Práctica 1 SPSI

Cómo funciona el cifrado de enigma.

1)Debe de configurarse la máquina empezando por el tipo, después colocar los rotores que usaremos(Walzenlage) y elegiremos la posición de los mismos (Ringstellung). Ahora se deben de hacer las conexiones de la parte frontal una a una(Stecker).

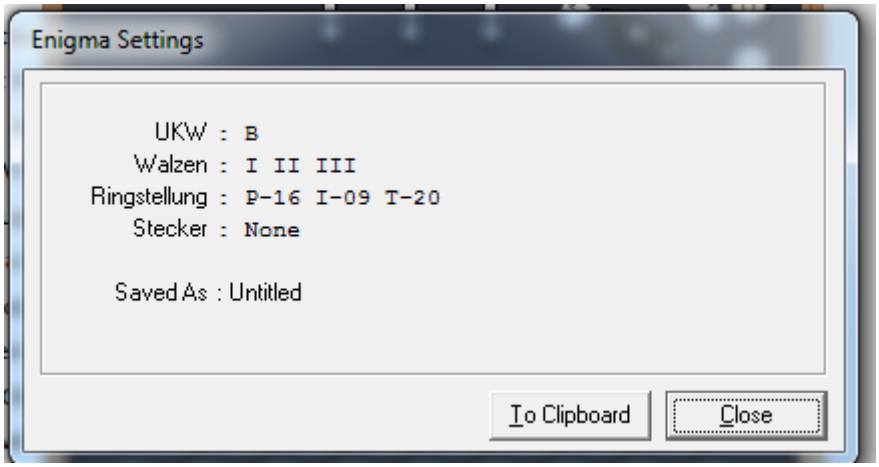
2)Debe seleccionarse el grupo de palabras del día compuesto por 4 palabras con 3 letras que se usarán en la primera palabra del texto cifrado.

3) Codificamos el texto

Primero debemos elegir la clave que codifica el texto por ejemplo RHC y después debemos de codificarla con otra clave que sería por ejemplo VTK. Poniendo los rotores en la posición VTK codificamos RHC y obtenemos ZIW. Ahora procedemos a codificar el texto como máximo de 250 caracteres.

Teniendo todo ya empezamos a emitir por la cabecera del mensaje que consta de destino, emisor, hora, número de grupos, la posición inicial de los rotores y la clave encriptada. Por último enviamos el grupo de identificación donde las 3 últimas letras dicen la clave del día a usar y el texto encriptado. Hacer notar que el grupo de identificación no se debe de encriptar.

6. La llave en enigma, en el caso de enigma I, consta de 3 rotores elegidos entre 5 posibles en el que influye como estén ordenados, una configuración inicial de los rotores elegidos (Ringstellung) y unas conexiones en la parte frontal que son permutaciones de las letras, y finalmente la posición de inicio de los rotores para que se obtenga el texto cifrado.



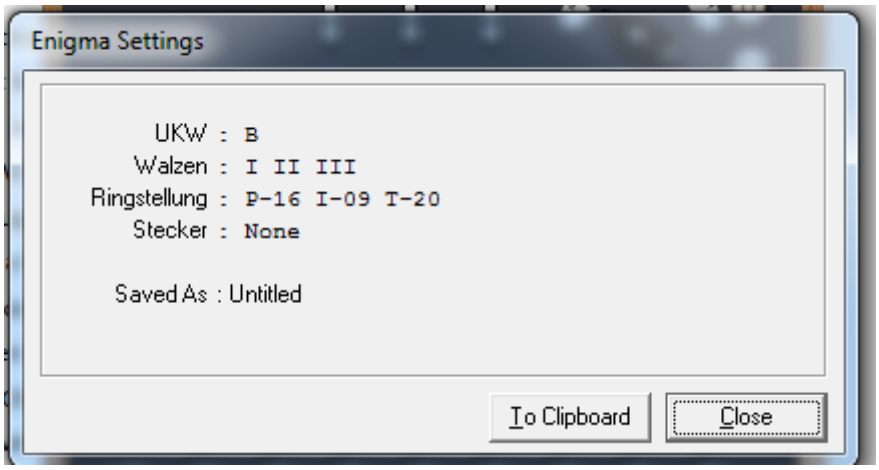
7. Con la configuración:

Walzenlage I II III

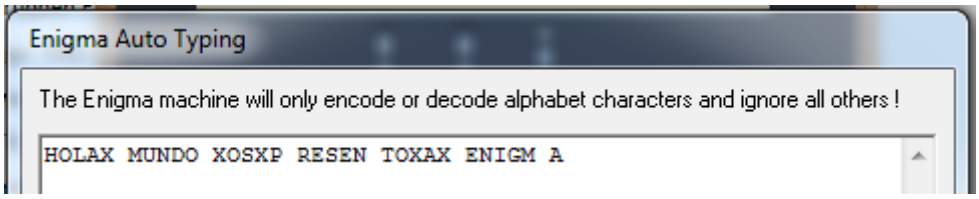
Ringstellung P I T

Sin steckerverbindungen

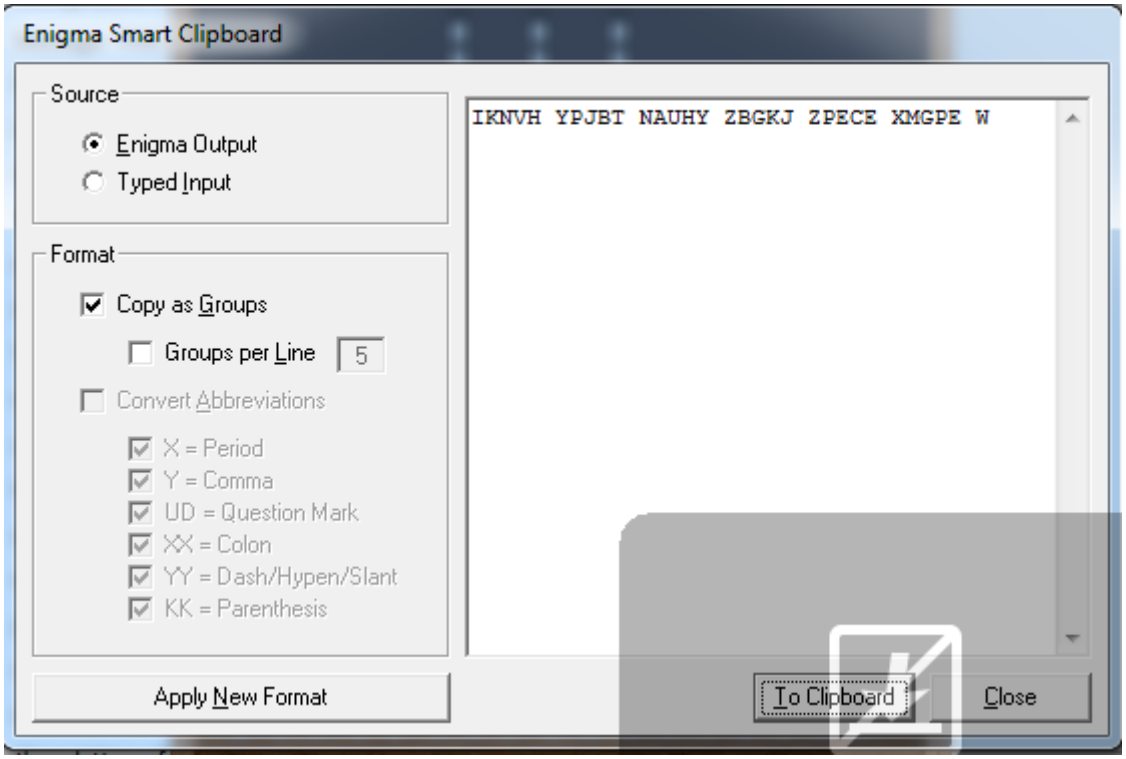
Kenngruppen ATK SVL RQP JCX



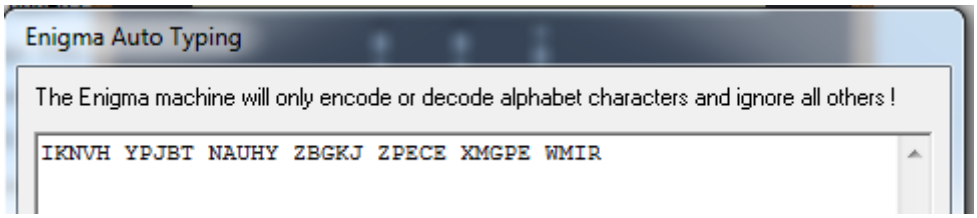
El mensaje Hola X mundo X os X presento X a X enigma

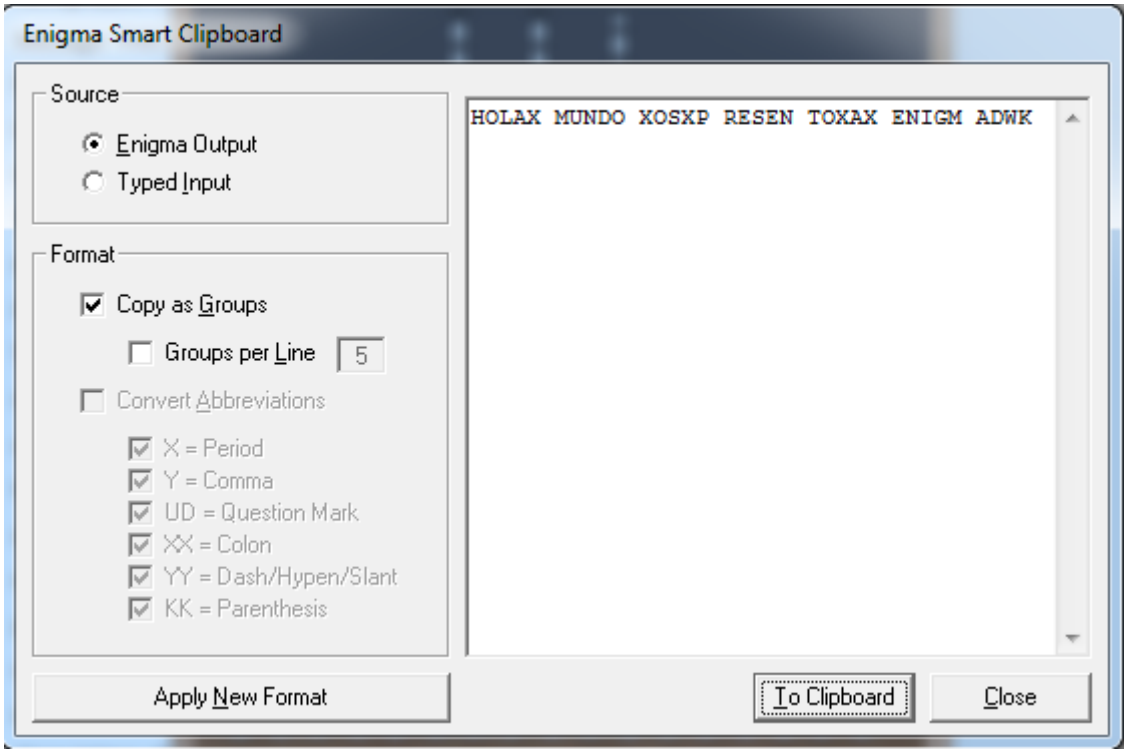


Que se cifra en



Para descifrar debemos conocer la clave del día KFC y la clave del texto cifrada que es WVM. Entonces decodificamos WVM a partir de la posición KFC y obtenemos la llave MIR. Colocando ahora en esta posición obtenemos a partir del texto cifrado





Como se observa se recupera el texto.

Ejercicio 8.

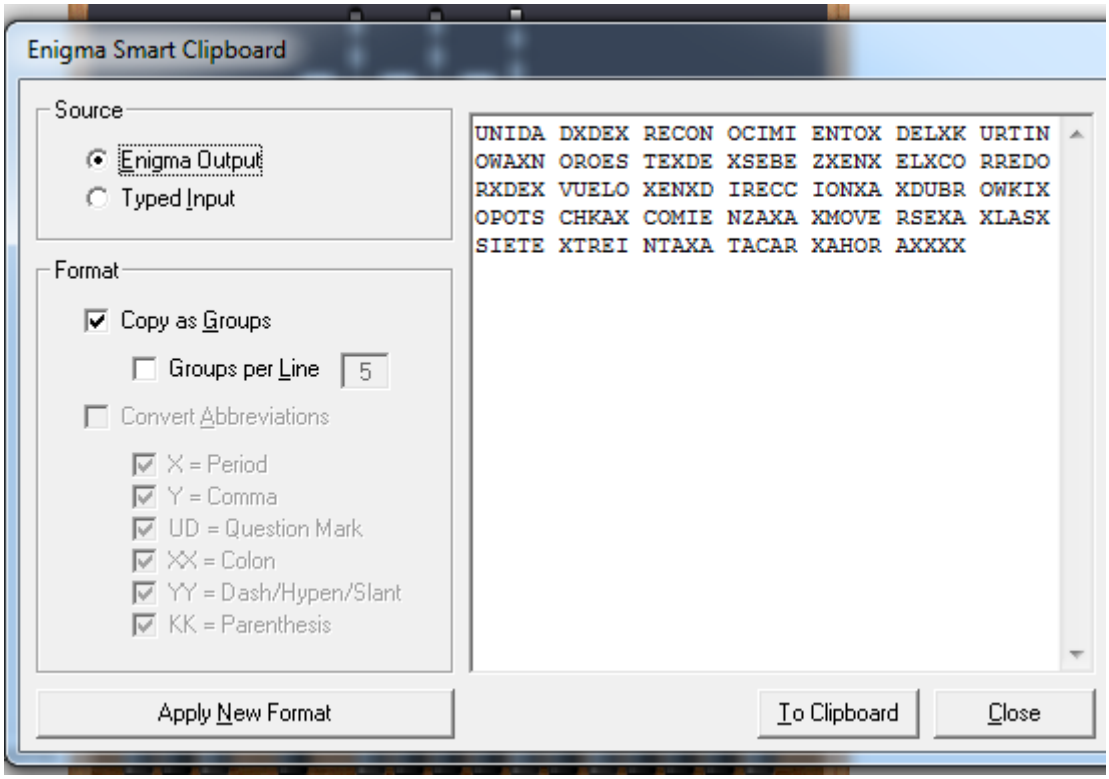
En caso de haber un error de sincronización a partir de ese momento todo lo que se descifra es basura.

Ejercicio 9.

Se observa como era de esperar que al ser una única letra en el texto cifrado no aperce dicha letra ya que no es posible. Por tanto, si ciframos una sola letra podría ser susceptible de criptoanálisis ya que faltaría dicha letra en el texto cifrado. En cuanto al periodo, esta máquina tiene un periodo igual al espacio de llaves y por tanto no es posible.

Ejercicio 10

Clave CFJ

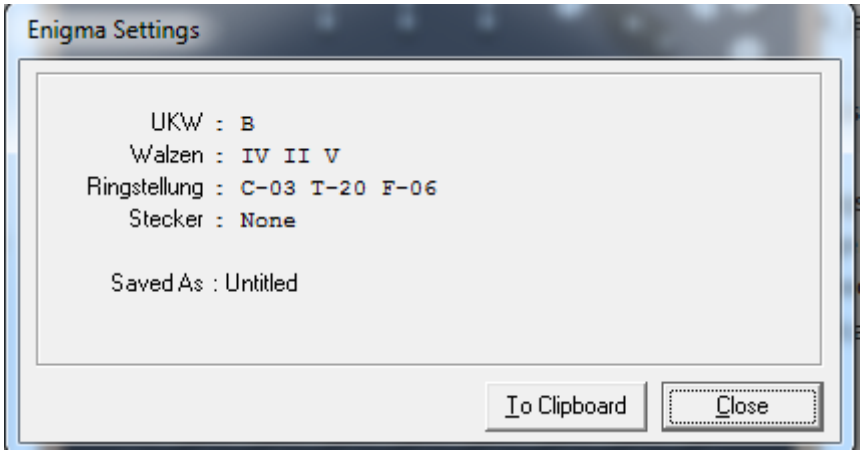


Ejercicio 11.

Al realizar un análisis de las letras que aparecen en el texto cifrado vemos que falta una letra y es la z. Esto quiere decir que es la letra utilizada ya que el cifrado de una letra nunca será la misma letra.

Ejercicio 12.

La configuración original es



Con la posición de inicio 3 21 4 pasamos a cifrarlo obteniendo

```
JDYVR HHDCZ PXNBP IUFUO ZESBN AXVYH PPRQO
CFTAX NIUSS SSTSI GVBFD DRAEN KJAKA AMWQI
NQEBO C
```

Ahora probamos a descifrar usando el programa en C.

```
javier@ubuntu:~/Universidad/SPSI/p1$ gcc break_enigma_1.c enigma.c NBestList.c
coreText.c -lm -O3
javier@ubuntu:~/Universidad/SPSI/p1$ ./a.out
searching for rotors: ......
```

```
javier@ubuntu:~/Universidad/SPSI/p1$ ./a.out
searching for rotors: ..........................................................
..
searching ring settings: ..
final key:
indicator=DSQ, rotors=235, rings=AIT, plugboard=
decryption: PBRNALKHKWIRENIASEXPERISPXGDDEJNQTEARESZLMOCICANCTINAGFNMBMQYKJNDSNC
URTZUJAD
```

El resultado no es el esperado ya que habíamos cambiado los espacios por X y eso inducía a error. Ahora cambiando el texto a cifrar, únicamente suprimiendo los espacios entre las letras, podemos obtener el texto plano a partir del texto cifrado.

```
JDYOS KMUPU OLLXC HOEVN MXOFZ ALIOF VHIIC
XABMD XEOUO TZZKG ZIKBP QHQGN KS
```

```
javier@ubuntu:~/Universidad/SPSI/p1$ ./a.out
searching for rotors: ..........................................................
..
searching ring settings: ..
final key:
indicator=AAZ, rotors=425, rings=AAB, plugboard=
decryption: THEENIGMACIPHERWASAFIEWDEJPHERUSEDBYTHEGERMANSDUQACAWORLDWARII
```