SEGUNDA PRÁCTICA DE LABORATORIO
CIFRADO POLIALFABÉTICO

I. OBJETIVOS:

- Implementar cifrado polialfabético
- Implementar descifrado polialfabético

II. EQUIPO Y SOFTWARE

- Computadora personal
- Software de desarrollo (libre elección c++, phyton, java u otro previa autorización del docente)

III. MARCO TEÓRICO

3.1 Cifrado de Vignere

En el siglo XVI el criptógrafo francés propone el más conocido de los métodos de cifrado polialfabéticos, invulnerable por más de 300 años, basada en matemáticas discretas, usa una tabla normalmente con alfabetos de mayúsculas con 26 o 27 caracteres, donde cada fila es la anterior desplazada una posición a la izquierda, las columnas se usan para el mensaje claro y las filas para la clave repetida cíclicamente tantas veces como se le necesite

	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	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
1	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
2	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	B
3	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	B	C
4	E	F	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
5	F	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
6	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
7	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	G
8	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	G	H
9	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
0	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
1	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
2	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
3	N	Ñ	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
4	Ñ	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
5	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	Ñ
6	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	Ñ	O
7	Q	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
8	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
9	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	R
0	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	R	S
1	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
2	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
3	W	X	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
4	X	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
5	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
6	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	Y

Tabla de Vignere mod 27

Por ejemplo, el cifrado de HERMOSO a partir de la clave CIELO será la respuesta no lineal

H	E	R	M	O	S	O
C	I	E	L	O	C	I
J	M	V	W	D	U	W

Usando matemáticas discretas, se escribe la clave debajo del texto claro tantas veces como se necesite y considerando la ubicación de las letras en el alfabeto

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
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

Se implementa el algoritmo

$$c_i = m_i + k_i \bmod n$$

como se muestra

H	E	R	M	O	S	O
7	4	18	12	15	19	15
C	I	E	L	O	C	I
2	8	4	11	15	2	8
7+2 = 9	4+8 = 12	18+4 = 22	12+11 = 23	15+15 = 30	19+2 = 21	15+8 = 23
mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27
9	12	22	23	3	21	23
J	M	V	W	D	U	W

El proceso de descifrado aplicando matemáticas discretas sería:

$$m_i = c_i - k_i \bmod n$$
$$m_i = c_i + (n - k_i) \bmod n$$

Para el cifrado anterior:

J	M	V	W	D	U	W
9	12	22	23	3	21	23
C	I	E	L	O	C	I
2	8	4	11	15	2	8
9-2=7	12-8=4	22-4=18	23-11=12	3-15=-12	21-2=19	23-8=15
mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27
7	4	18	12	15	19	15
H	E	R	M	O	S	O

3.2 Cifrado Autoclave

La debilidad evidente de Vigenère es el hecho de que el cifrado es periódico, por lo que se irá repitiendo a largo del mensaje, lo que facilitará el criptoanálisis. Se puede usar una variante del sistema Vigenère conocida como autoclave y que consiste en:

a) Se escribe la clave
b) Al llegar a la última letra de esa clave, ésta ya no se repite
c) Se continúa la clave con el propio mensaje en claro a continuación

Por ejemplo, el cifrado de AUTOCLAVE con la clave LUNA SERÍA:

A	U	T	O	C	L	A	V	E
0	21	20	15	2	11	0	22	4
L	U	N	A	A	U	T	O	C
11	21	13	0	0	21	20	15	2
0+11=11	21+21=42	20+13=33	15+0=15	2+0=-2	11+21=32	0+20=20	22+15=37	4+2=6
mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27
11	15	6	15	2	5	20	10	6
L	O	G	O	C	F	T	K	G

3.3 Criptoanálisis: el ataque Kasiski

Kasiski observó la existencia de secuencias de caracteres repetidos en el texto cifrado (poligramas) lo cual significaba casi con toda probabilidad que dichas secuencias no sólo eran la misma antes del cifrado sino que además la clave debía coincidir en la misma posición, en esto basó su ataque, en detectar secuencias de letras cifradas repetidas.

Por ejemplo, para el siguiente criptograma, se puede implementar la búsqueda de cadenas repetidas:

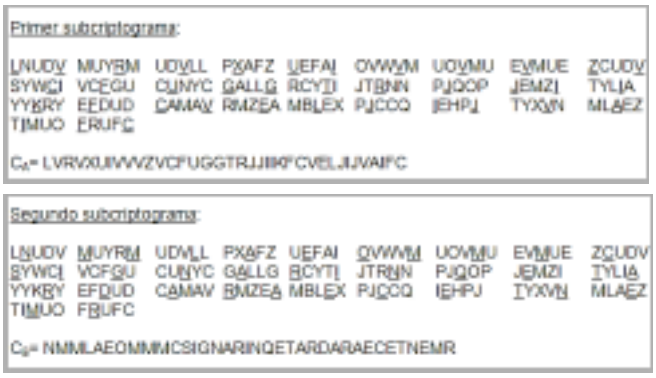
LNUDVMUYRMUDVLLPXAFZUEFAIOVWVMUOVMUEVMUEZCUDVSYWCIVCFGUCU
NYCGALLGRCYTIJTRNNPJQOPJEMZITYLIAYYKRYEFDUDCAMAVRMZEAMBLEXPJC
CQIEHPJTYXVNMLAEZTIMUOFRUFC

Es decir:

- 3 cadenas "UDV" separadas por 8 y 32 posiciones.
- 2 cadenas "MUE" separadas por 4 posiciones.
- 2 cadenas "MUO" separadas por 108 posiciones.

Luego podemos pensar que el número de caracteres de la clave puede ser L=*mcd*(4, 8, 32, 108) = 4. Es decir, la longitud más probable de la clave es L=4, que es el máximo común divisor.

A partir de esta presunción se divide el cripto en L subcriptogramas formados por las letras cada L posiciones



Tercer subcriptograma:

LNUDV MUYRM UDVLL PXAFZ UEFAI OVWVM UDVMU EVMUE ZCUDV
SYWCI VCFGU CUNYC GALLG RCYTI JTRNN PJQQP JEMZI TYLIA
YYKRY EFDUD CAMAV RMZEA MBLEX PJCCQ IEHPJ TYXVN MLAEZ
TIMUO FRUFC

C_C= UUULFFVUUUUYVUYLCJNOMYYYUMMMXCHYMZUU

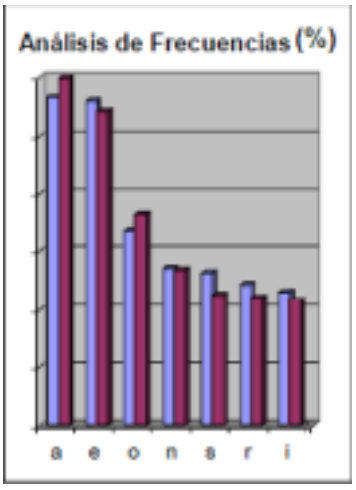
Cuarto subcriptograma:

LNUDV MUYRM UDVLL PXAFZ UEFAI OVWVM UDVMU EVMUE ZCUDV
SYWCI VCFGU CUNYC GALLG RCYTI JTRNN PJQQP JEMZI TYLIA
YYKRY EFDUD CAMAV RMZEA MBLEX PJCCQ IEHPJ TYXVN MLAEZ
TIMUO FRUFC

C_D= DYDPZAWDEEDWCCCLYTPPZLYEDAZBPGPXLTOF

Luego en cada subcriptograma se implementa un análisis estadístico de frecuencias por caracter:

	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
C_A	1	0	3	0	1	3	2	0	5	4	1	2	0	0	0	0	0	0	2	0	1	2	8	0	1	0	1
C_B	5	0	2	1	5	0	1	0	2	0	0	1	6	4	0	1	0	1	4	1	2	0	0	0	0	0	0
C_C	0	0	2	0	0	2	0	1	0	1	0	2	5	1	0	1	0	0	0	0	0	11	2	0	1	6	1
C_D	2	1	3	4	3	1	0	0	0	0	0	3	0	0	0	2	5	1	0	0	2	0	0	2	1	3	3



Ya que la letra “A” es la más frecuente y ocupa la posición 0, la letra "E" es la segunda y ocupa la posición +4 y la letra "O" está +11 posiciones a partir de la letra "E"; con ello se busca en cada subcriptograma (Ci) caracteres que cumplan con la distribución: 0, +4, +11 mod 27:

• Para el subcriptograma C_A elegimos RVG (2, 8, 2), luego la letra clave sería la "R". •
Para el subcriptograma C_B elegimos AEO (5, 5, 1), luego la letra clave sería la "A". •
Para el subcriptograma C_C elegimos UYJ (11, 6, 1), luego la letra clave sería la "U". •
Para el subcriptograma C_D elegimos LOZ (3, 2, 3), luego la letra clave sería la "L".

De esta manera la clave sería "RAUL", con ello se puede descifrar el cripto:

UNASEMANAMASELREGALODELPROBLEMADEMATEMATICASESELLIBROGARDNER

PARAPRINCIPIANTESQUESESORTEARAENTRETODASLASPERSONASQUEDESCIFREN ESTEMENSAJEFIRMADORAUL

Insertando espacios:

UNA SEMANA MAS EL REGALO DEL PROBLEMA DE MATEMATICAS ES EL LIBRO GARDNER PARA PRINCIPIANTES QUE SE SORTEARA ENTRE TODAS LAS PERSONAS QUE DESCIFREN ESTE MENSAJE FIRMADO RAUL

Resumen de los pasos a seguir en el ataque de Kasiski:

1. Buscar en el criptograma repeticiones de al menos 3 letras y hallar la distancia que separa a las repeticiones.
2. Encontrar el máximo común divisor (*mcd*) de todas esas separaciones. Ese valor indicará la posible longitud *L* de la clave.
3. Se divide el criptograma en L subcriptogramas con las letras del criptograma principal cada L espacios.
4. Para cada uno de los L subcriptogramas, se apunta la frecuencia de aparición de cada una de las letras.
5. Se busca en cada uno de los L subcriptograma las cuatro frecuencias más altas (AEOS) o tres (AEO) y que cumplan con la distancia que separa a las letras con más frecuencia del alfabeto español mod 27, es decir la A, la E, la O y la S (+4,+11,+4), en donde Letra 1, Letra 2, Letra 3 y Letra 4 serán las posiciones relativas de las letras AEOS del texto en claro.
6. Ubicada la posición de la Letra 1, que es la relativa a la letra A del texto en claro, se mira con qué letra se ha cifrado, dando así la letra correspondiente de la clave en esa posición. 7. Se repite este proceso con todos los subcriptogramas para obtener la clave buscada. 8. Si se cuenta con poco texto cifrado, es posible que no sea fácil encontrar esas posiciones relativas de la AEOS al no existir letras en los subcriptogramas que se destaquen por su alta frecuencia.

IV. ACTIVIDADES

Cifrado de Vignere

10. Implementar un cifrador de Vignere, donde se pueda seleccionar el módulo, alfabeto módulo 27 o módulo 191 (ASCII), ingresar el texto claro (en archivo o por interface) y genere la cifra resultante
11. Verificar cifrando “Creer que es posible es el paso número uno hacia el éxito. Despertarse y pensar en algo positivo puede cambiar el transcurso de todo el día. No eres lo suficientemente viejo como para no iniciar un nuevo camino hacia tus sueños. Levántate cada mañana creyendo que vas a vivir el mejor día de tu vida”. Usando la clave POSITIVO
12. Verifica el resultado obtenido a partir del cifrador **Criptoclásicos v2.1 (**http://www.criptored.upm.es/software/sw_m001c.htm) haciendo las capturas de pantalla respectivas para los módulos 27 y 191
13. Mostrar el resultado de cifrar usando al menos otros dos métodos disponibles (deberá explicar el principio de dicho método de cifrado)
14. Muestre las frecuencias de cada letra del mensaje original usando como claves POSITIVO, HIELO y MAR, compare y concluya sobre la variación de las frecuencias en base a la longitud

de la clave.Verifique el resultado usando la aplicación desarrollada en la práctica anterior

15. Desarrolle un algoritmo que encuentre el texto claro si recibió la cifra WPIXHVYYOSRTECSZBEEGHUUFWRWTZGRWUFSRIWESSXVOHAIHOHWWHCWH UZOBOZEAOYBMCRLTEYOTI, y se sabe que ha cifrado con la clave HIELO
16. Usando el software anterior, verifique el resultado, eligiendo el cifrado Vignere con módulo 27
17. Usando matemáticas discretas, descifre manualmente YGVMSSKKOX si la clave fue FORTALEZA en un alfabeto de 27 caracteres

Cifrado con autoclave

18. Descifre el texto, usando la clave UNODELOSMASGRANDESCRIPTOGRAFOS:
    XHGDQESDMPKÑDEEDKNGJZPFJSUIFZOLFCINFJCESVZTGBFXCIUDAYNUUDIZY
    WWZBEYNVQWIVUNKZEPHDODQUZZLBDNDRWTHQSERÑIVMLERCMGIFLSORZ
    XTSDIGLOXQSDJHWVCIWQXQJCKMBPOKMPSKMUVIMNJDNBLCSZHXHNYYUIX
    DBSOXHZLXWVGDJGXHWLTDWKÑSAQIMZLNBVMLXHUOQQXIQGWGUFTWKZK
    MOKUDNINSIFJDUOZIJBSVVOWFAIEÑGYOWPSOAP

Ataque de Kasiski

19. Criptoanalizar el siguiente criptograma mod 27, encontrar la clave y el texto en claro.

    MAXYHGAVAPUUGZHEGZQOWOBNIPQKRNÑMEXIGONIICUCAWIGCTEAGMNOL
    RSZJNLWÑAWWIGLDDZSNIZDNBIXGZLAYMXÑCVEKIETMOEOPBEWPTNIXCXUI
    HMECXLNOCECYXEQPBWUFANIICÑJIKISCZUAILBGSOANKBFWUAYWNSCHLCW
    YDZHDZAQVMPTVGFGPVAJWFVPUOYMXCWERVLQCZWECIFVITUZSNCZUAIKBF
    MÑALIEGLBSZLQUXÑOHWOCGHNYWÑQKDANZUDIFOIMXNPHNUWQOKLMVBN
    NKRMKONDPDPNMIKAWOXMEEIVEKGBGSFHVADWPGOYMHOIUEEIPGOLENZBS
    CHAGKQTZDRÑMÑNWTUZIÑCMÑAXKQUWDLVANNIHLÑCQNWGEHIPGZDTZTÑN
    WÑEEWFUMGIÑXNTWXNVIXCZOAZSOQUVENDNFWUSZYHGLRACPGGUGIYWH
    OTRMZUGQQDDZIZFWHVVSHCUGOGIFKBXAXPBOBRDVDUCMVTKGIKDRSZLUQ
    SDVPMXVIVEYMFGTEANIMQLHLGPQOHRYWCFEWFOISNÑPUAYINNÑXNÑPGKW
    GOILQGAFOILQTAHEIIDWMÑEÑXNEPRCVDQTURSK

V. CONCLUSIONES

Emitir al menos ocho conclusiones en torno a las técnicas de cifrado por sustitución

VI. CUESTIONARIO FINAL

1. Trabajando en módulo 191 (un subconjunto imprimible del código ASCII del software Criptoclásicos), cifra el siguiente texto en claro con la clave: El ingenioso hidalgo. *En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lentejas los viernes, algún palomino de añadidura los domingos, consumían las tres partes de su hacienda. El resto della concluían sayo de velarte, calzas de velludo para las fiestas con sus pantuflos de lo mismo, los días de entre semana se honraba con su vellori de lo más fino. Tenía en su casa una ama que pasaba de los cuarenta, y una sobrina que no llegaba a los veinte, y un mozo de*

campo y plaza, que así ensillaba el rocín como tomaba la podadera.

2. Descifre el criptograma en el mismo software ¿Por qué crees que el software no permite hacer un criptoanálisis?
3. Si el cifrado de Vigenere es IZLQOD y la clave SOL, ¿cuál era el mensaje en claro?
4. ¿Cuál será la cifra con autoclave del texto HABIA UNA VEZ, con la clave CIRCO?
5. En el ataque a Vigenere por Kasiski ¿Qué buscamos preferentemente?
6. Encontradas las cadenas repetidas en el criptograma, con separación d1, d2, d3 y d4 ¿Cuál sería la longitud L de la clave?
7. Si las distancias entre repeticiones de cadenas en un criptograma son 35, 112, 70. ¿Cuál sería la longitud L de la clave?

8. ¿Qué diferencia la regla AEOS de AEO en Kasiski?

BIBLIOGRAFÍA