Práctica 3

ENCRIPTACIÓN CLÁSICA

José Ángel Dorado González

Seguridad Informática

ÍNDICE

6º)¿Cómo podría romperse por fuerza bruta automáticamente la encriptación Caesar general de un fichero?. Realiza una pequeña investigación. ¿Serías capaz de implementarla?.

Lo que se podría hacer es coger las palabras de todas las posibles combinaciones del ejercicio anterior y meterlas en un diccionario, una vez hecho esto, iríamos comprobando la cantidad de palabras del diccionario que aparecen en las combinaciones hasta encontrar la combinación que más palabras tenga, cuando se encuentre esa será la combinación correcta porque es la que más palabras del diccionario posee.

10º)Intentar romper el cifrado mono-alfabético anterior mediante análisis de frecuencias. Analiza e idea un plan con las herramientas de que dispones para llevarlo a cabo. ¿Podría automatizarse el proceso?

El análisis de frecuencias resulta tremendamente efectivo para lograr romper el cifrado monoalfabético, lo que se intenta realizar es lograr saber el desplazamiento que se ha aplicado. Para conseguir esto cogeremos las frecuencias de aparición de letras en español, dicha lista es la siguiente:

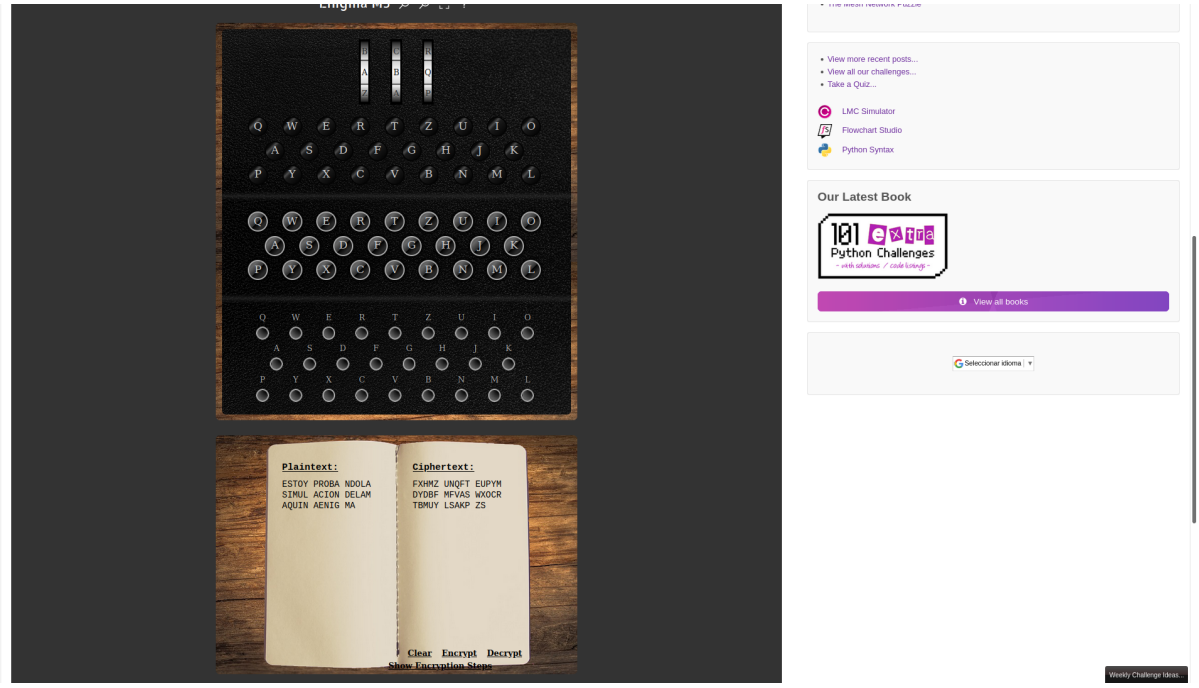
Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Porcentaje	12,53%	1,42%	4,68%	5,86%	13,68%	0,69%	1,01%	0,70%	6,25%	0,44%	0,02%	4,97%	3,15%	6,71%
Letra	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Porcentaje	0,31%	8,68%	2,51%	0,88%	6,87%	7,98%	4,63%	3,93%	0,90%	0,01%	0,22%	0,90%	0,52%	

Posteriormente contaríamos el número de veces que aparece cada letra en el mensaje cifrado para saber su probabilidad, una vez hecho esto bastaría con encontrar el porcentaje de probabilidad que más se asemeje en la tabla de arriba y ver su desplazamiento con dicha información.

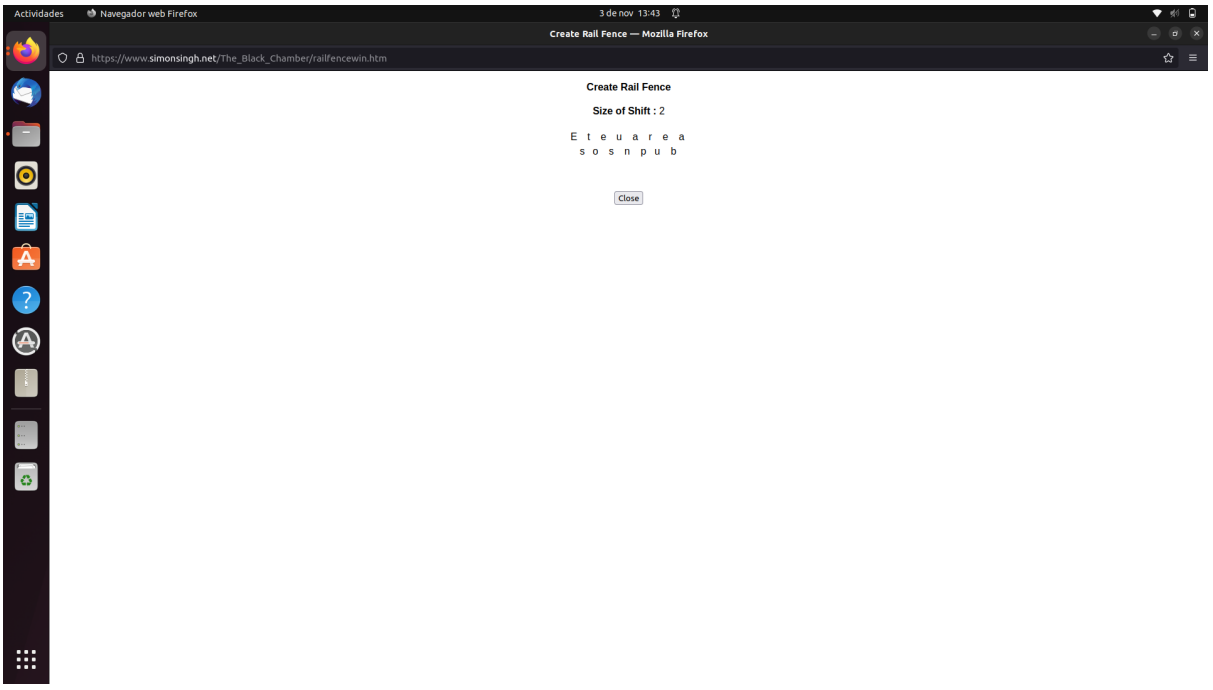
Este proceso se puede automatizar muy fácilmente, se podría realizar un programa que contenga los datos de la anterior tabla y que se encargue de contar las letras del mensaje cifrado, una vez hecho esto sería ir comprobando la frecuencia de aparición de cada letra del texto cifrado con la de los datos introducidos anteriormente, con esto conseguiremos saber su desplazamiento y por lo tanto el mensaje se podrá descifrar.

13º)Acceder al enlace de ejercicios de encriptación de la página web de la asignatura y probar sus herramientas de encriptación.

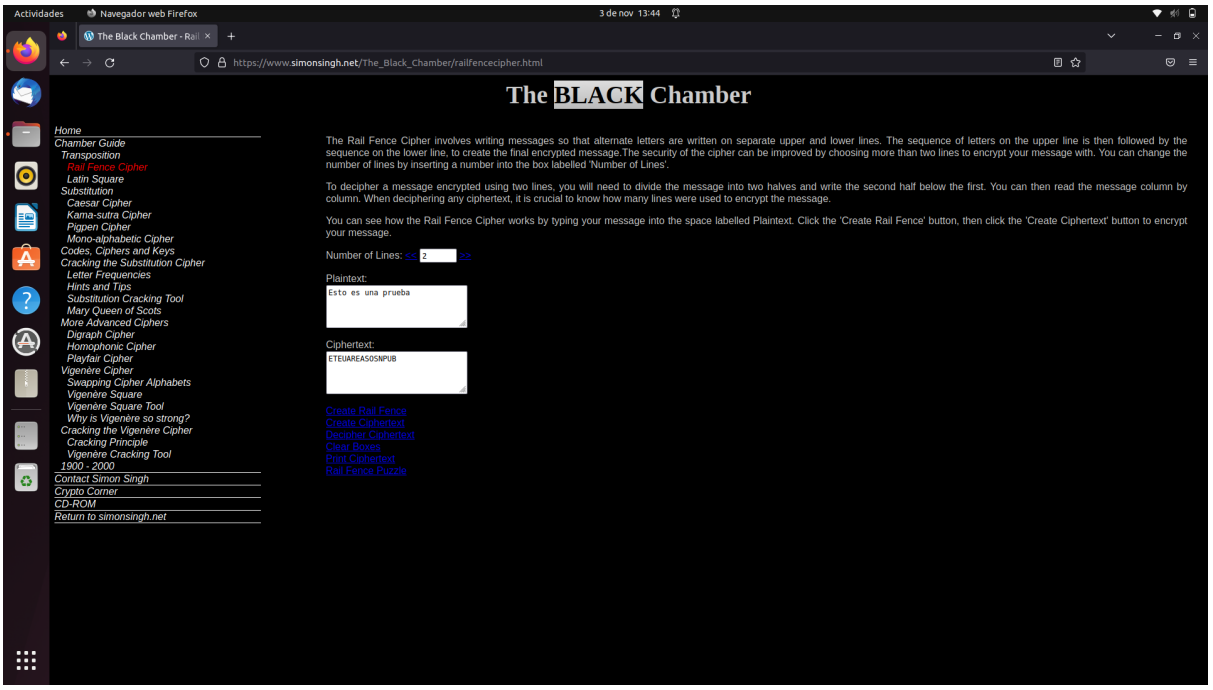
Enigma



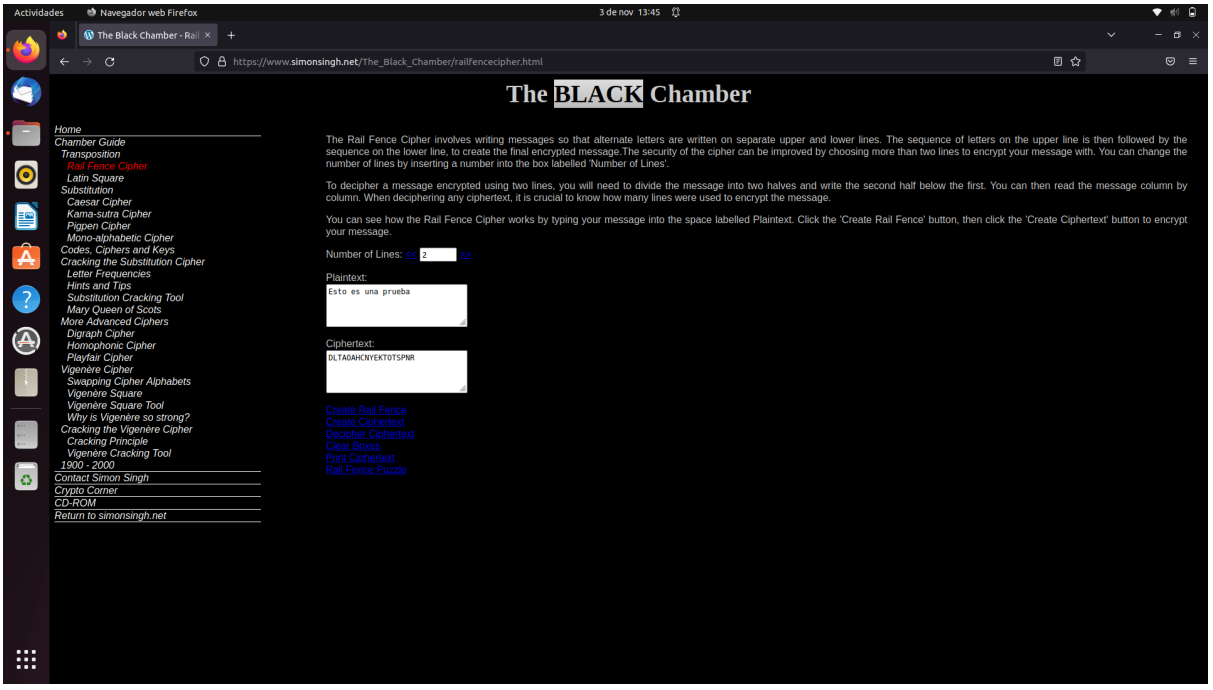
Rail Fence



Ciphertext



Rail Fence Puzle



15º)Busca en Internet varias 'Rotor Machines' (al menos 3) y anota el autor, año de fabricación y uso de cada una de ellas. Las rotor machines supusieron un gran avance en la historia de la criptografía y un paso hacia la criptografía moderna.

Combined Cipher Machine

Año

Surgió durante la Segunda Guerra Mundial, fue aprobada en octubre de 1942 y su producción comenzó dos meses más tarde.

Autor

Los británicos habían mostrado su principal máquina de cifrado, Typex, a los EE. UU. cuando entraron en la guerra, pero los estadounidenses se mostraron contrarios a compartir su máquina, la ECM Mark II. Existía una necesidad de comunicaciones seguras entre los aliados, por lo que la Marina de los EE. UU. desarrolló esta máquina de cifrado adaptada a los sistemas de ambos países.

Uso

Se utilizó inicialmente a pequeña escala para uso naval a partir del 1 de noviembre de 1943, y entró en funcionamiento en todas las fuerzas armadas de EE. UU. y el Reino Unido en abril de 1944.

Enigma Machine

Año

Surgió al final de la Primera Guerra Mundial, los primeros modelos se utilizaron comercialmente desde principios de la década de 1920.

Autor

La máquina Enigma fue inventada por el ingeniero alemán Arthur Scberbius.

Uso

La máquina Enigma es un dispositivo de cifrado utilizado para proteger las comunicaciones comerciales, diplomáticas y militares. Fue empleado ampliamente por la Alemania nazi durante la Segunda Guerra Mundial, en todas las ramas del ejército alemán. La máquina Enigma se consideraba tan segura que se usaba para cifrar los mensajes más secretos, además era compacta y fácil de transportar.

La seguridad del sistema depende de las configuraciones de la máquina que generalmente se cambiaban a diario, según las listas de claves secretas distribuidas con anticipación, y de otras configuraciones que se cambiaban para cada mensaje. La estación receptora tendría que conocer y utilizar la configuración exacta empleada por la estación transmisora para descifrar correctamente un mensaje.

Lorenz Cipher

Año

Fue desarrollada en 1940.

Autor

Fue desarrollada y creada por una empresa alemana llamada Lorenz, que era un importante productor de telecomunicaciones en Alemania en ese momento.

Uso

Los alemanes utilizaron las máquinas de rotor Lorenz durante la Segunda Guerra Mundial para la comunicación estratégica entre las principales ciudades de la Europa ocupada por los alemanes.

Estas máquinas se empezaron a utilizar de forma sustancial desde mediados de 1942 en adelante para comunicaciones de alto nivel entre el Alto Mando alemán en Wünsdorf, cerca de Berlín, y los Mandos del Ejército en toda la Europa ocupada.Más adelante, entre febrero de 1943 y junio de 1944, su uso era prácticamente rutinario.

Los mensajes descifrados de Lorenz hicieron una de las contribuciones más significativas a la inteligencia ultramilitar británica y a la victoria aliada en Europa, debido a la naturaleza estratégica de alto nivel de la información que se obtuvo de los descifrados de Lorenz.