Práctica 2

Ejercicio 1.

Cifre el mensaje ''SABER Y SABERLO DEMOSTRAR ES VALER DOS VECES''  mediante un criptograma de Hill trigrámico con la palabra clave ''REVOLUTIO''.

Multiplicamos la matriz de cifrado por cada uno de los trigramas:

A={{18,4,22},{15,11,21},{20,8,15}}

A={{R,E,V},{O,L,U},{T,I,O}}

Mod[A.{19,0,1},27]

{13,9,17}

Mod[A.{4,18,25},27]

{19,0,5}

Mod[A.{19,0,1},27]

{13,9,17}

Mod[A.{4,18,11},27]

{8,3,11}

Mod[A.{15,3,4},27]

{19,18,6}

Mod[A.{12,15,19},27]

{19,15,24}

Mod[A.{20,18,0},27]

{0,12,4}

Mod[A.{18,4,19},27]

{2,11,2}

Mod[A.{22,0,11},27]

{17,21,11}

Mod[A.{4,18,3},27]

{21,24,26}

Mod[A.{15,19,22},27]

{20,5,26}

Mod[A.{4,2,4},27]

{6,4,21}

Mod[A.{19,24,24},27]

{21,0,14}

Y nos da el siguiente resultado:

N J Q S A F N J Q I D L S R G S O X A M E C L C Q U L U X Z T F Z G E U U A Ñ

**Descifre el mensaje ''SXLEWVNKCOMX'' que ha sido cifrado con un cifrado de Hill trigrámico y con palabra clave ''BARCELONA''.**

Hacemos la inversa de la clave de cifrado para sacar la clave de descifrado y la multiplicamos por cada trigrama.

A = {{1,0,18},{2,4,11},{15,13,0}}

A = {{B,A,R},{C,E,L},{O,N,A}}

MatrixForm[B=Inverse[A,Modulus27]]



Clave descifrado = S R J D A Y T Ñ E

Mod[B.{19,24,11},27]

{1,8,4}

Mod[B.{4,23,22},27]

{13,22,4}

Mod[B.{13,10,2},27]

{13,8,3}

Mod[B.{15,12,24},27]

{15,24,24}

Y nos da el siguiente resultado:

1 8 4 13 22 4 13 8 3 15 24 24

B I E N V E N I D O X X

Ejercicio 2.

En este archivo se muestra un texto en claro y el texto cifrado correspondiente. Sabiendo que ha sido encriptado con un cifrado de Hill trigrámico encuentre la clave.

Texto en claro: PIENSOLUEGOEXISTOX

Texto cifrado: UWWVZAENCSDNGMJJNY

B={{16,8,4,21,23,23},{13,19,15,22,26,0},{11,21,4,4,13,2},{6,15,4,19,3,13},{24,8,19,6,12,9},{20,15,24,9,13,25}}

PowerMod[16,-1,27]

22

Mod[22\*13,27]

Mod[22\*11,27]

Mod[22\*6,27]

Mod[22\*24,27]

Mod[22\*20,27]

16

26

24

15

8

c= Mod[{{16,8,4,21,23,23},{13,19,15,22,26,0}-16{16,8,4,21,23,23},{11,21,4,4,13,2}-26{16,8,4,21,23,23},{6,15,4,19,3,13}-24{16,8,4,21,23,23},{24,8,19,6,12,9}-15{16,8,4,21,23,23},{20,15,24,9,13,25}-8{16,8,4,21,23,23}},27]

{{16,8,4,21,23,23},{0,26,5,10,9,10},{0,2,8,25,9,25},{0,12,16,1,18,1},{0,23,13,15,18,15},{0,5,19,3,18,3}}

PowerMod[26,-1,27]

26

Mod[26\*2,27]

Mod[26\*12,27]

Mod[26\*23,27]

Mod[26\*5,27]

25

15

4

22

e=Mod[{{16,8,4,21,23,23},{0,26,5,10,9,10},{0,2,8,25,9,25}-25{0,26,5,10,9,10},{0,12,16,1,18,1}-15{0,26,5,10,9,10},{0,23,13,15,18,15}-4{0,26,5,10,9,10},{0,5,19,3,18,3}-22{0,26,5,10,9,10}},27]

{{16,8,4,21,23,23},{0,26,5,10,9,10},{0,0,18,18,0,18},{0,0,22,13,18,13},{0,0,20,2,9,2},{0,0,17,26,9,26}}

PowerMod[18,-1,27]

PowerMod::ninv: \[NoBreak]18\[NoBreak] is not invertible modulo \[NoBreak]27\[NoBreak]. [](http://reference.wolfram.com/mathematica/ref/message/PowerMod/ninv.html)

PowerMod[18,-1,27]

f=Mod[{{16,8,4,21,23,23},{0,26,5,10,9,10},3{0,0,18,18,0,18},{0,0,22,13,18,13},{0,0,20,2,9,2},{0,0,17,26,9,26}},27]

{{16,8,4,21,23,23},{0,26,5,10,9,10},{0,0,0,0,0,0},{0,0,22,13,18,13},{0,0,20,2,9,2},{0,0,17,26,9,26}}

Cambio 3º fila por 6º

{{16,8,4,21,23,23},{0,26,5,10,9,10},{0,0,17,26,9,26},{0,0,22,13,18,13},{0,0,20,2,9,2},{0,0,0,0,0,0}}

PowerMod[17,-1,27]

8

Mod[8\*22,27]

Mod[8\*20,27]

14

25

f=Mod[{{16,8,4,21,23,23},{0,26,5,10,9,10},{0,0,17,26,9,26},{0,0,22,13,18,13}-14{0,0,17,26,9,26},{0,0,20,2,9,2}-25{0,0,17,26,9,26},{0,0,0,0,0,0}},27]

{{16,8,4,21,23,23},{0,26,5,10,9,10},{0,0,17,26,9,26},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}}

PowerMod[26,-1,27]

PowerMod[17,-1,27]

26

8

Mod[26\*8,27]

Mod[8\*5,27]

19

13

Mod[{{16,8,4,21,23,23}-19{0,26,5,10,9,10},{0,26,5,10,9,10}-13{0,0,17,26,9,26},{0,0,17,26,9,26},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}},27]

{{16,0,17,20,14,22},{0,26,0,23,0,23},{0,0,17,26,9,26},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}}

PowerMod[17,-1,27]

8

Mod[8\*17,27]

1

Mod[{{16,0,17,20,14,22}-{0,0,17,26,9,26},{0,26,0,23,0,23},{0,0,17,26,9,26},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}},27]

{{16,0,0,21,5,23},{0,26,0,23,0,23},{0,0,17,26,9,26},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}}

PowerMod[16,-1,27]

PowerMod[26,-1,27]

PowerMod[17,-1,27]

22

26

8

Mod[{22{16,0,0,21,5,23},26{0,26,0,23,0,23},8{0,0,17,26,9,26},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}},27]

{{1,0,0,3,2,20},{0,1,0,4,0,4},{0,0,1,19,18,19},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}}

MatrixForm[{{1,0,0,3,2,20},{0,1,0,4,0,4},{0,0,1,19,18,19},{0,0,0,0,0,0},{0,0,0,0,0,0},{0,0,0,0,0,0}}]

{{1, 0, 0, 3, 2, 20},

{0, 1, 0, 4, 0, 4},

{0, 0, 1, 19, 18, 19},

{0, 0, 0, 0, 0, 0},

{0, 0, 0, 0, 0, 0},

{0, 0, 0, 0, 0, 0}}

Al final como podemos ver la clave convertida a letras sería :

D C T

E A E

S R S

DESCARTES

Ejercicio 2.

**Descifre mediante la técnica de análisis de frecuencias (de digramas) el siguiente mensaje que ha sido cifrado por el cifrado de Playfair.**

EPVRNKVFCGMFHAMTCYSGMIFCZUMUFMTSRMEUMIFUPHMGIGDNQEETGSETUZLDMSFIRPCPESGYSCMUUNSFCWPCLUPEDUEPQPCYBCFRGARFYKBDPETOMEESFIHDGSLUCSGSZUUPDPFUBDUFPCCTSGPIDTRUHASELDNTEPBMRMHCABCTSGPIEMIGPEIFIETOSFSEFIDTBMETIAMESDGV

He sacado las frecuencias de los digramas del texto

Digrama Análisis de <Sin nombre1>. Tamaño del archivo 208 bytes.

Ordenados descendentemente por frecuencia.

Nº Subcadena Frequencia (en %) Frecuencia

1 ET 2.4155 5

2 SG 2.4155 5

3 FI 1.9324 4

4 ME 1.9324 4

5 PC 1.9324 4

6 PE 1.9324 4

7 SF 1.9324 4

8 EP 1.4493 3

9 ES 1.4493 3

10 FC 1.4493 3

11 GP 1.4493 3

12 GS 1.4493 3

13 IF 1.4493 3

14 MI 1.4493 3

15 SE 1.4493 3

16 TS 1.4493 3

17 UP 1.4493 3

18 AM 0.9662 2

19 BC 0.9662 2

20 BD 0.9662 2

21 BM 0.9662 2

22 CT 0.9662 2

23 CY 0.9662 2

24 DG 0.9662 2

25 DN 0.9662 2

26 DP 0.9662 2

Los he comparado y sustituido con los digramas mas frecuentes en español

DE

ES

EN

OS

AD

TE

IN

ER

AS

EL

SE

OR

RE

NT

ST

RA

AR

DA

RO

NE

ED

LE

SA

SO

NI

ET

TN

TS

Pero no he conseguido sacar el texto como se puede ver en esta prueba:

ER VRNKV EL GMFHAMTCY ES NT EL ZUMUFM RA R OS UM RE AR HMGIG NI QE DE OR DE UZLDMS EN R AD TE ES YSCMUUN IN CW AD LU TE DU ER Q AD YBCFRGARFYKB ET DE O OS AS EN HD OR LUC ES SZUUP ET FUBDUF AD LE ES PIDTRUHASEL NI T ER BMRMHCABCTS SE IE NT G TE I EN DE O IN ST EN DTBM DE IAM AS DGV