

#Practica 1 SPSI: Maquina Enigma ##Rafael Lachica Garrido

###9. Hacer el seguimiento por permutaciones y sustituciones (Plugboard y rotores) del trigramma de texto llano “AAA”. ¿Qué conclusión sugiere el cifrado que sale de aquí? ¿Existe la posibilidad de repetición por periodo en la máquina Enigma? Si es así, documéntalo con un caso práctico con una Enigma de 3 rotores. ¿Cuál sería, si existe, el periodo para una máquina Enigma de 4 rotores? ¿Coincide lo obtenido en un ejemplo práctico con lo esperado teóricamente? **Llave:**

UKW B


Walzenlage I II III

Ringstellung A A A

Steckerverbindungen

Start position 1 1 1

El periodo, cuando tenemos 3 rotores se cumple alrededor de $26^3 = 17576$ letras pulsadas, se repite todo el periodo, desde que se pulsa la letra por primera vez, debido a que hay 3 rotores, se ponen otra vez todos como si fuese el inicio. En el caso práctico, probamos con la quintupla ABCDE, y con una web que nos cuenta las letras vemos el número exacto en el que comienza los períodos: 17576. Al volver a contar el resultado se va a 20000 pero porque le introduce espacios. Aquí las imagenes del resultado:



The image shows a screenshot of a Parrot Bebop Drone advertisement at the top, featuring the drone, the text "Parrot BEBOP DRONE", and "El drone para smartphones y tabletas" with a price of "499€". Below the ad is a blue banner that reads "Write or paste your text into this online character counter:". Underneath the banner is a text area filled with the word "ABCDE" repeated many times. At the bottom of the text area are two buttons: "Count characters" and "Reset". To the right of the "Reset" button is a text box displaying the number "17576".

Enigma Machine Simulator

by Mike Koss

Initialization


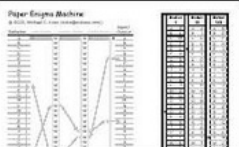
Rotors:

Rotor Start:

Rings:

Plugboard:

To learn more about the [Enigma Machine](#), try using the [Paper Engima](#). You can also read the [source code](#) used by this Enigma Simulator.

Encoding

T B O

Type Message Here:

ABCDE ABCDE ABCDE ABCDE ABCDE

ABCDE ABCDE ABCDE ABCDE ABCDE

ABCDE ABCDE ABCDE

Read Output Here:

BJELR WJJRC KFQFS CLYIP MLWMC

XDPNO TQVMZ LLIOT XKLUV NYEWV

RPQGY KVJMQ BGMBT SNOMU SRNGD

FEBAY BEDHT LSTMU IGRQP DCPXB

IADUP JAJIW CIZRO GAMKL IXYHT

DEACM IZORR KTJSC FUSBO TLTUV

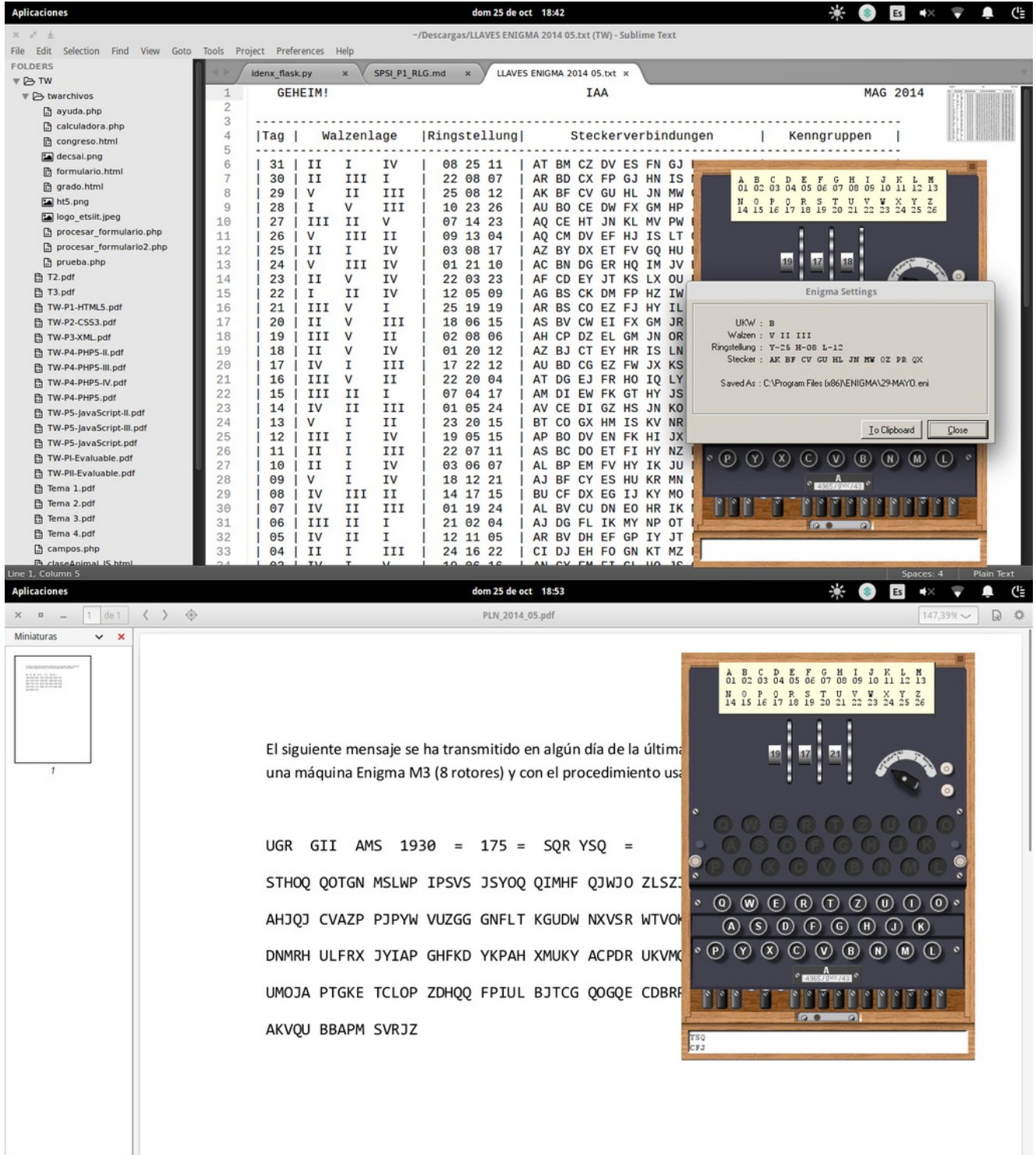
^ v
Highlight All
Match Case
2 of 2 matches

Aquí vemos que hay encontrado dos veces la quintupla BJELR, a la que después seguirán las demas tuplas correspondientes desde el inicio.

Para 4 rotores se supone que sería para $26^4 = 456976$ letras. En el caso práctico nos da algo menos de letras, alrededor de 456000. (no pongo el numero exacto porque se congela javascript en el navegador al tener que mandar una cantidad enorme de datos).

###10. Toma el mensaje cifrado dado en el fichero "PLN_2014_05", y descífralo usando el Libro de llaves dado en el fichero "LLAVES ENIGMA 2014 05". Ultima semana de Mayo de 2014, del 26 al 31. Es el **día 29 de Mayo**, para descifrar el mensaje seguimos los siguientes pasos, que están ya puestos en el archivo sim_Manual.

1. Seleccionamos los rotores e introducimos la clave:
2. Introducimos en el stecker los pares.
3. Ponemos la posición inicial, que se encuentra en el mensaje cifrado: SQR
4. Tecleamos la clave YSQ, y lo que nos devuelve, **CFJ**, lo introducimos en la posición inicial.
5. Desciframos, saltandonos las primeras tuplas que pertenecen al Kerngruppen.



The screenshot shows a computer screen with two applications open. The top application is Sublime Text, editing a file named 'LLAVES ENIGMA 2014 05.txt'. The file contains a table of Enigma machine settings, including rotor positions and connections. The bottom application is a PDF viewer showing a document titled 'PLN_2014_05.pdf'. The document contains a message in Spanish and a diagram of an Enigma machine.

Sublime Text Content:

dom 25 de oct 18:42

~/Descargas/LLAVES ENIGMA 2014 05.txt (TW) - Sublime Text

File Edit Selection Find View Goto Tools Project Preferences Help

FOLDERS

▼ TW

▼ twarchivos

ayuda.php

calculadora.php

congreso.html

decsal.png

formulario.html

grado.html

ht5.png

logo_etsiit.jpeg

procesar_formulario.php

procesar_formulario2.php

prueba.php

T2.pdf

T3.pdf

TW-P1-HTML5.pdf

TW-P2-CSS3.pdf

TW-P3-XML.pdf

TW-P4-PHP5-IL.pdf

TW-P4-PHP5-III.pdf

TW-P4-PHP5-IV.pdf

TW-P4-PHP5.pdf

TW-P5-JavaScript-II.pdf

TW-P5-JavaScript-III.pdf

TW-P5-JavaScript.pdf

TW-Pi-Evaluable.pdf

TW-Pi-Evaluale.pdf

Tema 1.pdf

Tema 2.pdf

Tema 3.pdf

Tema 4.pdf

campos.php

classAnimalJS.html

Line 1, Column 5

dom 25 de oct 18:53

PLN_2014_05.pdf

147,39%

Miniaturas

El siguiente mensaje se ha transmitido en algún día de la última una máquina Enigma M3 (8 rotores) y con el procedimiento us

UGR GII AMS 1930 = 175 = SQR YSQ =

STHOQ QOTGN MSLWP IPSVS JSYQ QIMHF QJWJO ZLSZ

AHJQJ CVAZP PJPYW VUZGG GNFLT KGUDW NXVSR WTVOK

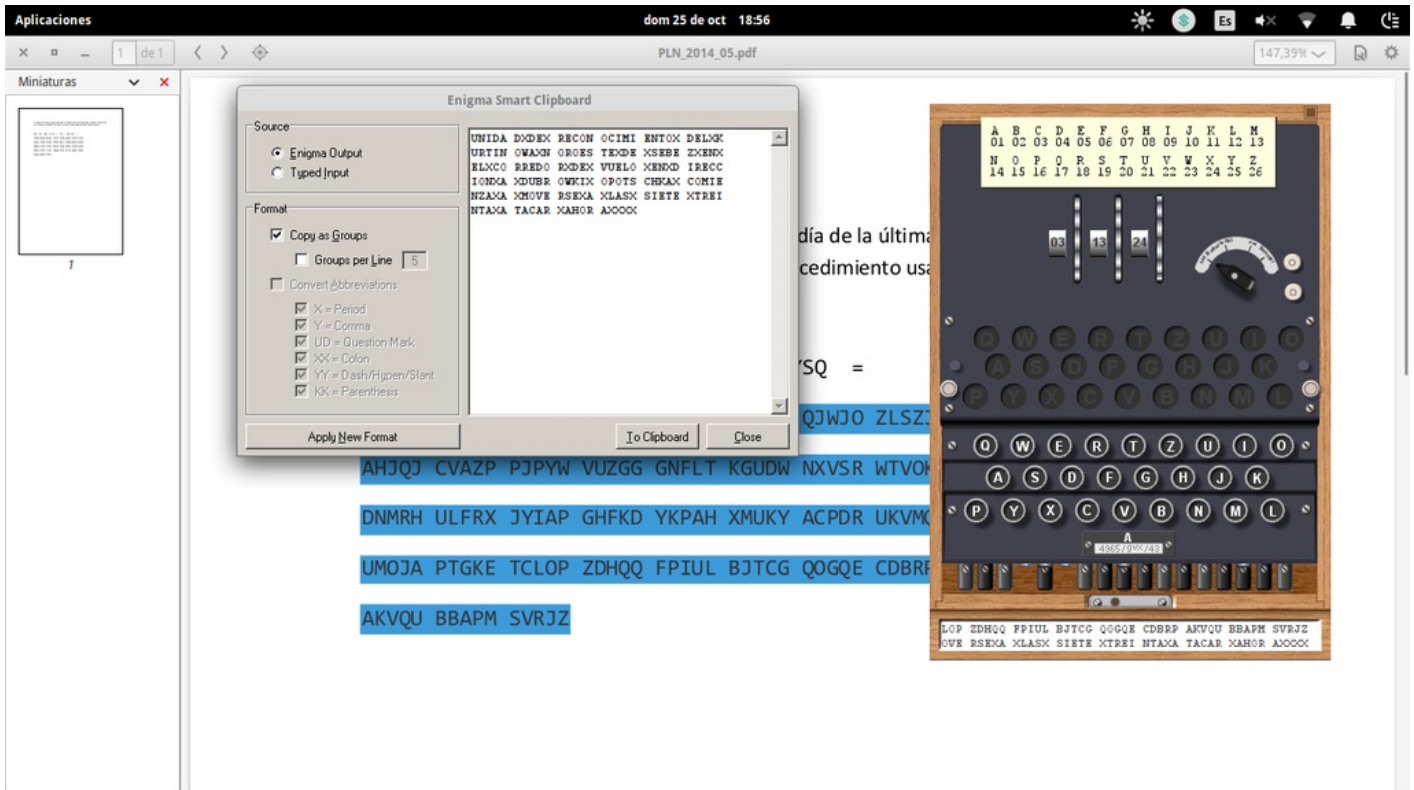
DNMRH ULFRX JYIAP GHFKD YKPAH XMUKY ACPDR UKVM

UMOJA PTGKE TCLOP ZDHQQ FPIUL BJTCG QOGQE CDBR

AKVQU BBAPM SVRJZ

Diagrama de la máquina Enigma M3 (8 rotores) y con el procedimiento us

Resultado el mensaje: Unidadxdexreconocimiento....



(he tenido problemas al copiar, pegar en enigma, debido a que esto usando wine para ejecutar en linux, por eso el pantallazo)

###11. Toma ahora el mensaje cifrado dado en el fichero “CYP_RETO2_ENIGMA” y descífralo sabiendo que es el cifrado de un mensaje que consiste en la repetición de una única letra. Encuentra después la llave usada. Esta cifrado con la máquina Enigma I, con 3 rotores escogidos de entre 5 de ellos. Enigma nunca cifra la misma letra que pulsas, como me he dado cuenta en el ejercicio 9. Por esto la única letra que no aparece es la Z, la cual es la que se pulsa continuamente. Para demostrarlo, vamos a realizar un análisis de frecuencias de las veces que aparecen los caracteres en el mensaje cifrado. Vemos que nos aparece el carácter z sin ninguna aparición, y el que más aparece es la letra f. **Es por ello que esta es una debilidad de enigma, ya que nunca usa la letra que estamos usando a la hora de cifrar.**

Aplicaciones mar 27 de oct 13:44

Cálculo de frecuencias - Mozilla Firefox

Cálculo de frecuencias x SWAD UGR x +

roble.pntic.mec.es/jgad0020/cripto/frecuencias.php

Resultados

Frecuencias:

Dígrafos:

LETRAS	f	t	g	i	e	r	j	x	l	m	b	k	c
CANTIDAD	40	38	37	37	36	36	35	34	34	34	34	33	33
PORCENTAJE	4.94	4.69	4.57	4.57	4.44	4.44	4.32	4.20	4.20	4.20	4.20	4.07	4.07
LETRAS	n	o	q	d	a	v	w	h	y	s	u	p	z
CANTIDAD	32	32	31	31	30	30	29	28	27	27	26	26	0
PORCENTAJE	3.95	3.95	3.83	3.83	3.70	3.70	3.58	3.46	3.33	3.33	3.21	3.21	0.00

lc	ad	lh	jb	ic	md	rk	tf	hw	xp	ht	ih	pv	ym	cf	gn	xj	ct	dg	rx	tb	wj	qn	fb	ex
7	6	6	5	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3

Trígrafos:

mdk	rok	oka	xpn	hqm	kad	geq	xqn	qtu	txp	ict	ftk	adq	hft	qhw	yad	gqa	bym	xrx	hwj	eke	ouk	yme	btb	fhf
3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1

Otros datos:

Número de letras	810
Número de vocales	161
Proporción de vocales	19.88%
Índice de coincidencia	0.03937

[Volver](#)

###12. Obtén un texto cifrado a elección, a partir de un texto llano de entre 60 y 100 caracteres, en una máquina Enigma M3 sin stecker. Aplícale el ataque dado en el siguiente enlace para romperlo y obtener tanto el texto llano como la Llave.

###Obtén un texto cifrado a elección, a partir de un texto llano de entre 60 y 100 caracteres, en una máquina Enigma M3 sin stecker. Aplícale el ataque dado en el siguiente enlace para romperlo y obtener tanto el texto llano como la Llave.

<http://practicalcryptography.com/cryptanalysis/breaking-machine-ciphers/cryptanalysis-enigma/> **Llave** que le asigno:

UKW B
Walzenlage I II III
Ringstellung Z Z Z
Steckerverbindungen
Start position 1 2 3

Mensaje original: XAJKL HOLA MUNDO MI NOMBRE ES RAFAEL LACHICA GARRIDO ALUMNO DE SPSI DE LA ETSIT DE LA UNIVERSIDAD DE GRANADA CURSO DOS MIL QUINCE DOS MIL 16 Mensaje cifrado: JNYCD OVJD WHEUZ DA XTSYTI UY OQGWXP ZORBLMW UUSMNZF KRPWRB XS BJQG HM SB AYAUAI RW DO GTSBHJPEOOW NZ

Actualizamos el código de **break_enigma_1.c**:

```

20 // assumes no playground is used.
21 // *****/
22 argc, char *argv[]){
23     // text variable must be all capitals, with no spacing or punctuation, use e.g. http://practicalcryptography.com/ciphers/mechanical
24     // generate messages. This version can not break enigma messages with plugs.
25     t[] = "JNYCDOVDJDWHEUZXSYTIUYOQGWXPZORBLMUUSMNZFKRPWRBXSBJQGHMSBAYAUAIRWDOGTSBHPJPEOOWNYKWFYFZTJGWWFAUEDFURXGCMKNFU16";
26     txt = malloc(sizeof(char)*(strlen(ctext)+1));
27     *ref;
28     mak_enigma(ctext);
29     final key: \n";
30     maKey(ref);
31     f, ctext, ptext);
32     decryption: %s\n", ptext);
33     t);
34     ;
35
36     // ie permutations of 5 rotors, there are 60 total
37     [3] = {{ 1, 2, 3 }, { 1, 2, 4 }, { 1, 2, 5 }, { 1, 3, 2 }, { 1, 3, 4 }, { 1, 3, 5 }, { 1, 4, 2 }, { 1, 4, 3 }, {
38
39     ps = NULL;
40

```

```
rafaellg8@system32:~/Documentos/GII/Cuarto/SPSI/P1_SPSI/cryptoBreak$
./a.out
searching for rotors: .....
searching ring settings: ..
final key:
indicator=BBC, rotors=123, rings=AZZ, plugboard=
decryption:
XAJKLHOLAMUNDOMINOMBREESRAFAELLACHICAGARRIDOALUMNODESPSID
ELAETSIITDELAUNIVERSIDADDEGRANADACURSODOSMILQUINCEDOSMILRM
```

**XAJKLHOLAMUNDOMINOMBREESRAFAELLACHICAGARRIDOALUMNODESPSIDELAE
TSIITDELAUNIVERSIDADDEGRANADACURSODOSMILQUINCEDOSMILRM**

Lo rompe fácilmente, lo único que da al final RM porque he metido números.

```
rafaell8@system32:~/Documentos/GII/Cuarto/SPSI/P1_SPSI/cryptoBreak$ gcc break_enigma_1.c enigma.c NbestList.c/scoreText.c -lm -O3
rafaell8@system32:~/Documentos/GII/Cuarto/SPSI/P1_SPSI/cryptoBreak$ ./a.out
searching for rotors: .....
searching ring settings: ..
final key: a 4.pdf
indicator=BBC, rotors=123, rings=AZZ, plugboard=
decryption: XAJKLHOLAMUNDONOMBREESRAFAELLACHICAGARRIDOAALUMNODESPIDELAETSITDELAUNIVERSIDADDEGRANADACURSODOSMILQUINCECOSMILIRM
rafaell8@system32:~/Documentos/GII/Cuarto/SPSI/P1_SPSI/cryptoBreak$
```

##Referencias

1. <http://roble.pntic.mec.es/jgad0020/cripto/frecuencias.php> Análisis de frecuencias
2. https://es.wikipedia.org/wiki/Enigma_%28m%C3%A1quina%29
3. <http://www.lettercount.com/> Cuenta caracteres

4. Material dejado en los links de la práctica1