sustitución: cifrado por decimación , cifrado por desplazamiento puro, cifrado por sustitución afín, los cuales se explicarán más adelante en qué consisten.

--La plataforma utilizada es el C++ builder, ya que he decidido realizarlo en el lenguaje C++ debido a que es un lenguaje fundamental en la ingeniería en informática, seguro para el desarrollo de aplicaciones y el cual conozco bastante bien.

--El sistema se compone de una interfaz de usuario en la cual dicho usuario puede interactuar para realizar el cifrado y descifrado, dicha interfaz estará realizado así como su desarrollo en Borland C++ Builder.



Antes de empezar con los tipos de criptosistemas que existen, debemos entender y tener claro: los elementos que configuran la seguridad informática, la terminología utilizada, los requisitos de un criptosistema y cómo se clasifican dichos criptosistemas.

1.4 ELEMENTOS QUE CONFIGURAN LA SEGURIDAD INFORMÁTICA

Existen 4 elementos que configuran la seguridad informática:

1) **Confidencialidad:** Sólo los usuarios autorizados tienen acceso a componentes del sistema.

2) **Integridad:** Sólo los usuarios autorizados pueden modificar los componentes del sistema.

3) **Disponibilidad:** Sólo los usuarios autorizados tienen disponibles los componentes del sistema.

4) **No repudio:** Los usuarios autorizados tienen los derechos y deberes que el sistema proporciona, y no pueden renunciar a ellos.

El canal es la parte más vulnerable en una comunicación entre emisor y receptor, por ello se usa la criptografía como elemento básico de seguridad.

1.5 TERMINOLOGÍA

En este apartado definimos algunos términos que resultan básicos en criptografía:

1) **Criptología:** Ciencia que estudia la criptografía.
2) **Criptografía:** Rama de la ciencia matemática cuyo objetivo es el cifrado de mensajes mediante un algoritmo y distintas claves, lo que constituye distintos criptosistemas.
3) **Criptosistemas:** Sistemas informáticos capaces de codificar y descodificar un mensaje mediante un algoritmo y una clave.
4) **Criptogramas:** Mensajes cifrados.
5) **Criptoanálisis:** Técnicas que usa un usuario ajeno al sistema para revelar el mensaje original del criptograma.
6) **Cifrar, descifrar:** Los actos de cifrar y descifrar un mensaje.

1.6 REQUISITOS Y CLASIFICACIÓN DE CRIPTOSISTEMAS

Los criptosistemas debieran caracterizarse en:

- Ser rápidos y fiables.
- Que el cifrado y descifrado deben ser fáciles de usar y disponibles en cualquier momento para el usuario.
- Que el tiempo de cifrado y descifrado no debe producir retardos.
- Que la seguridad dependerá de la clave, no del algoritmo.
- Que la clave debe tener tal fortaleza que sea casi imposible su determinación.

En cuanto a la clasificación de los criptosistemas debemos tener en cuenta dos aspectos importantes, como son la clave y la forma en que el algoritmo incide en el mensaje.

*** Según la clave** podemos distinguir dos tipos de criptosistemas :

-Los que generan cifrados simétricos o de clave pública :

En dichos criptosistemas existe una sola clave compartida por emisor y receptor. La fortaleza del sistema se fundamenta en la propia clave y su secreto. La confidencialidad, integridad, y autenticidad del sistema se obtiene únicamente de la clave.

-Los que generan cifrados asimétricos o de clave privada :

Cada usuario tiene un par de claves, una pública y una privada. Ambas claves son inversas, es decir, una cifra y la otra descifra.

Existen dos formas de emplear las claves:

-El emisor codifica con la clave pública del receptor, y éste descifra con su clave privada, de este modo se garantiza confidencialidad.

-El emisor codifica con su clave privada, y el receptor descifra con la clave pública del emisor, de este modo se garantiza integridad y autenticidad.

Conclusiones:

- Con los cifrados de clave pública tenemos que gestionar menor número de claves que con los sistemas de clave privada, lo que supone una ventaja para éste sistema frente a los sistemas de clave privada.

- La fuerza de los sistemas de clave privada radica en la imposibilidad computacional de obtener la clave privada a partir de la clave pública.

*** Según la forma en que el algoritmo incide en el mensaje** podemos distinguir dos tipos de cifrados :

-Cifrado en bloque: Divide el mensaje en bloques independientes, todos del mismo tamaño. Se detecta fácilmente intervenciones extrañas a través del tamaño de alguno de los bloques, es un sistema más lento al trabajar bloque a bloque y es capaz de recuperarse ante caídas del sistema.

-Cifrado en flujo: Se van cifrando los datos en continuo. Es más difícil de detectar intrusiones pero es más rápido y no se recupera ante caídas del sistema.

2. CRIPTOSISTEMAS CLÁSICOS

HISTORIA DE LA CRIPTOGRAFÍA

La Criptografía como medio de proteger la información personal es un arte tan antiguo como la propia escritura. Con la utilización de los ordenadores ha alcanzado plena madurez.

Era utilizada por los egipcios en el 2000 A.C. Durante siglos estuvo vinculada a los círculos militares y diplomáticos.

La Criptografía moderna se inicia fundamentalmente en la 2ª guerra mundial con la rotura de la máquina Enigma utilizada por los alemanes, que fue desarrollada en Alemania durante la 1ª guerra mundial. El primer intento de romper su sistema de cifrado proviene de Polonia.

Después de la caída de Polonia los polacos pasaron la información de que disponían a los franceses y británicos. Bajo la dirección del matemático Alan Turing los británicos pusieron en marcha el proyecto secreto Ultra, que se dedicó a descifrar los mensajes de la armada alemana y que propició la construcción de uno de los primeros ordenadores modernos, el Colossus.

El desarrollo de las comunicaciones electrónicas mas el uso masivo y generalizado de los ordenadores propició la transmisión y almacenamiento de grandes flujos de información confidencial que es necesario proteger, con lo que la criptografía pasa de ser una exigencia de minorías a una necesidad real del hombre.

CRIPTOSISTEMAS CLÁSICOS

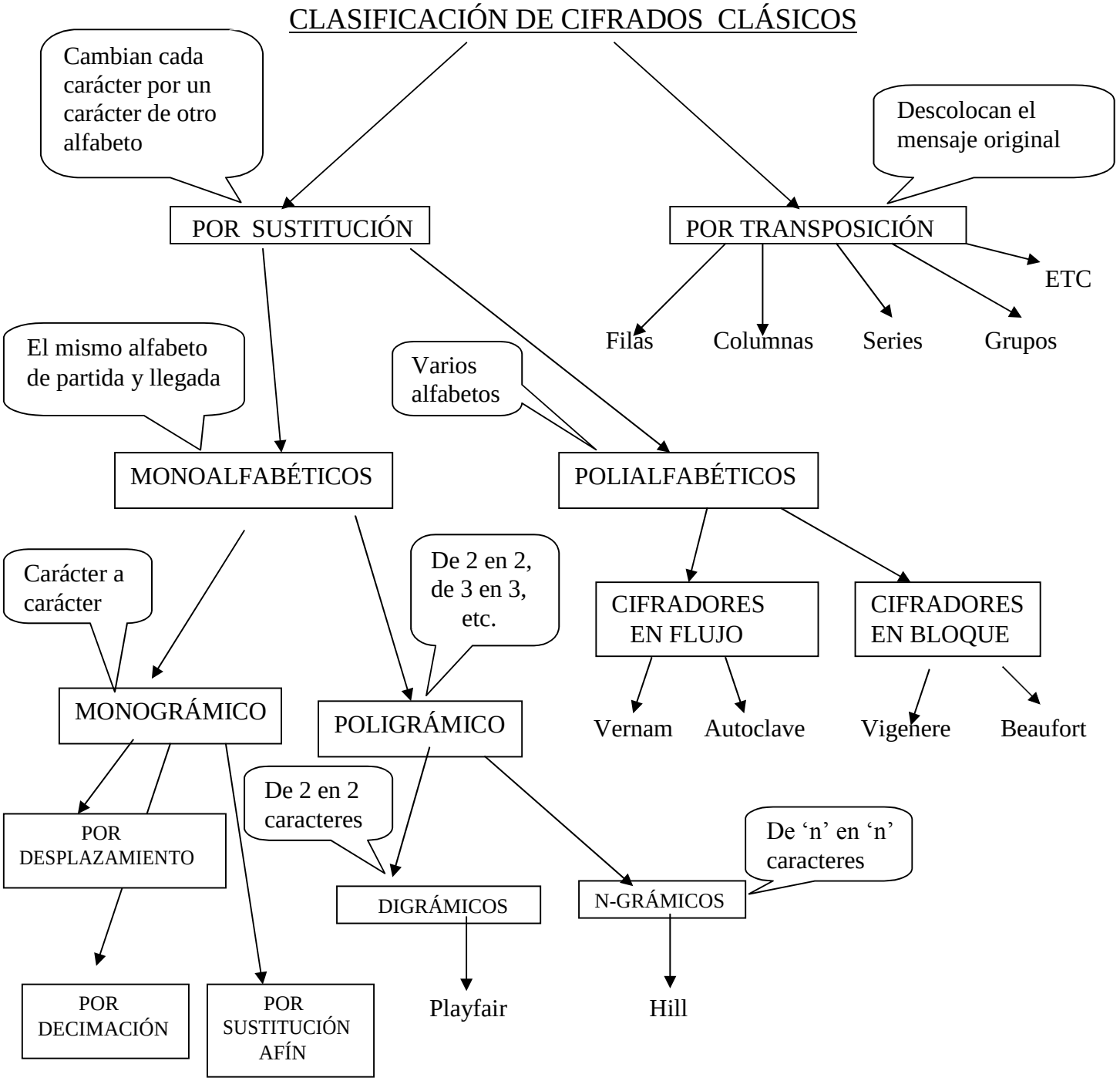
Los cifrados clásicos emplean un alfabeto de cifrado igual que el lenguaje natural. Debido a esto surgen distintos tipos de alfabetos:

-[A..Z] →27 caracteres.
-[A..Z,a..z] →54 caracteres.
-ASCII →224 caracteres.
-etc.

Si empezamos desde la posición 0, A=0, B=1,...,Z=26, de este modo podemos hacer operaciones con los caracteres, teniendo en cuenta que las operaciones más comunes en criptografía clásica son sumas y productos.

Al realizar una suma o un producto de caracteres, las cuales se realizan sobre el número asociado a cada carácter, nos da como resultado un valor entero, el

cual corresponde con el carácter asociado. Si dicho número se desborda con el número de caracteres empleado se aplica el módulo de ‘n’ (Siendo ‘n’ el conjunto de caracteres elegido).



NOTA: En un sistema polialfabético puede darse que un mismo carácter en un mensaje a enviar se encripte en dos caracteres distintos en el mensaje encriptado, mientras que en los monoalfabéticos esto no sucede.

2.1 CIFRADOS POR SUSTITUCIÓN

Conceptos:

Espacio de mensajes originales (M)
Espacio de mensajes cifrados(C)
Espacio de claves (K)
Conjunto de posibles cifrados (E)
Conjunto de correspondientes descifrados (D)
Ci, carácter del criptograma.
Mi, carácter del mensaje.
A, constante de decimación.
B, constante de desplazamiento.
N, grupo de trabajo.

Este tipo de cifrados debe cumplir tres restricciones:

1) La constante de decimación no puede ser 0 (a<>0).
2) a y n deben ser primos entre si, es decir, mcd(a,n)=1.
3) $0 \leq b \leq n-1$

Para realizar el cifrado utilizaremos esta fórmula:

$$Ci=(mi*a+b) \bmod n$$

Cada carácter del mensaje original mediante dicha fórmula obtendremos su carácter cifrado. Entonces el criptograma $C= \sum Ci$

2.1.1 Cifrado por desplazamiento puro

Este tipo de cifrado es un cifrado por sustitución, pero la constante de decimación es 1, es decir, a=1. Por lo que la fórmula anterior quedaría así:

$$Ci=(mi+b) \bmod n$$

Para obtener el criptograma: $C= \sum Ci$

Para descifrar un criptograma: $Mi= (Ci-b) \bmod n$

2.1.2 Cifrado por decimación pura

Este tipo de cifrado es un cifrado por sustitución, pero la constante de desplazamiento es nula, es decir, b=0. Por lo que la fórmula anterior quedaría así:

$$Ci=(a*mi) \bmod n$$

Para obtener el criptograma: $C= \sum Ci$

Para obtener el mensaje en claro : $Mi=(Ci / a) \bmod n$

2.1.3 Cifrado por sustitución afín

Este es exactamente un cifrado por sustitución pero además se le puede incluir una clave supletoria que mejora las características de seguridad.

Sin clave → Para realizar el cifrado utilizaremos esta fórmula:

$$Ci=(mi*a+b) \bmod n$$

Cada carácter del mensaje original mediante dicha fórmula obtendremos su carácter cifrado. Entonces el criptograma $C= \sum Ci$

Con clave → 'K' contendrá la clave y 'r' contendrá la posición donde se va a colocar la clave en cuestión en la tabla del cifrado.

1) Se han de eliminar los caracteres repetidos de la clave.
2) Colocamos la clave en la posición r+1.
3) A continuación se retorna el alfabeto del criptograma(C), comenzando por el primer carácter, y colocándolos después de la clave, eliminando los caracteres repetidos.

DESCIFRADO→ En el descifrado tenemos que realizar lo mismo que en el cifrado con la única diferencia que en el último paso tenemos que sustituir las letras del texto cifrado por las letras del alfabeto en claro.

<u>NOTA :</u> Todos estos cifrados los veremos más adelante con ejemplos en el apartado 3 .(MÉTODOS IMPLEMENTADOS)

2.2 CIFRADOS POR SUSTITUCIÓN POLIALFABÉTICA

2.2.1 VIGENERE

El sistema de cifrado de Vigenère (en honor al criptógrafo francés del mismo nombre) es un sistema polialfabético o de sustitución múltiple. Este tipo de criptosistemas aparecieron para sustituir a los monoalfabéticos o de sustitución simple, que presentaban ciertas debilidades frente al ataque de los criptoanalistas relativas a la frecuencia de aparición de elementos del alfabeto. El principal elemento de este sistema es la llamada Tabla de Vigenère, una matriz de caracteres cuadrada, con dimensión, que se muestra en la tabla siguiente :

	0	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
	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

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

El mensaje a cifrar en texto claro ha de descomponerse en bloques de elementos - letras - y aplicar sucesivamente la clave empleada a cada uno de estos bloques, utilizando la tabla anteriormente proporcionada.

Veamos un ejemplo de aplicación del criptosistema de Vigenère: queremos codificar la frase *La abrumadora soledad del programador* utilizando la clave *prueba*. En primer lugar, nos fijamos en la longitud de la clave: es de seis caracteres, por lo que descomponemos la frase en bloques de longitud seis; aunque el último bloque es de longitud tres, esto no afecta para nada al proceso de cifrado:

laabru madora soleda ddelpr ograma dor

Ahora, aplicamos a cada bloque la clave *prueba* y buscamos los resultados como entradas de la tabla de Vigenère:

laabru madora soleda ddelpr ograma dor
prueba prueba prueba prueba prueba pru
arufsu brxhsa igfiea suyoqr exmena sgm

El cifrado se ha realizado de la siguiente manera:

*Busco la L en el alfabeto de la P
*Busco la A en el alfabeto de la R
*Busco la A en el alfabeto de la U
*Busco la B en el alfabeto de la E
...
*Busco la R en el alfabeto de la U

Todo ello de tal manera que la L en el alfabeto (sin desordenar) se sustituye por la letra que ocupa esa misma posición en el alfabeto de la P (en este caso se sustituiría por la A), y así sucesivamente. De tal manera que el cifrado queda así:

arufsu brxhsa igfiea suyoqr exmena sgm.

Lo que realmente se está aplicando es:

Ci=(mi+ki)mod n

Para desencriptar el texto cifrado aplicaremos:

Mi=(Ci-ki) mod n

Este método de cifrado polialfabético se consideraba invulnerable hasta que en el S.XIX se consiguieron descifrar algunos mensajes codificados con este sistema, mediante el estudio de la repetición de bloques de letras: la distancia entre un bloque y su repetición suele ser múltiplo de la palabra tomada como clave.

2.2.2 BEAUFORT

Es una modificación del cifrado de Vigenere, en la cual en vez de sumar las letras del mensaje en claro, se suma su inversa.

El cifrado y el descifrado son la misma operación, por lo que a este cifrado se le ve como cifrado recíproco o involutivo.

Tiene las mismas debilidades que el método de Vigenere.

Ejemplo:

K=MORATILLA

HOLA ME LLAMO ANTONIO ⟶ Mensaje(∑ mi)
MORA T I LLAMO RAT I LLA ⟶ Clave (∑ ki)
FAGA HE AAAAA RNAUYDM ⟶ Mensaje cifrado (∑ ci)

Realmente lo que estamos aplicando es:

$$Ci=(Ki-mi) \bmod n$$

$C1=(12-7) \bmod 26= 5 \bmod 26 = 5 =F$
$C2=(24-24) \bmod 26=0 \bmod 26 = 0 =A$
…

Cada carácter del mensaje original mediante dicha fórmula obtendremos su carácter cifrado. Entonces el criptograma $C= \sum Ci$

Para obtener el mensaje en claro : $Mi=(Ki-Ci) \bmod n$

2.3 CIFRADOS POR SUSTITUCIÓN POLIALFABÉTICA NO PERIÓDICA

La esencia de estos cifrados es que la longitud de la clave es superior o igual a la del mensaje, de modo que se evita la repetición de la misma por bloques.

2.3.1 AUTOCLAVE

Se debe construir una tabla con los símbolos del alfabeto, se elige una clave que se escribe debajo del mensaje solo una vez, seguidamente no se repite la clave sino que se continua con el mismo mensaje, se suman ordinalmente ambas informaciones en modulo (de los caracteres que estemos utilizando), y se busca en la tabla la letra asociada a la suma, formándose el cifrado.

Mensaje: CARCEL

Clave: PAN

Aplicando el método:

Mensaje: CARCEL (2 0 17 2 4 11)
Clave: PANCAR (15 0 13 2 0 17)

Cifrado: RAEEEC

NOTA: el cifrado se ha realizado sin tener en cuenta la letra Ñ en el alfabeto

Realmente lo que se está aplicando en el cifrado es:

$Ci=(mi+ki) \bmod n$ (En este caso n=26, desde 0..25)

Para desencriptar hemos de tener en cuenta que una vez aplicada la clave primaria deberemos empezar a aplicar los caracteres decodificados que vamos obteniendo.

DESCIFRADO: $Mi=(Ci-ki) \bmod n$

CIFRADO POR CLAVE CONTINUA

En este caso únicamente se ha de trabajar con una clave cuya longitud sea efectivamente igual o mayor que la del mensaje a cifrar, utilizando como apoyo el método de Vigenere.

2.3.2 VERNAM

- Es el caso límite del cifrado de Vigenére.
- Utiliza un alfabeto binario.
- Las operaciones son módulo 2.
- La clave sólo se utiliza una vez.
- El procedimiento de cifrado y descifrado es el mismo.
- Se basa en las propiedades de la operación XOR.

Ci=(mi XOR ki) mod 2

Para poder dar un significado hemos de codificar los caracteres del alfabeto en binario empleando 5 bits para la codificación.

M= BYTES	00001	11001	10100	00100	10011
K= VERNAM	10110	00100	10010	01101	00000
C= WCGJS	10111	11101	00110	01001	10011

- Es el único cifrado incondicionalmente seguro, con seguridad total comprobada matemáticamente.

DESCIFRADO→ Como hemos dicho anteriormente el procedimiento de cifrado y descifrado es el mismo, por lo tanto:

Mi=(Ci XOR ki) mod 2

2.4 CIFRADOS POR SUSTITUCIÓN MONOALFABÉTICA POLIGRÁMICOS

2.4.1 PLAYFAIR (DIGRÁMICO)

Este sistema criptográfico fue inventado en 1854 por Charles Wheatstone, pero debe su nombre al Baron Playfair de St Andrews quien promovió el uso de este criptosistema.

El algoritmo utiliza una tabla o matriz de 5x5.

La tabla se llena con una palabra o frase secreta descartando las letras repetidas. Se rellenan los espacios de la tabla con las letras del alfabeto en orden. Usualmente se omite la "W" y se utiliza la "V" en su lugar o se reemplazan las "J" por "I". Esto se hace debido a que la tabla tiene 25 espacios y el alfabeto tiene 26 símbolos. La frase secreta usualmente se ingresa a la tabla de izquierda a derecha y arriba hacia abajo o en forma de espiral, pero puede utilizarse algún otro patrón. La frase secreta junto con las convenciones para llenar la tabla de 5x5 constituyen la clave de encriptación.

Por ejemplo:

Si la frase secreta es "CRIPTOSISTEMA PLAYFAIR"

Llenaremos de izquierda a derecha y arriba hacia abajo y omitiremos la W

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

La encriptación se realiza de la siguiente forma:

El mensaje original que se desea encriptar es dividido en bloques de dos caracteres cada uno y se le aplican las siguientes cuatro reglas en orden

Si en el bloque las dos letras son la misma, se reemplaza la segunda generalmente por una X (o alguna letra poco frecuente) y se encripta el nuevo par.

Si las dos letras del bloque aparecen en la misma fila de la tabla, cada una se reemplaza por la letra adyacente que se encuentra a su derecha (si es la letra que se encuentra en la última posición a la derecha de la fila se la reemplaza con la primera de la izquierda de esa fila). Ej. SM se reemplazará por EA y AE por OM.

Si las dos letras del bloque aparecen en la misma columna de la tabla, cada una se reemplaza por la letra adyacente que se encuentra por debajo (si es la letra que se encuentra en la última posición inferior de la columna se reemplaza con la primera de arriba de esa columna). Ej. LC se reemplazará por GO y GQ por QC.

Si las letras no se encuentran en la misma fila ni columna se determina el rectángulo formado por los dos caracteres y se encripta tomando los caracteres que están en las esquinas del rectángulo y en la misma fila que el carácter a encriptar. Ej. SB se reemplazará por MY y KR por HP.

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

Para desencriptar se aplican estas cuatro reglas en forma inversa, descartando las "X" que no tengan sentido en el mensaje final.

Ejemplo:

Si queremos codificar "LENGUAJE"

Tomamos "LE" como no están ni en la misma fila ni columna se utiliza la regla 4, "LE" se reemplaza por "FO".

Tomamos "NG" como están en la misma fila utilizamos la regla 2, "NG" se reemplaza por "GH".

Luego, tomamos "UA" como no están ni en la misma fila ni columna se utiliza la regla 4, "UA" se reemplaza por "ZS".

Finalmente tomamos "JE" como están en la misma columna utilizamos la regla 3, "JE" se reemplaza por "VF".

Por lo tanto "LENGUAJE se encriptará como ""FOGHZSVF"

De este esquema podemos deducir que el sistema es polialfabético pues por ejemplo "LE"="FO" implica que "E"="O" y "JE"="VF" implica que "E"="F" lo cual demuestra que el sistema es polialfabético. En el sistema Playfair si bien no es cierto que todo carácter siempre sea encriptado en un mismo carácter si vale que todo par de caracteres siempre sea encriptado en el mismo par de caracteres, por lo que en lugar de decir que el sistema es polialfabético podemos decir que es monoalfabético de orden 2.

Criptoanálisis:

El sistema Playfair es un sistema de encriptación bastante bueno, la cantidad de posibles claves es enorme ya que son las permutaciones de 25 elementos tomados de entre 26 lo cual da un número muy grande como para derrotar al algoritmo por fuerza bruta. Además es un sistema polialfabético por lo que un análisis de la frecuencia de aparición de cada carácter en el código cifrado no nos aporta nada.

2.4.2 HILL (N-GRÁMICA)

Este sistema está basado en el álgebra lineal y ha sido importante en la historia de la criptografía. Fue Inventado por Lester S. Hill en 1929, y fue el primer sistema criptográfico polialfabético que era práctico para trabajar con más de tres símbolos simultáneamente.

Este sistema es polialfabético pues puede darse que un mismo carácter en un mensaje a enviar se encripte en dos caracteres distintos en el mensaje encriptado.

Suponiendo que trabajamos con un alfabeto de 26 caracteres.

Las letras se numeran en orden alfabético de forma tal que A=0, B=1,..., Z=25

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Se elije un entero d que determina bloques de d elementos que son tratados como un vector de d dimensiones.

Se elije de forma aleatoria una matriz de d × d elementos los cuales serán la clave a utilizar.

Los elementos de la matriz de d × d serán enteros entre 0 y 25, además la matriz M debe ser inversible en $\mathbb{Z}_{26}^{n}$.

Para la encriptación, el texto es dividido en bloques de d elementos los cuales se multiplican por la matriz d × d

Todas las operaciones aritméticas se realizan en la forma modulo 26, es decir que 26=0, 27=1, 28=2 etc.

Dado un mensaje a encriptar debemos tomar bloques del mensaje de "d" caracteres y aplicar:

$M \times P_i = C$, donde C es el código cifrado para el mensaje P_i

Ejemplo:

Si tomamos la matriz $A=\begin{pmatrix}5 & 17 & 20\\ 9 & 23 & 3\\ 2 & 11 & 13\end{pmatrix}$ como matriz de claves.

Para encriptar el mensaje "CODIGO" debemos encriptar los seis caracteres de "CODIGO" en bloques de 3 caracteres cada uno, el primer bloque

$$P_1=\text{"COD"}=\begin{pmatrix}2\\ 14\\ 3\end{pmatrix} \qquad P_2=\text{"IGO"}=\begin{pmatrix}6\\ 8\\ 14\end{pmatrix}$$

$$A\cdot P_1=\begin{pmatrix}5 & 17 & 20\\ 9 & 23 & 3\\ 2 & 11 & 13\end{pmatrix}\begin{pmatrix}2\\ 14\\ 3\end{pmatrix}=\begin{pmatrix}308\\ 349\\ 197\end{pmatrix}=\begin{pmatrix}22\\ 11\\ 15\end{pmatrix}(\text{mod}\,26)$$

El primer bloque "COD" se codificara como "WLP"

$$A\cdot P_2=\begin{pmatrix}5 & 17 & 20\\ 9 & 23 & 3\\ 2 & 11 & 13\end{pmatrix}\begin{pmatrix}8\\ 6\\ 14\end{pmatrix}=\begin{pmatrix}422\\ 252\\ 264\end{pmatrix}=\begin{pmatrix}6\\ 18\\ 4\end{pmatrix}(\text{mod}\,26)$$

El segundo bloque "IGO" se codificara como "GSE"

Luego 'CODIGO' encriptado equivale a 'WLPGSE'.

Observar que las dos "O" se codificaran de forma diferente.

Para desencriptar el método es idéntico al anterior pero usando la matriz inversa de la usada para encriptar.

Cálculo de la matriz inversa

Antes que nada debemos verificar que la matriz elegida sea invertible en modulo 26. Hay una forma relativamente sencilla de averiguar esto a través del cálculo del determinante. Si el determinante de la matriz es 0 o tiene factores comunes con el módulo (en el caso de 26 los factores son 2 y 13), entonces la matriz no puede utilizarse. Al ser 2 uno de los factores de 26 muchas matrices no podrán utilizarse (no servirán todas en las que su determinante sea 0, un múltiplo de 2 o un múltiplo de 13).

Para ver si es invertible calculo el determinante de A

$$\begin{vmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{vmatrix}$$

$5\ (23 \cdot 13 - 3 \cdot 11) - 17\ (9 \cdot 13 - 3 \cdot 2) + 20\ (9 \cdot 11 - 23 \cdot 2) =$

$1215 - 1734 + 1060 = 503$

$503 = 9 \bmod 26$

La matriz A es invertible en modulo 26 ya que 26 y 9 son coprimos

Para hallar la inversa de la matriz modulo 26, utilizamos la formula

$$A^{-1} = C^{T} \cdot \left(\det(A)\right)^{-1}$$

Donde CT es la matriz de cofactores de A transpuesta

Hay que tener en cuenta que $\left(\det(A)\right)^{-1}$ debe realizarse en modulo 26

por lo tanto para el ejemplo la inversa de 9 (mod 26) es 3 (mod 26) ya que

9 (mod 26) · 3 (mod 26) = 27 mod 26 = 1 (mod 26)

Por lo tanto 3 es la inversa multiplicativa de 9 en modulo 26

Para calcular C hay que calcular los cofactores de A

$$C_{11} = +\begin{vmatrix} 23 & 3 \\ 11 & 13 \end{vmatrix} \qquad C_{12} = -\begin{vmatrix} 9 & 3 \\ 2 & 13 \end{vmatrix} \qquad C_{13} = +\begin{vmatrix} 9 & 23 \\ 2 & 11 \end{vmatrix}$$

$$C_{21} = -\begin{vmatrix} 17 & 20 \\ 11 & 13 \end{vmatrix} \qquad C_{22} = +\begin{vmatrix} 5 & 20 \\ 2 & 13 \end{vmatrix} \qquad C_{23} = -\begin{vmatrix} 5 & 17 \\ 2 & 11 \end{vmatrix}$$

$$C_{31} = +\begin{vmatrix} 17 & 20 \\ 23 & 3 \end{vmatrix} \qquad C_{23} = -\begin{vmatrix} 5 & 20 \\ 9 & 3 \end{vmatrix} \qquad C_{33} = +\begin{vmatrix} 5 & 17 \\ 9 & 23 \end{vmatrix}$$

$$C = \begin{pmatrix} 266 & -111 & 53 \\ -1 & 25 & -21 \\ -409 & 165 & -38 \end{pmatrix} \qquad C^T = \begin{pmatrix} 266 & -1 & -409 \\ -111 & 25 & 165 \\ 53 & -21 & -38 \end{pmatrix}$$

Ahora aplicamos la formula de la inversa

$$A^{-1} = C^T \cdot \left(\det(A)\right)^{-1} = \begin{pmatrix} 266 & -1 & -409 \\ -111 & 25 & 165 \\ 53 & -21 & -38 \end{pmatrix} \cdot 3$$

$$A^{-1} = \begin{pmatrix} 798 & -3 & -1227 \\ -333 & 75 & 495 \\ 159 & -63 & -114 \end{pmatrix} \qquad A^{-1} = \begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix} (\mathrm{mod}\, 26)$$

Esta última es la matriz que utilizamos para desencriptar.

Criptoanálisis

El sistema de Hill plantea a los criptoanalistas muchos problemas. Para empezar el espacio de claves es mucho mayor, en este caso es de 4C25, es decir las permutaciones de 4 elementos tomados de entre 25 posibles. Y usando una matriz más grande la cantidad de posibles claves se puede hacer tan grande como sea necesario para hacer que sea imposible un ataque por fuerza bruta.

Lo mejor que puede hacer un criptoanalista es tratar de conseguir un código para el cual se conozca una parte del mensaje. Y ver si con ambos datos es capaz de encontrar cual fue la matriz utilizada para encriptar el mensaje.

2.5 CIFRADOS POR TRANSPOSICIÓN

- Por grupos.
- Por series.
- Por filas y por columnas.

2.5.1 GRUPOS

Se divide el mensaje en bloques de p elementos, siendo p el número de caracteres de la clave. Los números de la clave indican el carácter que ocupa cada posición en el criptograma.

M= HOLA ME LLAMO RAYCO
K= (2 4 5 3 1)

H	**O**	**L**	**A**		**M**	**E**		**L**	**L**	**A**	**M**	**O**		**R**	**A**	**Y**	C	**O**		**X**	**X**	**X**	**X**		
1	2	3	4		5	1		2	3	4	5	1		2	3	4	5	1		2	3	4	5		
O	**A**	**M**	**L**		**H**	**L**		**A**	**M**	**L**	**E**	**R**		**Y**	**C**	**A**	**O**	**X**		**X**	**X**	**X**	**O**		
2	4	5	3		1	2		4	5	3	1	2		4	5	3	1	2		4	5	3	1		

Para desencriptar se enumera el texto cifrado según la clave y se cogen las letras en orden ascendente.

NOTAS:

- Dos letras que tengan la misma numeración siempre tendrá prioridad la que esté a la izquierda.

- Las posiciones sobrantes para llegar al número de caracteres que indica la clave se rellenan con el carácter especial convenido (en este caso X).

2.5.2 TRANSPOSICIÓN POR SERIES

Consiste en definir un conjunto de series y en el orden deseado, es decir, las series pueden ser las mismas en un cifrado que en otro y salir diferentes cifrados debido a que dichas series están en diferente orden.

EJEMPLO:

Serie 1 = números primos =1 2 3 5 7 11 13 17 19
Serie 2 = pares no tomados = 4 6 8 10 12 14 16 18 20 22
Serie 3 = impares no tomados = 9 15 21

M= TRANSFIÉREME LOS CÓDIGOS

T	**R**	**A**	**N**	**S**	**F**	**I**	**É**	**R**	**E**	**M**	**E**		**L**	**O**	**S**		**C**	**Ó**	**D**	**I**	**G**	**O**	**S**
1	2	3	4	5	6	7	8	9	10	11	12		13	14	15		16	17	18	19	20	21	22
T	**R**	**A**	**S**	**I**	**M**	**L**	**Ó**	**I**	**N**	**F**	**É**		**E**	**E**	**O**		**C**	**D**	**G**	**S**	**R**	**S**	**O**
1	2	3	5	7	11	13	17	19	4	6	8		10	12	14		16	18	20	22	9	15	21

Para desencriptar se enumera el texto cifrado según las series y se cogen las letras en orden ascendente.

NOTA: Tenemos que tener en cuenta el mensaje a cifrar cuando vamos a definir las series.

2.5.3 TRANSPOSICIÓN POR FILAS

El mensaje original se coloca en una matriz en columnas (un carácter por cada fila). La codificación resulta de la escritura del mensaje por filas. Las posiciones sobrantes en la matriz se rellenan con el carácter especial convenido.

Parámetros→ Nf = número de filas de la matriz para codificar la información.

La descodificación se realizará formando una matriz de Nf x | C | /Nf (donde | C | es el número de caracteres del mensaje codificado) y colocando el mensaje codificado por filas en la matriz y obteniéndolo por columnas.

Ejemplo 1

Cifrado

Nf = 5
M = "HACE UN BUEN DIA EN TELDE"

H	U	E	A	T
A	N	N		E
C			E	L
E	B	D	N	D
	U	I		E

El mensaje lo hemos colocado por columnas en una matriz de 5 filas (como indica el parámetro Nf).

La codificación del mensaje consiste en recogerlo por filas, de ahí deriva el nombre del método.

M = "HACE UN BUEN DIA EN TELDE"

Obtenemos el mensaje cifrado:

C = “HUEATANN EC ELEBDND UI E”

Descifrado

Nf = 5
C = “HUEATANN EC ELEBDND UI E”

Para descifrar ponemos el mensaje cifrado por filas y lo recogemos por columnas (sabiendo que el número de filas es 5 en la matriz).

C = “HUEATANN EC ELEBDND UI E”

Obtenemos el mensaje:

M = “HACE UN BUEN DIA EN TELDE”

Ejemplo 2

Cifrado

Nf = 2
M= “INFORMÁTICA”

El mensaje lo hemos colocado por columnas en una matriz de 2 filas (como indica el parámetro Nf).

La codificación del mensaje consiste en recogerlo por filas, de ahí deriva el nombre del método.

Las posiciones sobrantes en la matriz se rellenan con el carácter especial convenido.

M = “INFORMÁTICA”

Obtenemos el mensaje codificado :

C = “IFRÁIANOMTC/”

Descifrado

Nf = 2
C = “IFRÁIANOMTC/”

Para descifrar ponemos el mensaje cifrado por filas y lo recogemos por columnas (sabiendo que el número de filas es 2 en la matriz).

El carácter especial convenido ‘/’ se ignora.

C = “IFRÁIANOMTC/”

Obtenemos el mensaje:

M = “INFORMÁTICA”

Ejemplo 3

Cifrado

Nf = 8
M = “MÁS VALE PÁJARO EN MANO QUE CIENTO VOLANDO”

M		E	Q	T	D
Á	P	N	U	O	O
S	Á		E		/
	J	M		V	/
V	A	A	C	O	/
A	R	N	I	L	/
L	O	O	E	A	/
E			N	N	/

El mensaje lo hemos colocado por columnas en una matriz de 8 filas (como indica el parámetro Nf).

La codificación del mensaje consiste en recogerlo por filas, de ahí deriva el nombre del método.

Las posiciones sobrantes en la matriz se rellenan con el carácter especial convenido.

M = “MÁS VALE PÁJARO EN MANO QUE CIENTO VOLANDO”

Obtenemos el mensaje cifrado:

C = “M EQTDÁPNUOOSÁ E / JM V/VAACO/ARNIL/LOOEA/E NN/”

Descifrado

Nf = 8
C = “M EQTDÁPNUOOSÁ E / JM V/VAACO/ARNIL/LOOEA/E NN/”

Para descifrar ponemos el mensaje cifrado por filas y lo recogemos por columnas (sabiendo que el número de filas es 8 en la matriz).

El carácter especial convenido ‘/’ se ignora.

C = “M EQTDÁPNUOOSÁ E / JM V/VAACO/ARNIL/LOOEA/E NN/”

Obtenemos el mensaje:

M = “MÁS VALE PÁJARO EN MANO QUE CIENTO VOLANDO”

2.5.4 TRANSPOSICIÓN POR COLUMNAS

Sigue la misma teoría que el método anterior; solo que esta vez Nc nos indica el número de columnas y el mensaje en claro se sitúa por filas (un carácter por cada columna). Las posiciones sobrantes en la matriz se rellenan con el carácter especial convenido.

Parámetros → Nc = número de columnas de la matriz para codificar la Información.

El descifrado se realiza colocando el mensaje codificado en una matriz de | C |/ Nc x Nc en columnas (un carácter por cada fila) y obteniéndolo por filas.

Ejemplo 1

Cifrado

Nc = 3
M = "MIÉRCOLES"

M	I	É
R	C	O
L	E	S

El mensaje lo hemos colocado por filas en una matriz de 3 columnas (como indica el parámetro Nc).

La codificación del mensaje consiste en recogerlo por columnas, de ahí deriva el nombre del método.

Las posiciones sobrantes en la matriz se rellenan con el carácter especial convenido.

M = “MIÉRCOLES”

Obtenemos el mensaje cifrado:

C = “MRLICEÉOS”

Descifrado

Nc = 3
C = “MRLICEÉOS”

Para descifrar ponemos el mensaje cifrado por columnas y lo recogemos por filas (sabiendo que el número de columnas es 3 en la matriz).

El carácter especial convenido ‘/’ se ignora.

C = “MRLICEÉOS”

Obtenemos el mensaje :

M = “MIÉRCOLES”

Ejemplo 2

Cifrado

Nc = 5
M = “DELITO INFORMÁTICO”

D	E	L	I	T
O		I	N	F
O	R	M	Á	T
I	C	O	/	/

El mensaje lo hemos colocado por filas en una matriz de 5 columnas (como indica el parámetro Nc).

La codificación del mensaje consiste en recogerlo por columnas.

Las posiciones sobrantes en la matriz se rellenan con el carácter especial convenido.

M = “DELITO INFORMÁTICO”

Obtenemos el mensaje cifrado:

C = “DOOIE RCLIMOINÁ/TFT/”

Descifrado

Nc = 5
C = “DOOIE RCLIMOINÁ/TFT/”

Para descifrar ponemos el mensaje cifrado por columnas y lo recogemos por filas (sabiendo que el número de columnas es 5 en la matriz).

El carácter especial convenido ‘/’ se ignora.

C = “DOOIE RCLIMOINÁ/TFT/”

Obtenemos el mensaje:

M = “DELITO INFORMÁTICO”

Ejemplo 3

Cifrado

Nc = 8
M = “MÁS VALE MALO CONOCIDO QUE BUENO POR CONOCER”

M	Á	S		V	A	L	E
	M	A	L	O		C	O
N	O	C	I	D	O		Q
U	E		B	U	E	N	O
	P	O	R		C	O	N
O	C	E	R	/	/	/	/

El mensaje lo hemos colocado por filas en una matriz de 8 columnas (como indica el parámetro Nc).

La codificación del mensaje consiste en recogerlo por columnas.

Las posiciones sobrantes en la matriz se rellenan con el carácter especial convenido.

M = “MÁS VALE MALO CONOCIDO QUE BUENO POR CONOCER”

Obtenemos el mensaje cifrado:

C = “M NU OÁMOEPCSAC OE LIBRRVODU /A OEC/LC NO/EOQON/”

Descifrado

Nc = 8
C = “M NU OÁMOEPCSAC OE LIBRRVODU /A OEC/LC NO/EOQON/”

Para descifrar ponemos el mensaje cifrado por columnas y lo recogemos por filas (sabiendo que el número de columnas es 8 en la matriz).

El carácter especial convenido ‘/’ se ignora.

C = “M NU OÁMOEPCSAC OE LIBRRVODU /A OEC/LC NO/EOQON/”

Obtenemos el mensaje:

M = “MÁS VALE MALO CONOCIDO QUE BUENO POR CONOCER”

3. MÉTODOS IMPLEMENTADOS

Los métodos implementados en este Trabajo Fin de Grado: Cifrado por decimación, cifrado por desplazamiento puro, cifrado por sustitución afín, han sido elegidos por ser sistemas que solo utilizan un alfabeto de sustitución lo cual proporciona mayor rapidez a la hora de encriptar y desencriptar mensajes o archivos de texto.

En este Trabajo Fin de Grado se ha priorizado que el sistema implementado tenga una mayor capacidad de respuesta, primando la rapidez de estos sistemas frente a los cifrados polialfabéticos, los cuales utilizan varios alfabetos siendo más lentos y con menor capacidad de respuesta para encriptar/desencriptar mensajes o archivos de texto.

3.1 CIFRADOS POR SUSTITUCIÓN

Antes de empezar con los ejemplos de los métodos de sustitución tenemos que recordar características y conceptos importantes para poder entender completamente como funcionan dichos métodos. Por tanto a continuación se plantean las características importantes de estos métodos:

Conceptos:

Espacio de mensajes originales (M)
Espacio de mensajes cifrados (C)
Espacio de claves (K)
Conjunto de posibles cifrados (E)
Conjunto de correspondientes descifrados (D)
Ci, carácter del criptograma.
Mi, carácter del mensaje.
A, constante de decimación.
B, constante de desplazamiento.
N, grupo de trabajo.

Este tipo de cifrados debe cumplir tres restricciones:

1) La constante de decimación no puede ser 0 (a<>0).
2) a y n deben ser primos entre si, es decir, mcd(a,n)=1.
3) $0 \leq b \leq n-1$

Para realizar el cifrado utilizaremos esta fórmula:

Ci=(mi*a+b) mod n

Cada carácter del mensaje original mediante dicha fórmula obtendremos su carácter cifrado. Entonces el criptograma C= ∑ Ci

3.1.1 CIFRADO POR DECIMACIÓN

Condiciones → b=0

EJEMPLO 1:

Cifrado

a= 2
M = "MAS VALE PAJARO EN MANO"

Recordemos la siguiente fórmula: Ci=(mi*a) mod 27

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**
0	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
A	**C**	**E**	**G**	**I**	**K**	**M**	**Ñ**	**P**	**R**	**T**	**V**	**X**	**Z**	**B**	**D**	**F**	**H**	**J**	**L**	**N**	**O**	**Q**	**S**	**U**	**W**	**Y**
0	2	4	6	8	10	12	14	16	18	20	22	24	26	1	3	5	7	9	11	13	15	17	19	21	23	25

Una vez construida esta tabla ya podemos codificar el mensaje sin ningún tipo de problema.

C = "XALQA VIFAR AJDIZ XAZD" →Por convenio reunimos los caracteres del mensaje cifrado en bloques de 5.

Descifrado

a=2
C = "XALQA VIFAR AJDIZ XAZD"

- Construimos el alfabeto con decimación 2 a partir del alfabeto español, de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto con decimación 2 al alfabeto español (proceso inverso al cifrado), como se muestra a continuación:

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**
0	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
A	**C**	**E**	**G**	**I**	**K**	**M**	**Ñ**	**P**	**R**	**T**	**V**	**X**	**Z**	**B**	**D**	**F**	**H**	**J**	**L**	**N**	**O**	**Q**	**S**	**U**	**W**	**Y**
0	2	4	6	8	10	12	14	16	18	20	22	24	26	1	3	5	7	9	11	13	15	17	19	21	23	25

C = “XALQA VIFAR AJDIZ XAZD”

Obtenemos el mensaje:

M= “MAS VALE PAJARO EN MANO”

El proceso real que estamos realizando al descifrar es el siguiente:

Mi= (Ci/ a) mod n (n=27 en este caso)

EJEMPLO 2:

Cifrado

a = 22
M= “RAYCO SEGURA TAVIO”

Recordemos la siguiente fórmula: Ci=(mi*a) mod 27

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**
0	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
A	**V**	**Q**	**M**	**H**	**C**	**X**	**S**	**Ñ**	**J**	**E**	**Z**	**U**	**P**	**L**	**G**	**B**	**W**	**R**	**N**	**I**	**D**	**Y**	**T**	**O**	**K**	**F**
0	22	17	12	7	2	24	19	14	9	4	26	21	16	11	6	1	23	18	13	8	3	25	20	15	10	5

Una vez construida esta tabla ya podemos codificar el mensaje sin ningún tipo de problema.

C= “RAKQG NHXDR AIAYÑ G”

Descifrado

a = 22
C= “RAKQG NHXDR AIAYÑ G”

- Construimos el alfabeto con decimación 22 a partir del alfabeto español, de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto con decimación 22 al alfabeto español (proceso inverso al cifrado), como se muestra a continuación:

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**
0	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
A	**V**	**Q**	**M**	**H**	**C**	**X**	**S**	**Ñ**	**J**	**E**	**Z**	**U**	**P**	**L**	**G**	**B**	**W**	**R**	**N**	**I**	**D**	**Y**	**T**	**O**	**K**	**F**
0	22	17	12	7	2	24	19	14	9	4	26	21	16	11	6	1	23	18	13	8	3	25	20	15	10	5

Hay que tener en cuenta que la constante de decimación no puede ser el 3 ni el 9,..., ya que el Mcd (a,n) no es igual a 1, siendo n=27.

Una vez construida esta tabla ya podemos descodificar el mensaje sin ningún tipo de problema.

C= “RAKQG NHXDR AIAYÑ G”

Obtenemos el mensaje:

M= “RAYCO SEGURA TAVIO”

El proceso real que estamos realizando al descifrar es el siguiente:

Mi= (Ci/ a) mod n (n=27 en este caso)

EJEMPLO 3:

Cifrado

a= 16
M= “HACE UN BUEN DIA”

Ci=(mi*a) mod 27

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**
0	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
A	**P**	**F**	**U**	**K**	**Z**	**O**	**E**	**T**	**J**	**Y**	**Ñ**	**D**	**S**	**I**	**X**	**N**	**C**	**R**	**H**	**W**	**M**	**B**	**Q**	**G**	**V**	**L**
0	16	5	21	10	26	15	4	20	9	25	14	3	19	8	24	13	2	18	7	23	12	1	17	6	22	11

A partir de esta tabla ya podemos codificar el mensaje.

C= “EAFKM SPMKS UTA”

Descifrado

a= 16
C= “EAFKM SPMKS UTA”

- Construimos el alfabeto con decimación 16 a partir del alfabeto español, de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto con decimación 16 al alfabeto español (proceso inverso al cifrado), como se muestra a continuación:

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**
0	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
A	**P**	**F**	**U**	**K**	**Z**	**O**	**E**	**T**	**J**	**Y**	**Ñ**	**D**	**S**	**I**	**X**	**N**	**C**	**R**	**H**	**W**	**M**	**B**	**Q**	**G**	**V**	**L**
0	16	5	21	10	26	15	4	20	9	25	14	3	19	8	24	13	2	18	7	23	12	1	17	6	22	11

Una vez construida esta tabla ya podemos descodificar el mensaje.

C= “EAFKM SPMKS UTA”

Obtenemos el mensaje:

M= “HACE UN BUEN DIA”

El proceso real que estamos realizando al descifrar es el siguiente:

Mi= (Ci/ a) mod n (n=27 en este caso)

3.1.2 CIFRADO POR DESPLAZAMIENTO PURO

Condiciones → a=1

Ejemplo1

Cifrado

b= 6
M= “HACE UN BUEN DIA”

Recordemos la siguiente fórmula: Ci= (mi+b) mod n ; a=1

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**
0	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
G	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5

Una vez construida esta tabla ya podemos codificar el mensaje sin ningún tipo de problema.

M= “HACE UN BUEN DIA”

Obtenemos el siguiente cifrado:

C= “NGIKA SHAKS JÑG” → Por convenio agrupamos los caracteres de 5 en 5

Descifrado

b=6
C= “NGIKA SHAKS JÑG”

Recordemos la siguiente fórmula : Mi= (Ci-b) mod n (n=27)

- Construimos el alfabeto con desplazamiento 6 a partir del alfabeto español, de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto con desplazamiento 6 al alfabeto español (proceso inverso al cifrado), como se muestra a continuación:

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**
0	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
G	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5

Una vez construida esta tabla ya podemos descodificar el mensaje.

C= “NGIKA SHAKS JÑG”

Obtenemos el mensaje:

M= “HACE UN BUEN DIA”

El proceso real que estamos realizando al descifrar es el siguiente:

Mi= (Ci-b) mod n (n=27 en este caso)

Ejemplo 2

Cifrado

b= 18
M= “RAYCO SEGURA TAVIO”

Recordemos la siguiente fórmula: Ci= (mi+b) mod n ; a=1

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**
0	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
R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**
18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Una vez construida esta tabla ya podemos codificar el mensaje.

C= “JRPTG KVXMJ RLRNZG” → Por convenio agrupamos los caracteres de 5 en 5.

Descifrado

b= 18
C= “JRPTG KVXMJ RLRNZG”

- Construimos el alfabeto con desplazamiento 18 a partir del alfabeto español de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto con desplazamiento 18 al alfabeto español (proceso inverso al cifrado), como se muestra a continuación:

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**
0	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
R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**
18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Una vez construida esta tabla ya podemos descodificar el mensaje.

C= “JRPTG KVXMJ RLRNZG”

Obtenemos el mensaje:

M= “RAYCO SEGURA TAVIO”

El proceso real que estamos realizando al descifrar es el siguiente:

Mi= (Ci-b) mod n (n=27 en este caso)

Ejemplo 3

Cifrado

b= 25
M= “MAS VALE PAJARO EN MANO”

Ci= (mi+b) mod n;

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**
0	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
Y	**Z**	**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**
25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

C= “KYQTY JCÑYH YPNCL KYLN”

Descifrado

b= 25
C= “KYQTY JCÑYH YPNCL KYLN

- Construimos el alfabeto con desplazamiento 25 a partir del alfabeto español, de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto con desplazamiento 25 al alfabeto español (proceso inverso al cifrado), como se muestra a continuación:

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**
0	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
Y	**Z**	**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**
25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Una vez construida esta tabla ya podemos descodificar el mensaje.

C= “KYQTY JCÑYH YPNCL KYLN

Obtenemos el mensaje:

M= “MAS VALE PAJARO EN MANO”

El proceso real que estamos realizando al descifrar es el siguiente:

Mi= (Ci-b) mod n (n=27 en este caso)

3.1.3 CIFRADO POR SUSTITUCIÓN AFÍN

Ejemplo 1

Cifrado

a= 4
b= 1
n= 27

M= “HOLA QUE TAL”

Recordemos la siguiente fórmula:

Ci = (mi*a + b) mod n	⟶	Mcd(a,n) = 1

- Construimos el alfabeto con desplazamiento 1 y con decimación 4 a partir del alfabeto español.

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**
0	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
B	**F**	**J**	**N**	**Q**	**U**	**Y**	**C**	**G**	**K**	**Ñ**	**R**	**V**	**Z**	**D**	**H**	**L**	**O**	**S**	**W**	**A**	**E**	**I**	**M**	**P**	**T**	**X**
1	5	9	13	17	21	25	2	6	10	14	18	22	26	3	7	11	15	19	23	0	4	8	12	16	20	24

Una vez hemos construido la tabla ya podemos codificar el mensaje.

M= “HOLA QUE TAL”

Obtenemos el cifrado del mensaje:

C= “CHRBO EQABR”

Se puede añadir a los cifrados de sustitución una clave supletoria que mejora las características de seguridad, veamos su modo de empleo:

Clave → k = "INFORMATICA"
R → r = 2

Se han de eliminar los caracteres repetidos de la clave. Se coloca en la posición r+1 de la tabla, y a continuación se retorna el alfabeto de C (en este caso el alfabeto de C es : B F J N Q U Y …), comenzando por el primer carácter, y colocándolos después de la clave, eliminando los caracteres repetidos. Como se muestra a continuación:

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**
0	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
B	**F**	**J**	**N**	**Q**	**U**	**Y**	**C**	**G**	**K**	**Ñ**	**R**	**V**	**Z**	**D**	**H**	**L**	**O**	**S**	**W**	**A**	**E**	**I**	**M**	**P**	**T**	**X**
1	5	9	13	17	21	25	2	6	10	14	18	22	26	3	7	11	15	19	23	0	4	8	12	16	20	24
P	X	***I***	***N***	***F***	***O***	***R***	***M***	***A***	***T***	***C***	**B**	**J**	**Q**	**U**	**Y**	**G**	**K**	**Ñ**	**V**	**Z**	**D**	**H**	**L**	**S**	**W**	**E**

Una vez construida la tabla podemos realizar el cifrado. Para ello nos tenemos que fijar en el primer y tercer alfabeto, ya que el segundo es un paso intermedio para llegar al tercer alfabeto.

M= "HOLA QUE TAL"

Obtenemos el siguiente cifrado:

C = "MYBPK DFZPB"

Descifrado

a= 4
b= 1
n= 27
Clave → k = "INFORMATICA"
R → r = 2

C = "MYBPK DFZPB"

- Construimos el alfabeto con desplazamiento 1 y con decimación 4 a partir del alfabeto español, de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto creado al alfabeto español (proceso inverso al cifrado), como se muestra a continuación:

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**
0	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
B	**F**	**J**	**N**	**Q**	**U**	**Y**	**C**	**G**	**K**	**Ñ**	**R**	**V**	**Z**	**D**	**H**	**L**	**O**	**S**	**W**	**A**	**E**	**I**	**M**	**P**	**T**	**X**
1	5	9	13	17	21	25	2	6	10	14	18	22	26	3	7	11	15	19	23	0	4	8	12	16	20	24
P	X	***I***	***N***	***F***	***Q***	***R***	***M***	***A***	***T***	***C***	**B**	**J**	**Q**	**U**	**Y**	**G**	**K**	**Ñ**	**V**	**Z**	**D**	**H**	**L**	**S**	**W**	**E**

Una vez construida la tabla podemos realizar el descifrado. Para ello nos tenemos que fijar en el tercer y primer alfabeto, ya que el segundo es un paso intermedio para llegar al tercer alfabeto.

C = “MYBPK DFZPB”

Obtenemos el siguiente mensaje:

M= “HOLA QUE TAL”

Si el descifrado lo queremos realizar sin clave entonces nos tendríamos que fijar en el segundo y primer alfabeto(sabiendo que el mensaje cifrado es distinto al mensaje cifrado con clave).

C= “CHRBO EQABR”

Obtenemos el mensaje:

M= “HOLA QUE TAL”

Ejemplo 2

Cifrado

a= 16
b= 14
n= 27

M= “CORREO ELECTRONICO”

Recordemos la siguiente fórmula:

$Ci = (mi*a + b) \bmod n$ ⟶ $Mcd(a,n) = 1$

- Construimos el alfabeto con desplazamiento 14 y con decimación 16 a partir del alfabeto español.

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**
0	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
Ñ	**D**	**S**	**I**	**X**	**N**	**C**	**R**	**H**	**W**	**M**	**B**	**Q**	**G**	**V**	**L**	**A**	**P**	**F**	**U**	**K**	**Z**	**O**	**E**	**T**	**J**	**Y**
14	3	19	8	24	13	2	18	7	23	12	1	17	6	22	11	0	16	5	21	10	26	15	4	20	9	25

Una vez hemos construido la tabla ya podemos codificar el mensaje.

M= “CORREO ELECTRONICO”

Obtenemos el cifrado del mensaje:

C= “SLFFX LXBXS KFLGH SL”

El descifrado sería la operación inversa obteniendo la tabla como se indica en el cifrado ya obtendríamos el mensaje original.

C= “SLFFX LXBXS KFLGH SL”

Obtenemos el mensaje : M= “CORREO ELECTRONICO”

Ejemplo 3

Cifrado

a= 22
b= 25
n= 27

M= "DELITO INFORMATICO"

Recordemos la siguiente fórmula :

Ci = (mi*a + b) mod n	⟶	Mcd(a,n) = 1

- Construimos el alfabeto con desplazamiento 25 y con decimación 22 a partir del alfabeto español.

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**
0	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
Y	**T**	**O**	**K**	**F**	**A**	**V**	**Q**	**M**	**H**	**C**	**X**	**S**	**Ñ**	**J**	**E**	**Z**	**U**	**P**	**L**	**G**	**B**	**W**	**R**	**N**	**I**	**D**
25	20	15	10	5	0	22	17	12	7	2	24	19	14	9	4	26	21	16	11	6	1	23	18	13	8	3

Una vez hemos construido la tabla ya podemos codificar el mensaje.

M= "DELITO INFORMATICO"

Obtenemos el mensaje codificado :

C = "KFXMG EMÑAE PSYGM OE

Si le queremos añadir una clave supletoria para mejorar las características de seguridad entonces se tendría que realizar lo siguiente.

Clave → k = "LAS PALMAS"
R → r = 20

Se han de eliminar los caracteres repetidos de la clave. Se coloca en la posición r+1 de la tabla, y a continuación se retorna el alfabeto de C comenzando por el primer carácter, y colocándolos después de la clave, eliminando los caracteres repetidos. Como se muestra a continuación:

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**
0	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
Y	**T**	**O**	**K**	**F**	**A**	**V**	**Q**	**M**	**H**	**C**	**X**	**S**	**Ñ**	**J**	**E**	**Z**	**U**	**P**	**L**	**G**	**B**	**W**	**R**	**N**	**I**	**D**
25	20	15	10	5	0	22	17	12	7	2	24	19	14	9	4	26	21	16	11	6	1	23	18	13	8	3
O	K	**F**	**V**	**Q**	**H**	**C**	**X**	**Ñ**	**J**	**E**	**Z**	**U**	**G**	**B**	**W**	**R**	**N**	**I**	**D**	***L***	***A***	***S***	***P***	***M***	**Y**	**T**

Una vez construida la tabla podemos realizar el cifrado. Para ello nos tenemos que fijar en el primer y tercer alfabeto.

M= “DELITO INFORMATICO”

Obtenemos el mensaje cifrado:

C= “VQZÑL WÑGHW IUOLÑ FW

Descifrado

a= 22
b= 25
n= 27
Clave → k = “LAS PALMAS”
R → r = 20

C= “VQZÑL WÑGHW IUOLÑ FW

Construimos el alfabeto con desplazamiento 25 y con decimación 22 a partir del alfabeto español, de la misma manera que en el cifrado. Luego realizamos la traducción del alfabeto creado al alfabeto español, como se muestra a continuación:

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**
0	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
Y	**T**	**O**	**K**	**F**	**A**	**V**	**Q**	**M**	**H**	**C**	**X**	**S**	**Ñ**	**J**	**E**	**Z**	**U**	**P**	**L**	**G**	**B**	**W**	**R**	**N**	**I**	**D**
25	20	15	10	5	0	22	17	12	7	2	24	19	14	9	4	26	21	16	11	6	1	23	18	13	8	3
O	K	**F**	**V**	**Q**	**H**	**C**	**X**	**Ñ**	**J**	**E**	**Z**	**U**	**G**	**B**	**W**	**R**	**N**	**I**	**D**	***L***	***A***	***S***	***P***	***M***	**Y**	**T**

Una vez construida la tabla podemos realizar el descifrado. Para ello nos tenemos que fijar en el tercer y primer alfabeto.

C= “VQZÑL WÑGHW IUOLÑ FW

Obtenemos el mensaje:

M= “DELITO INFORMATICO”

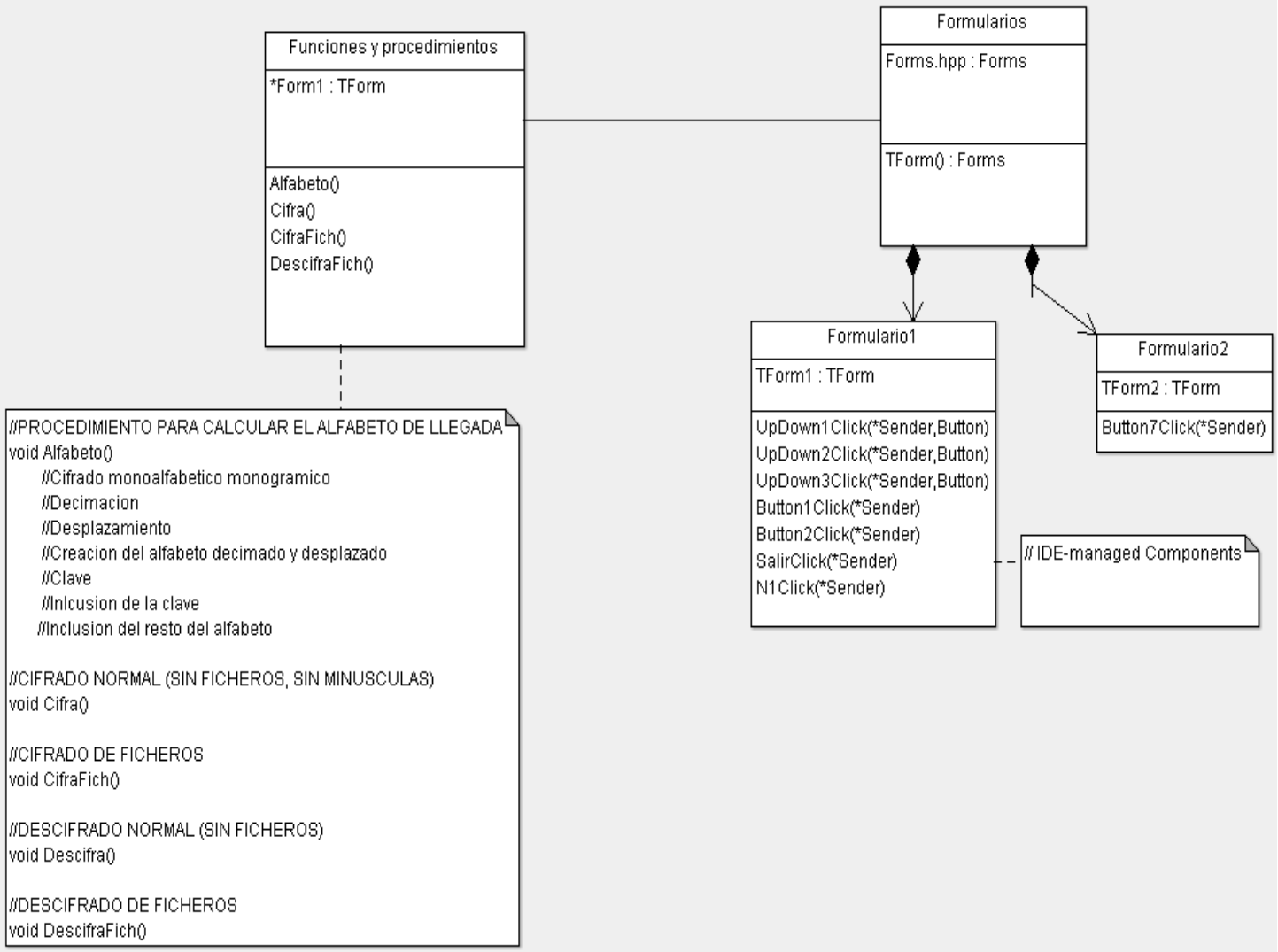
Si el descifrado lo queremos realizar sin clave entonces nos tendríamos que fijar en el segundo y primer alfabeto (sabiendo que el mensaje cifrado es distinto al mensaje cifrado con clave).

C = “KFXMG EMÑAE PSYGM OE

Obtenemos el mensaje:

M= “DELITO INFORMATICO”

Una vez que hemos explicado cada uno de los métodos implementados vamos a mostrar un diagrama de las clases y funciones implementadas para una fácil comprensión del sistema desarrollado.



4. GUIA DE USUARIO

En este Trabajo Fin de Grado se ha desarrollado un sistema informático el cual se estructurará en las siguientes partes en su interfaz de usuario.

A continuación pasamos a describir los diferentes pasos a seguir para el entendimiento a nivel de usuario del sistema implementado, en la que un usuario encripta y desencripta un texto o documento en base a los algoritmos de sustitución (Sustitución Afín, Sustitución por desplazamiento puro y Sustitución por decimación), será el usuario quien elija el algoritmo deseado.

4.1 INICIOS

Al inicializar el programa, verá una pantalla similar a la de la figura 1.

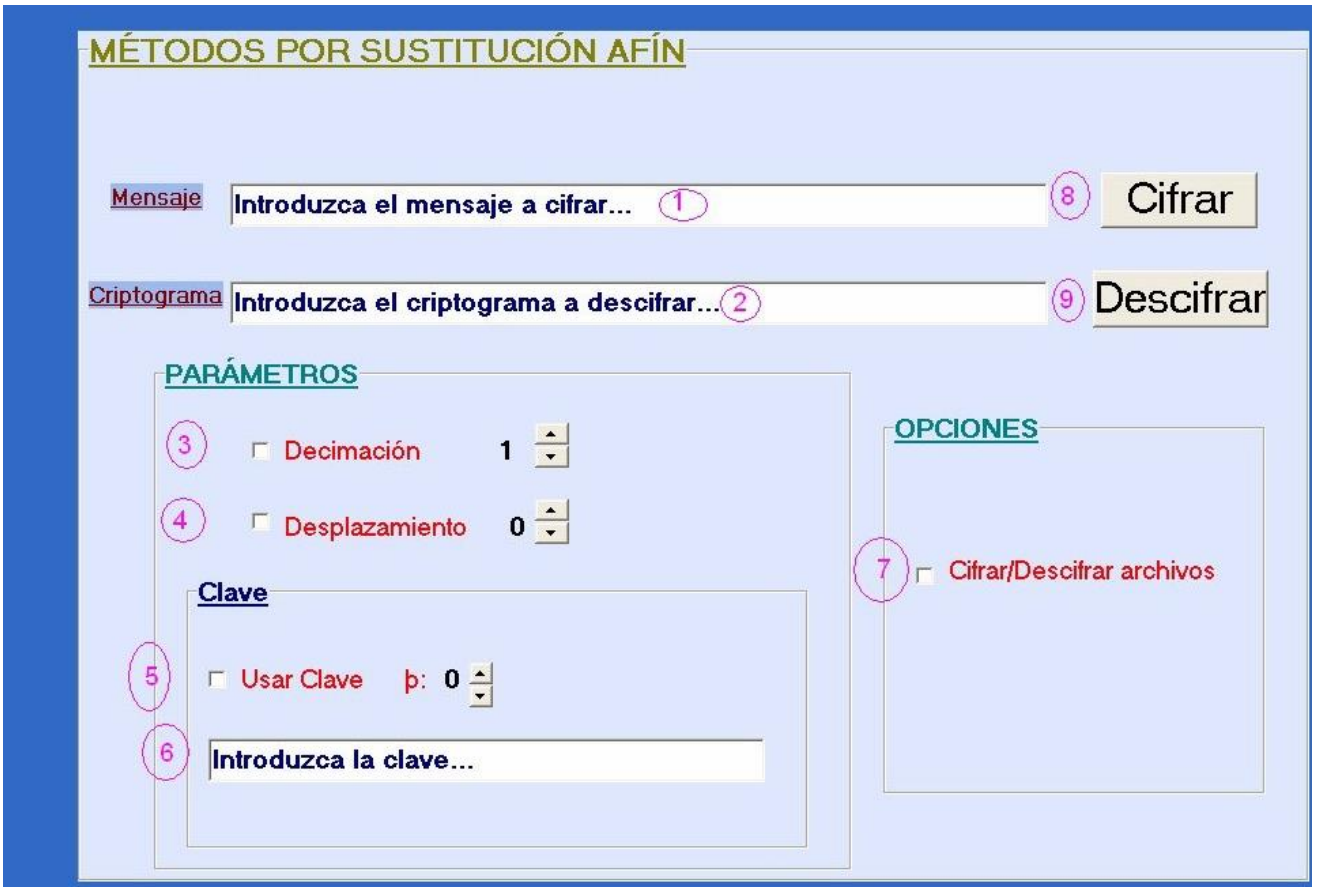


Figura 1.

1) **Mensaje:** introduzca en este cuadro de texto el mensaje que desea cifrar. Cuando descifre un criptograma, el mensaje en claro aparecerá en este recuadro. Cuando trabaje con archivos, aquí aparecerá el archivo de entrada (archivo con mensaje en claro al cifrar, archivo con criptograma al descifrar).

2) **Criptograma:** introduzca en este cuadro de texto el criptograma que desea descifrar. Cuando cifre un mensaje, el criptograma aparecerá en este recuadro. Cuando trabaje con archivos, aquí aparecerá el archivo de salida (archivo con criptograma al cifrar, archivo con mensaje en claro al descifrar).

3, 4, 5, y 6) **Parámetros:** aquí deberá especificar los parámetros del cifrado. Para usar decimación y/o desplazamiento, active el *checkbox* apropiado y ajuste el valor numérico de las constantes con las flechas (Importante: recuerde que la constante de decimación debe ser primo con el módulo de trabajo, así que absténgase de usar como constante de decimación 3 o 9). Para incluir una clave, active el *checkbox* presente para tal efecto, introduzca la clave en el cuadro de texto y ajuste la posición dentro del alfabeto en la que le gustaría incluir la clave.

7) **Opciones:** La opción "Cifrar/Descifrar archivos" alterna entre cifrado/descifrado de mensaje y de archivo. Cuando "Cifrar/Descifrar archivos" está desactivada, tanto el cifrado como el descifrado se lleva a cabo entre el mensaje en **1** y el criptograma en **2**; por el contrario, cuando "Cifrar/Descifrar archivos" está activada, cada vez que se intente cifrar/descifrar aparecerá un diálogo para seleccionar los archivos fuente y destino como el que se muestra en la figura 2.

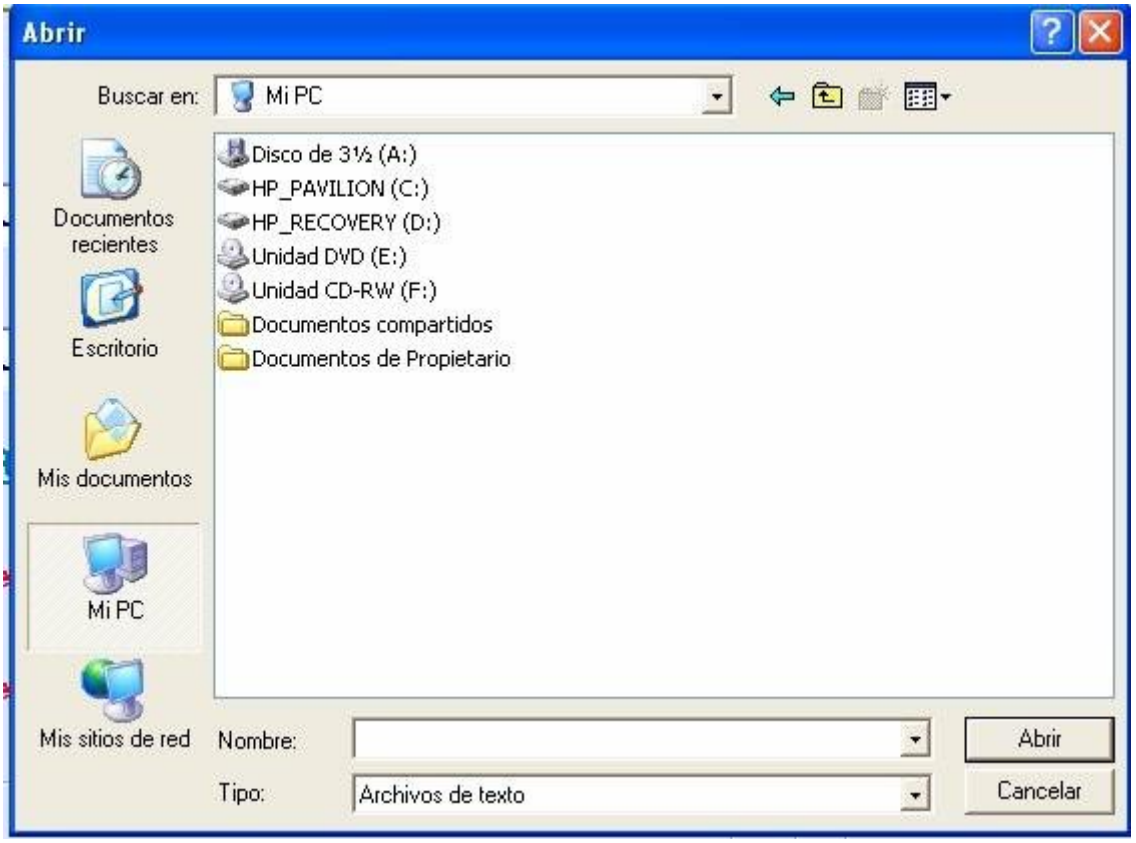


Figura 2.

8) **Cifrar:** al pulsar el botón "Cifrar", se lleva a cabo el cifrado acorde a los parámetros y opciones elegidos.

9) **Descifrar:** al pulsar el botón "Descifrar", se lleva a cabo el descifrado acorde a los parámetros y opciones elegidos.

4.2 MENÚ PRINCIPAL

Archivo: Dentro del menú archivo tenemos el botón salir, el cual nos permite abortar el programa.

Ayuda: Dentro del menú Ayuda tenemos tutorial y about. En tutorial nos encontramos con este documento explicativo del programa y en about podemos ver datos acerca del proyecto (versión , año …).

4.3 CIFRADO Y DESCIFRADO

En este apartado explicaremos paso a paso como se realiza un cifrado y un descifrado.

4.3.1 CIFRADO DE MENSAJE

Para cifrar mensaje introduzca en 1 su texto de elección. A continuación elija los parámetros en 3,4,5,6 deseados activando la casilla correspondiente a cada parámetro (El concepto de estos parámetros los encuentra en los apartados 3 de esta memoria). Una vez realizado los pasos anteriores pulse cifrar y le aparecerá el mensaje cifrado en 2 acorde a los parámetros elegidos. Los pasos anteriormente descritos aparecen reflejados en la figura 3.

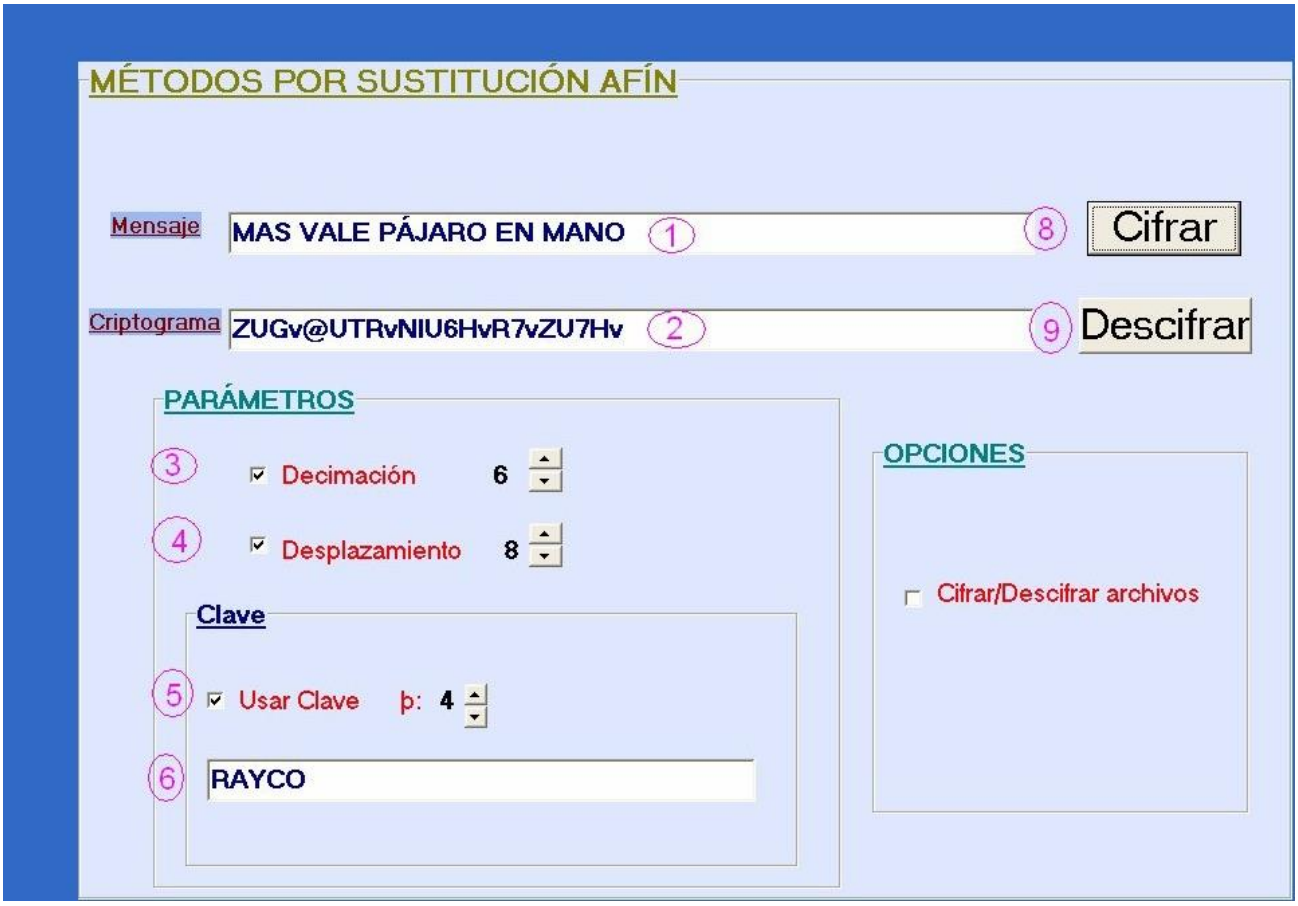


Figura 3.

4.3.2 CIFRADO DE ARCHIVOS

Para cifrar archivos primero elija los parámetros en 3,4,5,6 deseados activando la casilla correspondiente a cada parámetro (El concepto de estos parámetros los encuentra en los apartado 3 de esta memoria). Una vez realizado los pasos anteriores marque en 10 la casilla para cifrar y descifrar archivos. Luego pulse el botón cifrar (en 8) y le aparecerá un diálogo para seleccionar los archivos fuente y destino como el que se muestra en la figura 2. En la dirección seleccionada por el usuario se ha creado el archivo destino cifrado acorde a los parámetros elegidos. Los pasos anteriormente descritos aparecen reflejados en la figura 4.

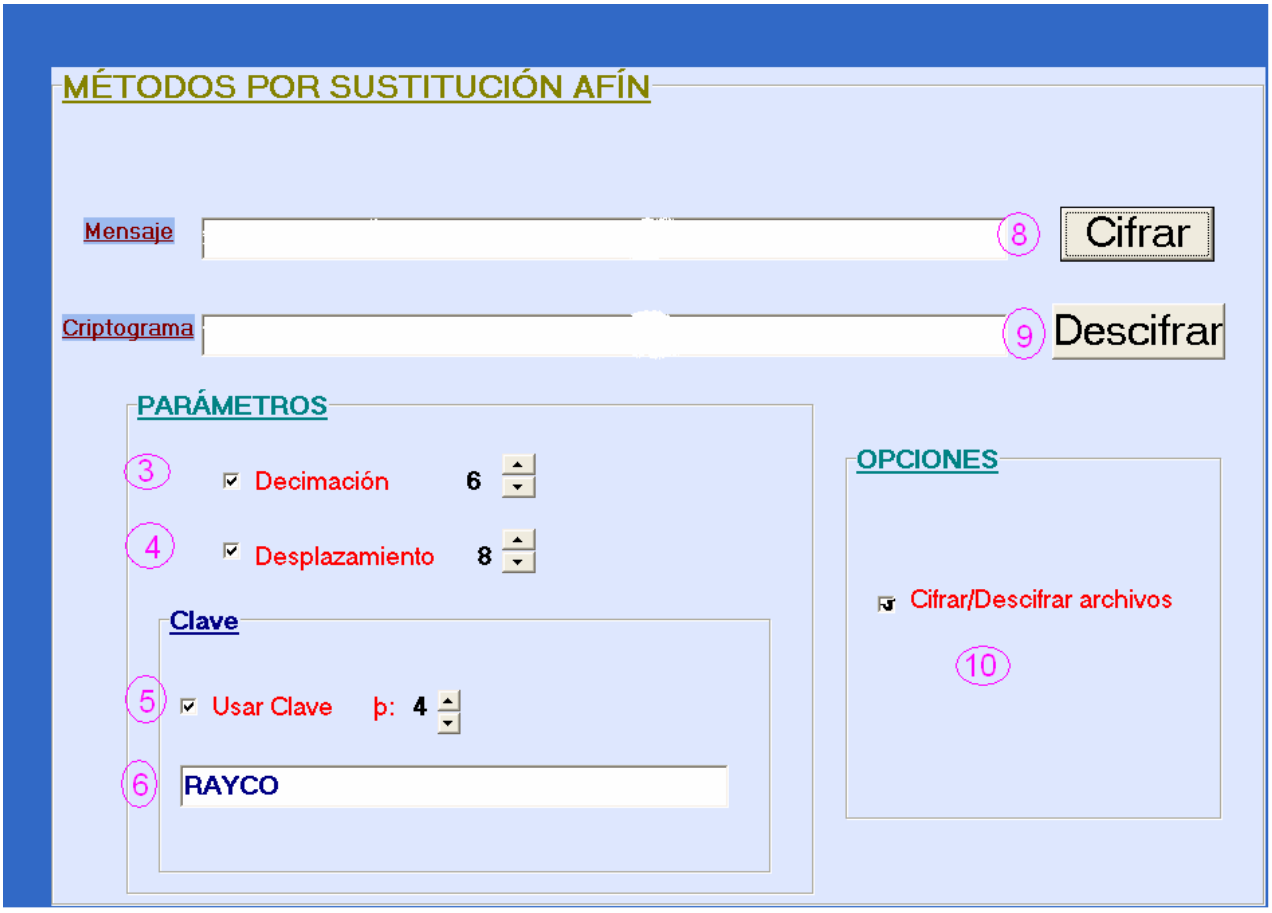


Figura 4.

.

4.3.3 DESCIFRADO DE MENSAJE

Para descifrar mensaje introduzca en 2 su texto cifrado. A continuación elija los parámetros en 3,4,5,6 deseados activando la casilla correspondiente a cada parámetro (El concepto de estos parámetros los encuentra en los apartado 3 de esta memoria). Una vez realizado los pasos anteriores pulse descifrar y le aparecerá el mensaje en claro en 1 acorde a los parámetros elegidos. Los pasos anteriormente descritos aparecen reflejados en la figura 5.

Figura 5.

4.3.4 DESCIFRADO DE ARCHIVOS

Para descifrar archivos primero elija los parámetros en 3,4,5,6 deseados activando la casilla correspondiente a cada parámetro (El concepto de estos parámetros los encuentra en los apartado 3 de esta memoria). Una vez realizado los pasos anteriores marque en 10 la casilla para cifrar y descifrar archivos. Luego pulse el botón descifrar (en 9) y le aparecerá un diálogo para seleccionar los archivos fuente y destino como el que se muestra en la figura 2. En la dirección seleccionada por el usuario se ha creado el archivo destino descifrado acorde a los parámetros elegidos. Los pasos anteriormente descritos aparecen reflejados en la figura 6.

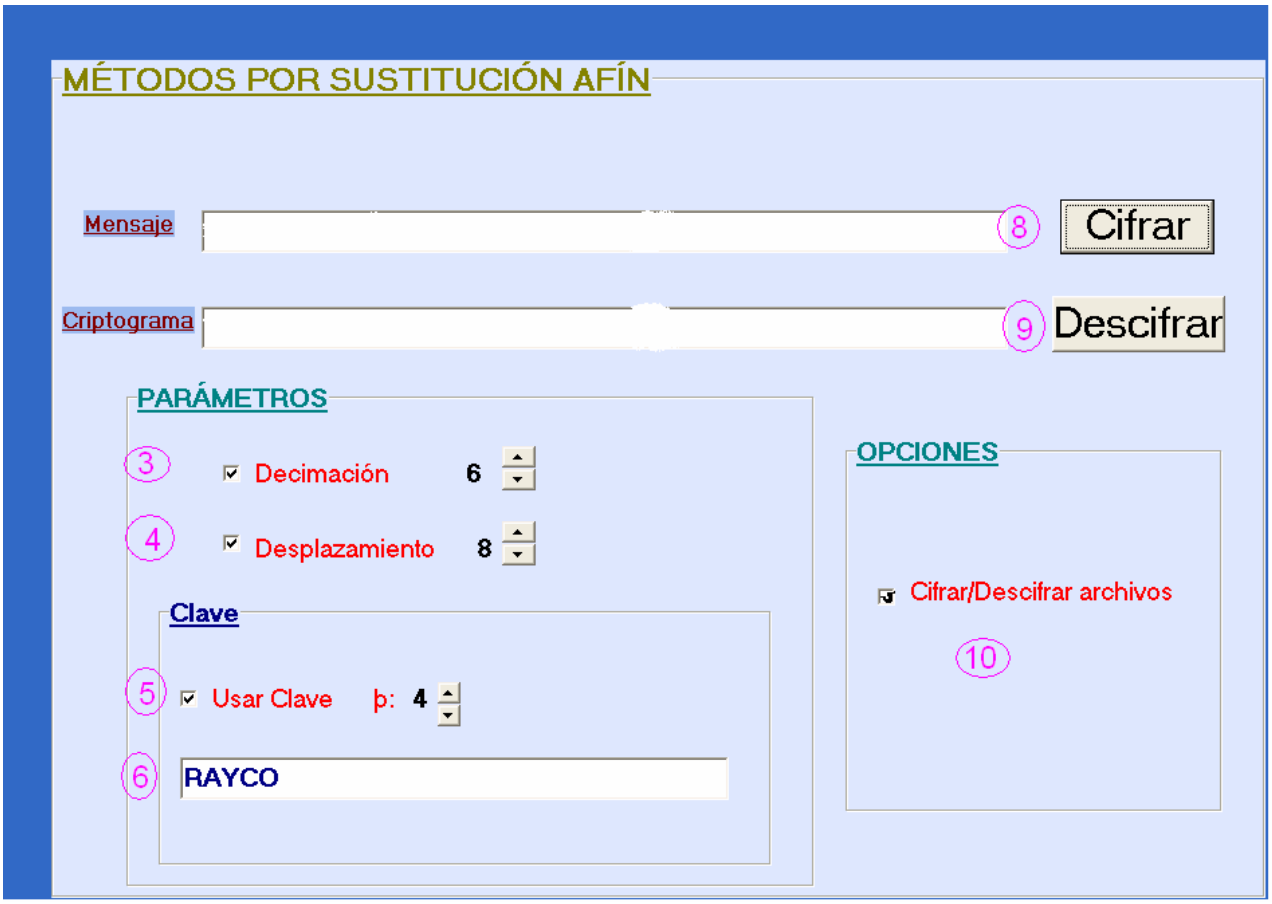


Figura 6.

5. EVALUACIÓN Y PRUEBAS

En este apartado vamos a definir los distintos tipos de pruebas realizados en dicho sistema de información, para posteriormente hacer una evaluación y saber si cumple con las expectativas, así como obtener conclusiones:

Pruebas funcionales

Comprobar la conformidad del software respecto al comportamiento esperado, detectar defectos en el software y realizar una valoración objetiva sobre la calidad funcional del mismo.

Pruebas de Aceptación

Determinar si el producto software satisface o no los criterios de aceptación, respecto a las necesidades del usuario, requisitos del proyecto y procesos de negocio. Estas pruebas guían el proceso de aceptación formal por parte del usuario, cliente u otra entidad autorizada, a determinar si el producto software es apto o no para su uso en el ambiente de producción.

Pruebas de Mantenibilidad

Implantación de sistemas de integración continua, para realizar revisión estática de código, con el objetivo de conocer la calidad intrínseca del mismo y cumplimiento de buenas prácticas.

Pruebas de Usabilidad

Evaluación heurística mediante la inspección del interfaz de la aplicación informando de los puntos fuertes y débiles, con el objetivo de plantear mejoras. Pruebas de usabilidad con usuarios, basadas en la observación y análisis del comportamiento de usuarios reales usando la aplicación.

Eficiencia y Fiabilidad

Determinar si el sistema satisface los requisitos de rendimiento. Localizando "cuellos de botella" en la arquitectura e infraestructura, el límite operativo de la aplicación bajo condiciones de carga y concurrencia, predecir y proyectar el

comportamiento en los equipos de producción y detectar defectos funcionales que sólo se producen bajo condiciones de estrés.

Evaluación y conclusiones

--**Pruebas funcionales:** el software se comporta como se espera, en cuanto al funcionamiento no se han encontrado defectos en el software, con lo cual podemos decir que cumple las expectativas de calidad funcional del mismo.

--**Pruebas de aceptación:** el producto software satisface los criterios de aceptación, así como los requisitos del trabajo fin de grado.

--**Pruebas de mantenibilidad:** se ha realizado la revisión estática de código, ofreciendo el mismo una calidad y sencillez del código implementado, con lo que es muy fácil el mantenimiento del mismo.

--**Pruebas de usabilidad:** la interfaz del sistema de información es muy sencilla con lo que podemos decir que cumple con los requisitos de usabilidad requeridos, se han realizado diversas pruebas con usuarios reales no obteniendo ninguna complicación para la utilización de dicho sistema.

--**Pruebas de eficiencia y fiabilidad:** el sistema satisface los requisitos de rendimiento siendo el mismo eficiente y fiable, ya que no se ha detectado ningún defecto funcional, así como la rapidez del mismo cumple con las expectativas esperadas.
En la métrica de velocidad indica que el sistema tarda en encriptar y desencriptar menos de 1 segundo, por lo que podemos decir que el sistema es eficiente.
En las diferentes pruebas realizadas de ataque estableciendo dicho sistema en red siendo ejecutado por diferentes usuarios a la misma vez, el sistema responde de manera fiable y rápida.

6. BIBLIOGRAFÍA Y MATERIAL UTILIZADO

Para realizar este Trabajo Fin de Grado, en su parte teórica (Criptografía) se ha utilizado básicamente la siguiente bibliografía:

-El libro:

Autor: Morant Ramón, José Luis

Título: Seguridad y protección de la información / José Luis Morant Ramón, Arturo Ribagorda Garnacho, Justo Sancho Rodríguez

Editorial: Madrid : Centro de estudios Ramón Areces, 1994

ISBN: 848004098X

Materias:
Ordenadores - Seguridad - Medidas
Criptografía

Autores:
Ribagorda Garnacho, Arturo
Sancho Rodríguez, Justo

Número de título: 58420

En cuanto a la programación:

- El libro:

Autor: Charte Ojeda, Francisco

Título: Programación con C++ Builder 5 / Francisco Charte Ojeda

Editorial: Madrid: Anaya Multimedia, D.L. 2000
Descripción física:1087 p. ; 23 cm. + 1 CD-ROM

ISBN: 84-415-1046-6

Materias:
Borland C++ Builder (Lenguaje de programación)

Número de título: 226677