Universidad de Alcalá

Kevin van Liebergen Ávila

Práctica 0
Explotación de la herramienta JCrypTool (i)

Máster en ciberseguridad

Asignatura: Criptografía aplicada

2021

Contents

Objetivo

Se presenta la herramienta JCrypTool y se solicitan diversos ejercicios para explotar sus funcionalidades. En esta primera práctica manejando la herramienta, se practica su instalación y se plantean ejercicios manejando los sistemas de criptografía clásica.

Resultados

Como resultado de esta práctica, se espera que cada alumno se familiarice con el uso de esta herramienta, explorando sus posibilidades más sencillas. Se sugieren los siguientes puntos:

1. Cifrado y descifrado con los cifradores clásicos de César y Vigenère, de sustitución y de trasposición.
2. Análisis de frecuencia en textos y criptogramas.
3. Generación de números aleatorios y cálculo de entropías.

Esta herramienta será la que utilicemos para la mayor parte de las prácticas de los distintos protocolos criptográficos estudiados en esta asignatura

1 HERRAMIENTA JCrypTool

Para desarrollar esta y las siguientes prácticas se ha procedido a instalar la herramienta JCrypTool, para ello se ha seguido las instrucciones, sin embargo se ha instalado en el directorio `/opt/` y se ha creado un enlace simbólico como aparece en la imagen 1 para no ejecutar la ruta ccompleta que aparece a continuación.

```
$ /usr/local/jcryptool/JCrypTool &
```

```
sudo ln -s /opt/jcryptool/JCrypTool /usr/local/bin/jcryptool
```

Figure 1: Link simbólico

De tal manera que lanzamos el comando y se nos abre la herramienta `JCrypTool` como se nos muestra en la imagen 2.

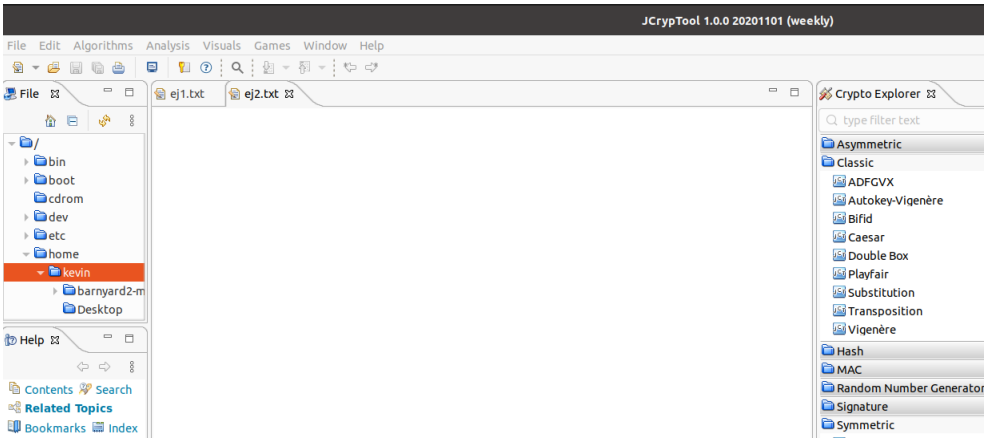


Figure 2: Página principal JCrypTool

2 DESARROLLO DE LA PRÁCTICA

En esta primera práctica, basta con familiarizarse con algunas de las funcionalidades más básicas:

- Cifrado de César y Vigenère.
- Mecanismos de sustitución y trasposición.
- Análisis de frecuencias.
- Análisis de entropía.

Idealmente, debemos leernos la primera parte titulada **Introduction to the e-learning software JCrypTool**, que nos proporciona una primera visión de la herramienta y sus posibilidades.

Es interesante ir recorriendo las distintas opciones y vistas que proporciona la herramienta siguiendo ese tutorial.

Por ejemplo, podemos dirigirnos al menú desplegable de Algorithms (también en la ventana Crypto Explorer) donde encontraremos los cifradores en el menú de algoritmos clásicos.

Por su parte, en el menú desplegable de Analysis encontraremos el análisis de frecuencias y de entropía.

[...]

La presentación contiene una (larga) segunda parte en que explica las distintas aplicaciones una por una. Como estamos empezando, conviene ir a una de las más sencillas titulada JCrypTool console for classic methods, y seguir la explicación. Con el paso del tiempo, iremos viendo otras aplicaciones más complejas (¡sin agotarlas, por supuesto!)

2.1 Cifrado de César Y Vigenère

Cifrado César

El cifrado César es un tipo de cifrado por susticución monoalfabética, en el que una letrase desplaza un número determinado de veces en el alfabeto, todas las letras se desplazan el mismo número de veces. Para realizar un cifrado de tipo César con el `JCryptTool` es necesario seleccionar en la ventana `Algorithms` la sección `Caesar`.

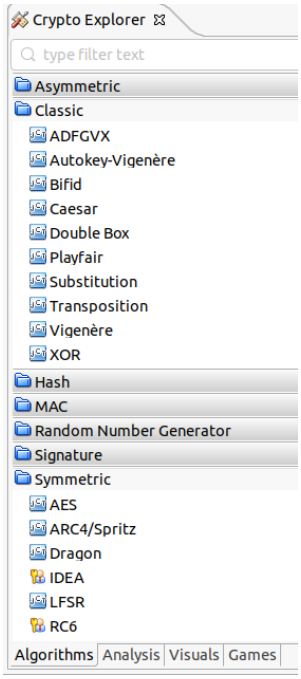


Figure 3: Sección algoritmos

Una vez hemos clickado nos aparecerá la ventana de la imagen 4 en el que podremos elegir si cifrar, descifrar el mensaje, y en vez de la selección nos pregunta el número de veces que se desplazará cada letra. El contenido del texto original es 'hola' y vamos a seleccionar que se desplacen 13 posiciones.

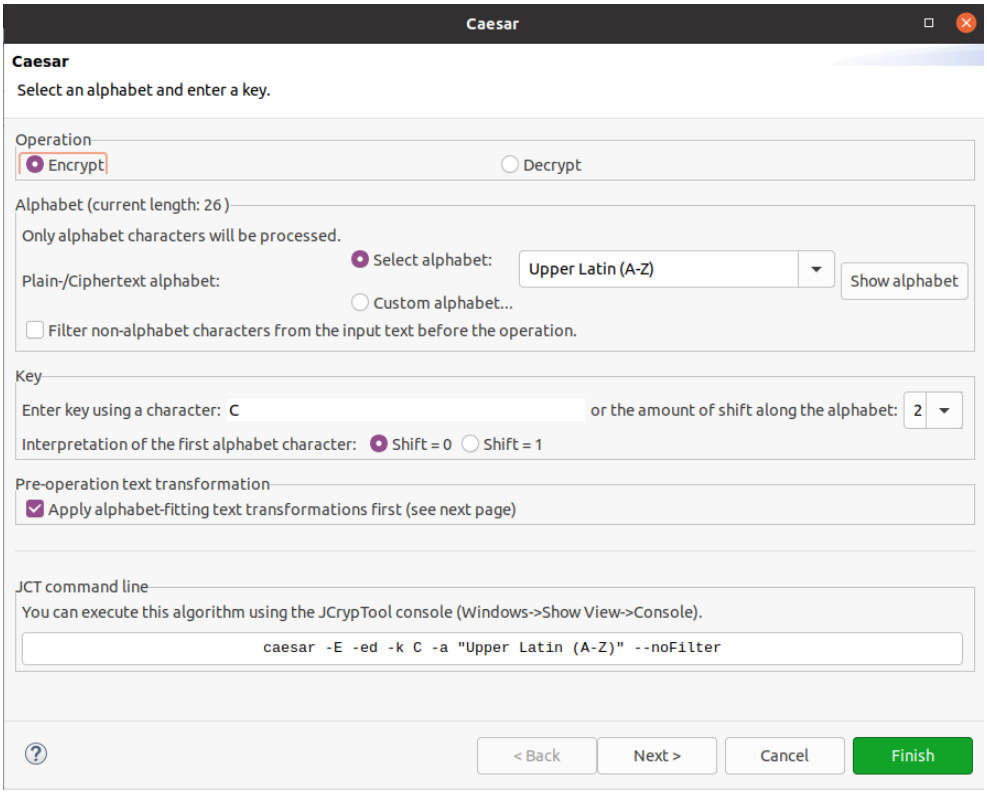


Figure 4: Ventana tipo César

Al desplazarse 13 posiciones la primera letra del mensaje en claro, la 'h' se transforma en la 'U', la 'O' en la letra 'B' y así sucesivamente como se muestra en la imagen 5.

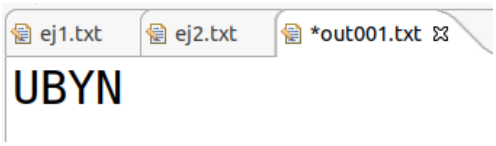


Figure 5: Mensaje cifrado mediante cifrado César

Este cifrado se considera roto debido a que es posible mediante fuerza bruta probar 26 veces (el número de letras del abecedario) desplazar las letras hasta que un texto coincida o sea legible.

Para textos muy grandes es posible realizar análisis por frecuencias y también se consideraría roto.

Cifrado Vigenère

El cifrado de Vigenère es un cifrado de sustitución polialfabético, la clave de cifrado/descifrado indican la cantidad de veces que se va a desplazar las letras del texto en plano, teniendo en cuenta que si la clave es '`LEMON`' la primera letra realizará una rotación de tipo desplazamiento 12 (ROT12) que corresponde a la L, la siguiente letra realizará un ROT5, la siguiente ROT13 y así sucesivamente hasta completar con la longitud de la clave, y después se volvería a empezar por la primera letra de la clave y así sucesivamente hasta completar todo el mensaje del texto plano.

En este caso el texto en plano el '`Hola buenas tardes que tal`' como aparece en la figura 6.

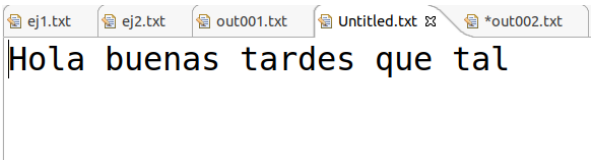


Figure 6: Texto a cifrar

En la figura 7 se observa las características que podemos aplicar al algoritmo, podemos seleccionar si queresmo cifrar o descifrar, el tipo de alfabeto que queremos, la clave, que en este caso hemos seleccionado `PERRO` y la generación del comando para que podamos insertarlo en la terminal de `JCrypTool`.

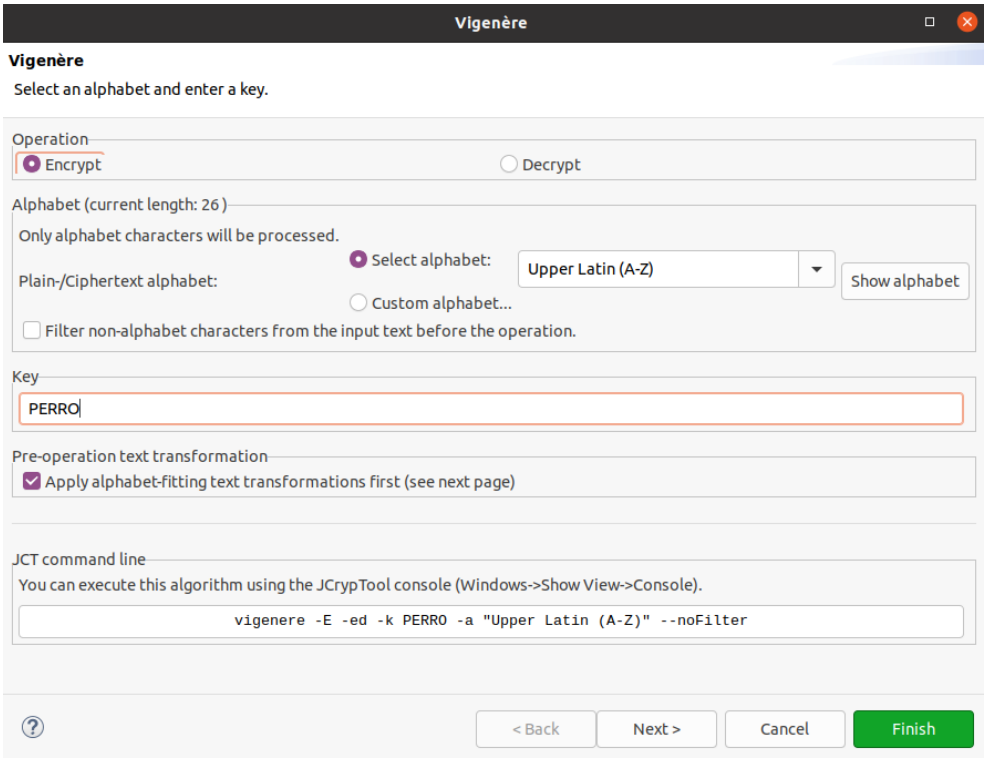


Figure 7: Ventana Vigenère

Cuando realizamos el cifrado con la clave `PERRO` nos aparece un fichero nuevo con el contenido del mensaje cifrado, como aparece en la figura 8.

Para analizar el contenido del mensaje vamos a realizar la comprobación de las dos primeras letras, para la letra 'H' (posición 8 del abecedario), le corresponde realizar una operación de cifrado con la letra 'P' (posición 16 del abecedario), por lo que se desplazará 15 veces (se resta 1 porque la letra A, cuenta como el desplazamiento 0, a partir del B se empieza a desplazar), el resultado debe encontrarse en la letra 23 del abecedario, la letra '`W`'.

Para la letra del mensaje en plano 'O' (posición 15) le corresponde realizar una operación de cifrado con la letra 'E' (posición 5 del abecedario), por lo que desplazando 5-1 posición, la letra final debe encontrarse en la posición 20 del abecedario, esto es la letra de la posición 19 (letra 'S') como se muestra en la figura 8.

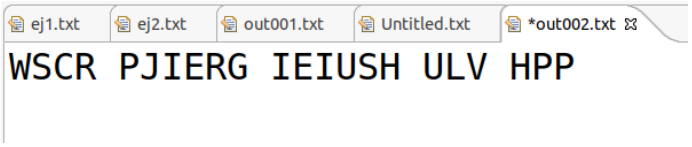


Figure 8: Texto cifrado por Vigenère

La fuerza del cifrado de Vigenère radica en la longitud de la clave, sin embargo, al igual que con el cifrado César, con textos largos es posible realizar análisis de frecuencias, uno de los métodos más conocidos se denomina el método Kasiski [1].

2.2 Mecanismos de sustitución y transposición

Sustitución

El cifrado por sustitución es un método de cifrado por el que unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular, estas unidades puedes ser una sola letra, pars de letras, etc. El receptor descifra el texto realizando la sustitución inversa.

Para este apartado debemos seleccionar la opción '`Substitution`' y nos debe aparecer una ventana como la de la imagen 9.

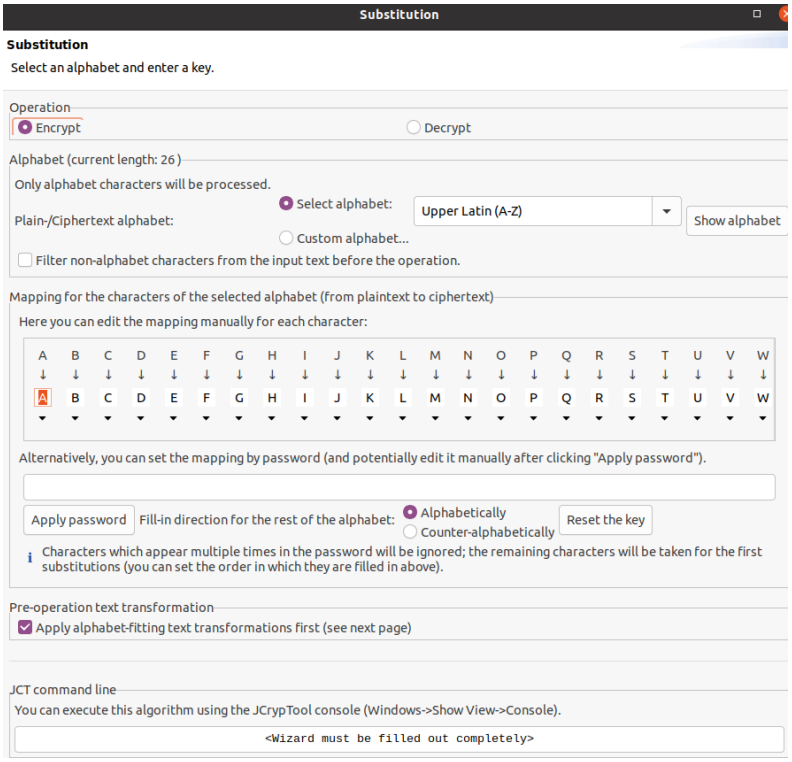


Figure 9: Ventana principal de ajustes para el cifrado de sustitución

Vamos a construir una tabla de sustitución para cifrar el mensaje en plano anterior, para ello la tabla/diccionario es la que se muestra en la imagen 10.

[1] https://es.wikipedia.org/wiki/Metodo_Kasiski

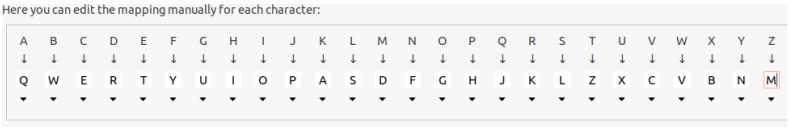


Figure 10:

Como se puede observar la letra '`H`' se sustituye por la '`I`' y así con todas las letras sucesivamente.

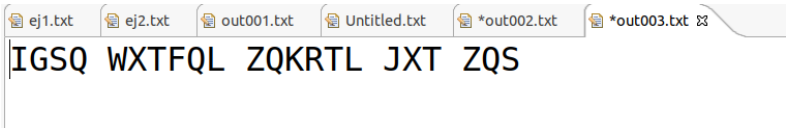


Figure 11: Mensaje cifrado por sustitución

La tabla de descifrado, como es lógico no es la misma que la de cifrado, si no su inversa, si en la imagen 10 la '`A`' se sustituye por la letra '`Q`', en la tabla de descifrado de la imagen 12 la letra '`Q`' se sustituye por la letra '`A`'.

Figure 12: Tabla de descifrado

Descifrando el mensaje nos aparece correctamente el mensaje original.

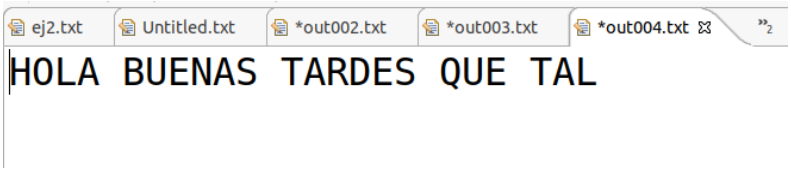


Figure 13: Mensaje original

Al igual que en los cifrados anteriores este tipo de cifrado con textos grandes se encuentra vulnerable frente a criptoanálisis, debido a que al ser cifrados monoalfabéticos (la misma letra en plano siempre resulta en la misma letra cifrada) es posible conocer las letras cifradas que más se repiten y cotejarlas con las letras que más se repiten para mensajes en plano.

Transposición

El cifrado por transposición es un tipo de cifrado simétrico en el que unidades de texo plano se cambian de posición siguiendo un esquema bien definido, es decir hay una permutación de unidades de texto (P. ej. la escítala).

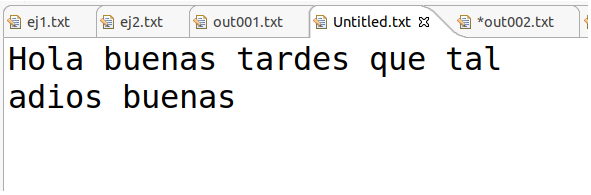


Figure 14: Texto plano a cifrar

Seleccionando la opción '`Transposition`' se nos muestra una ventana como en la figura 15 donde podemos elegir características propias del algoritmo de cifrado.

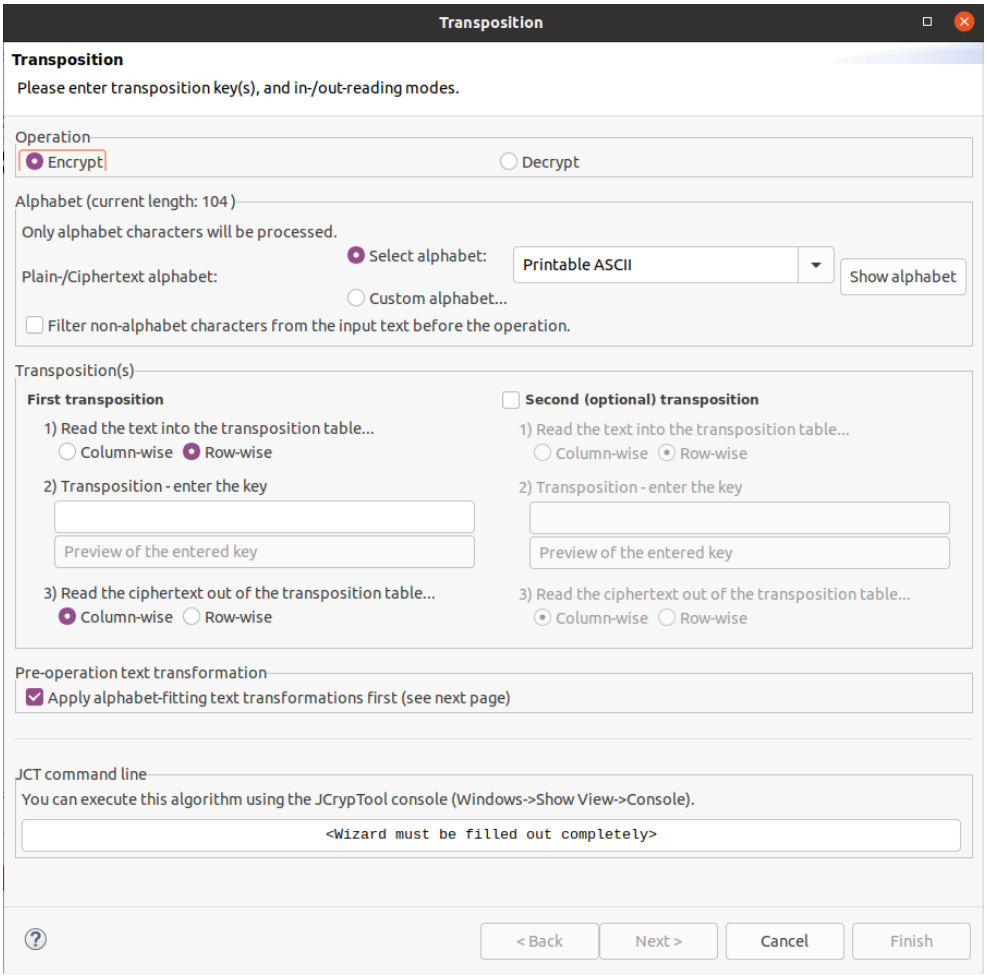


Figure 15: Ventana principal transposición

Eligiendo como clave de transposición la clave '`cba`' que se traduce como `3|2|1` cifrado el mensaje en plano anterior y nos devuelve el mensaje cifrado.

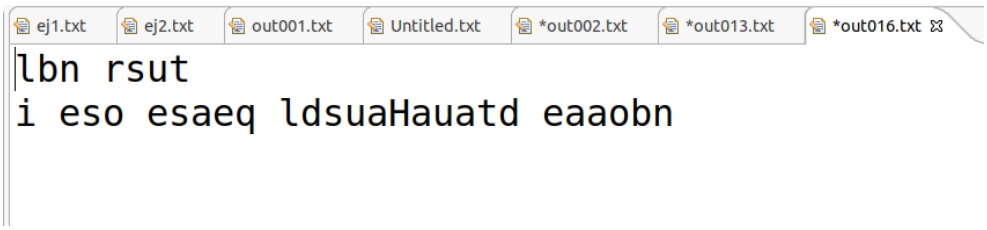


Figure 16: Mensaje cifrado mediante transposición

Eñ análisis por frecuencias revela una frecuencia de letras idéntica la del texto claro por lo que debe procederse a la utilización de métodos como el

anagramado múltiple, cabe mencionar que un ataque de texto claro conocido revela completamente la clave.

2.3 Análisis de frecuencias

El análisis de frecuencias es un tipo de criptoanálisis en el que se estudian el número de apariciones de una letra en un mensaje cifrado de tal manera que sea posible conocer y cotejar los datos con probabilidades del texto en plano.

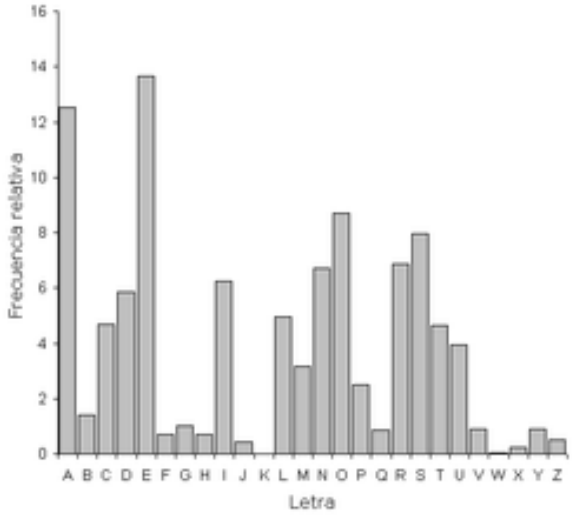


Figure 17: Frecuencia de las letras en un texto español

Para probar ello vamos a seleccionar un texto más largo que los anteriores, vamos a aplicar un cifrado de tipo César y seguidamente analizar realizar un análisis de frecuencias. Para ello el texto que hemos seleccionado es el de la figura 18.

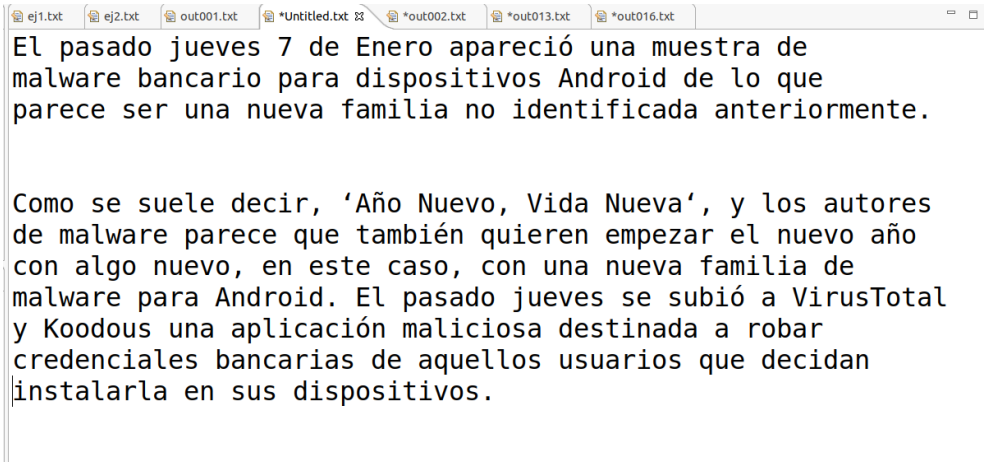


Figure 18: Texto a cifrar

El texto anterior cifrado mediante un cifrado Césr de tipo ROT7 es el de la figura 19.

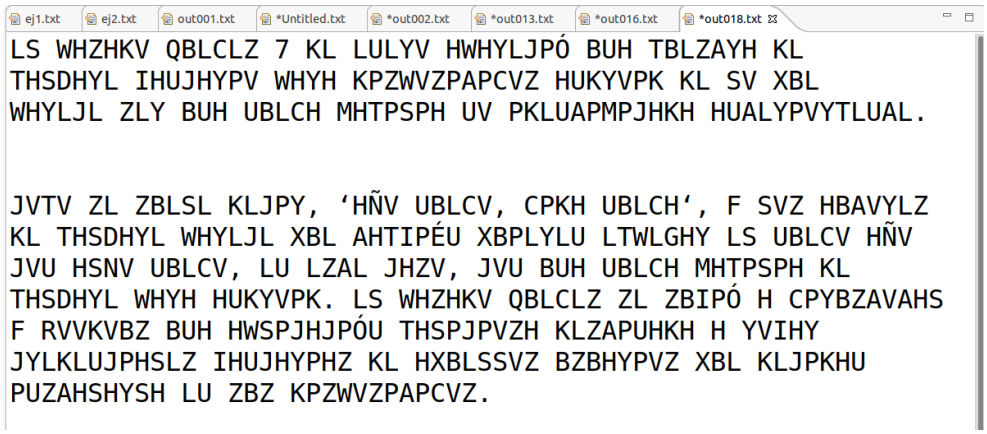


Figure 19: Texto cifrado

Seguidamente y con el texto vifrado vamos a analizar la frecuencia de aparciión de las letras, seleccionamos en la pestaña de '`Analysis`' la opción de '`Frequency Analysis`'.

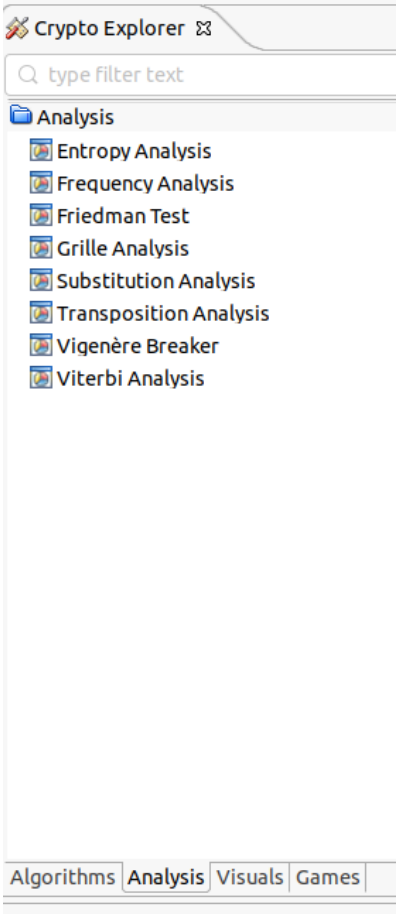


Figure 20: Sección análisis

Podemos observar en la figura 21 que la letra que más veces ha salido es la 'H' y después la 'L'. En el habla hispana las letras que más aparecen son la letra E con un 13,68%, A con un 12,53% y O con un 8,68%. Por ello podemos cotejar la letra 'L' y desplazar 8 veces (posición de la H) en el abecedario hacia atrás, así con todas las letras, si el mensaje es ilegible podríamos intentar desplazarlo 12 veces (posición 'L' en el abecedario).

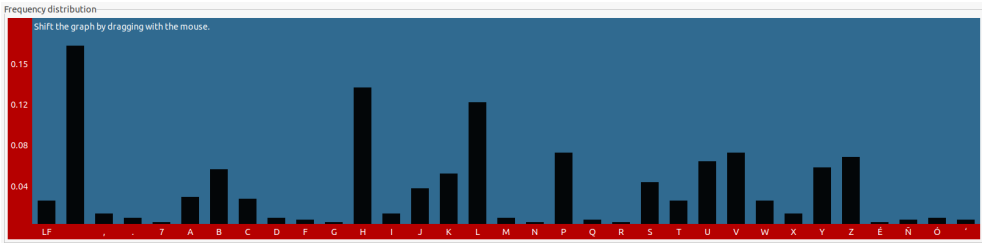


Figure 21: Análisis de frecuencia

Con ello podemos corresponder las letras del criptograma con ciertas letras del texto plano.

2.4 Análisis de entropía

La entropía mide la incertumbre de una fuente de información. Orientado a la seguridad es muy importante debido a que evalúa el grado de seguridad de los sistemas.

Para medir la entropía de un sistema mediante `JCrypTool` lo hacemos clickando en '`Entropy Analysis`' en la figura 20, con ello se nos abrirá una venta como aparece en la figura 22.

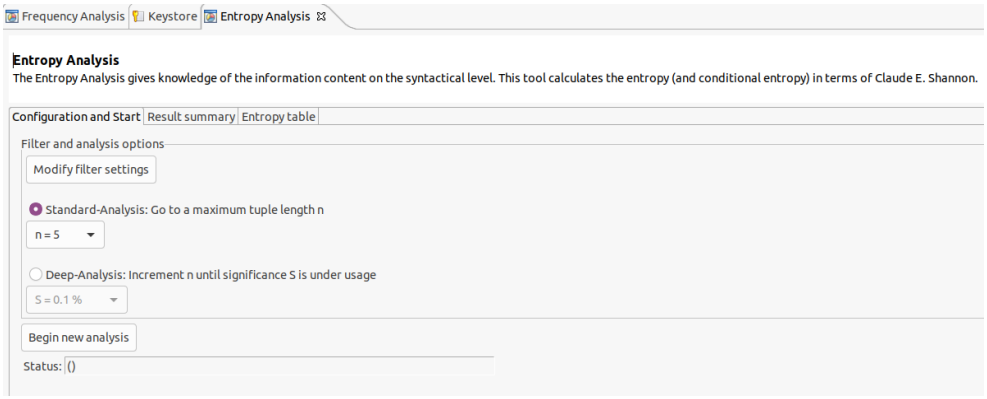


Figure 22: Ventana entropía

Los resultados del análisis los podemos observar en la imagen 23, en este caso nos aparece la información relacionada para l valores mínimos y máximos G(1) y G(5).

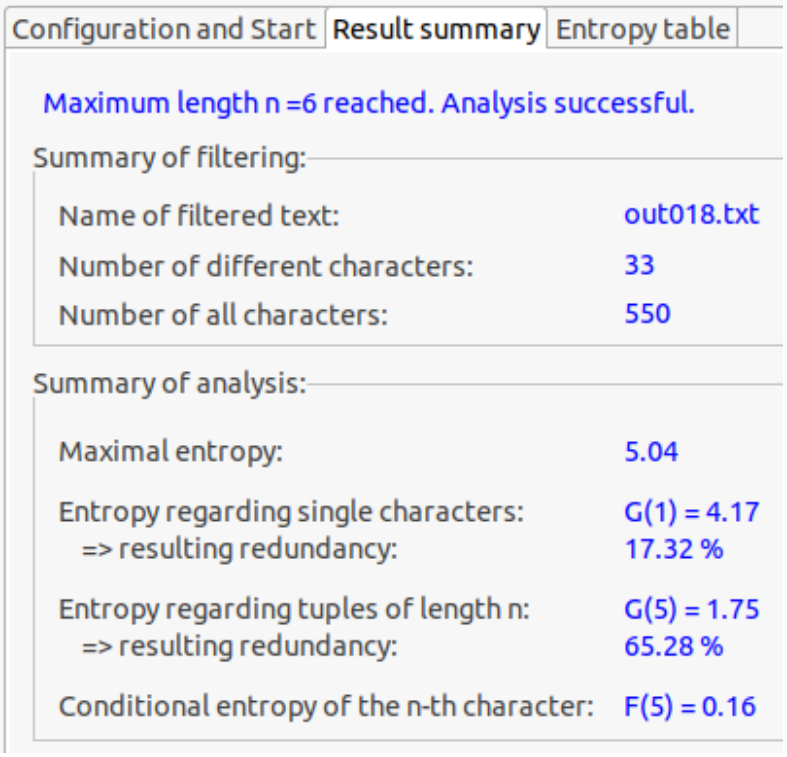
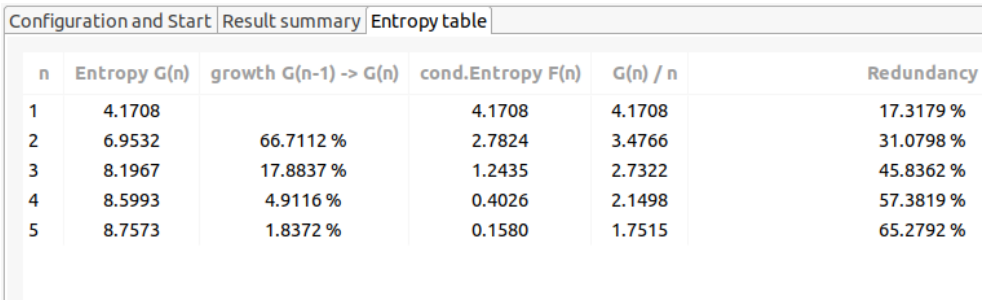


Figure 23: Resultados del análisis de entropía

Tambien nos aparece la información más detallada de la entropía para cada n en la figura 24, en lugar de para los valores n = 1 y 5 como en la figura 23.



n	Entropy G(n)	growth G(n-1) -> G(n)	cond.Entropy F(n)	G(n) / n	Redundancy
1	4.1708		4.1708	4.1708	17.3179 %
2	6.9532	66.7112 %	2.7824	3.4766	31.0798 %
3	8.1967	17.8837 %	1.2435	2.7322	45.8362 %
4	8.5993	4.9116 %	0.4026	2.1498	57.3819 %
5	8.7573	1.8372 %	0.1580	1.7515	65.2792 %

Figure 24: Tabla de resultados del análisis de entropía

2.5 Generación de números aleatorios

Un generador de números aleatorios está diseñado para producir secuencias de números sin un orden aparente, es ideal poder tener un enerador realmente aleatorio, sin embargo eficientemente es complicado y por ello se utilizan

generadores pseudo-aleatorios. `JCryptTool` nos provee de una herramienta para generar números aleatorios mediante el algoritmo SHA1, dentro de la pestaña `Algorithms` > `Random Number Generator` seleccionamos `SHA-1`.

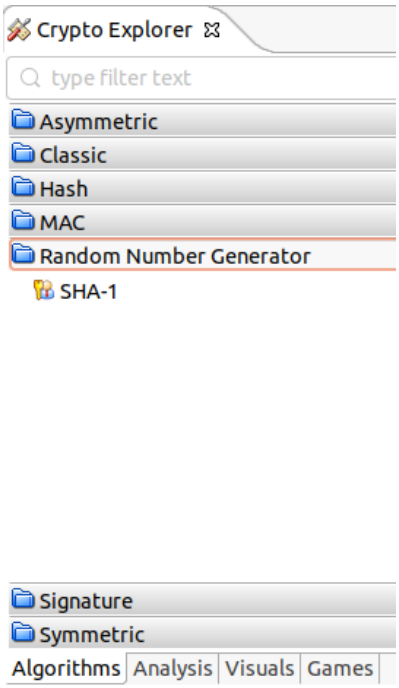


Figure 25: Pestaña generación de números aleatorios

En la pestaña que se nos aparece podemos elegir el tamaño de la salida del generador de números y el tipo de salida (hexadecimal, binaria, números) como se muestra en la figura 26.

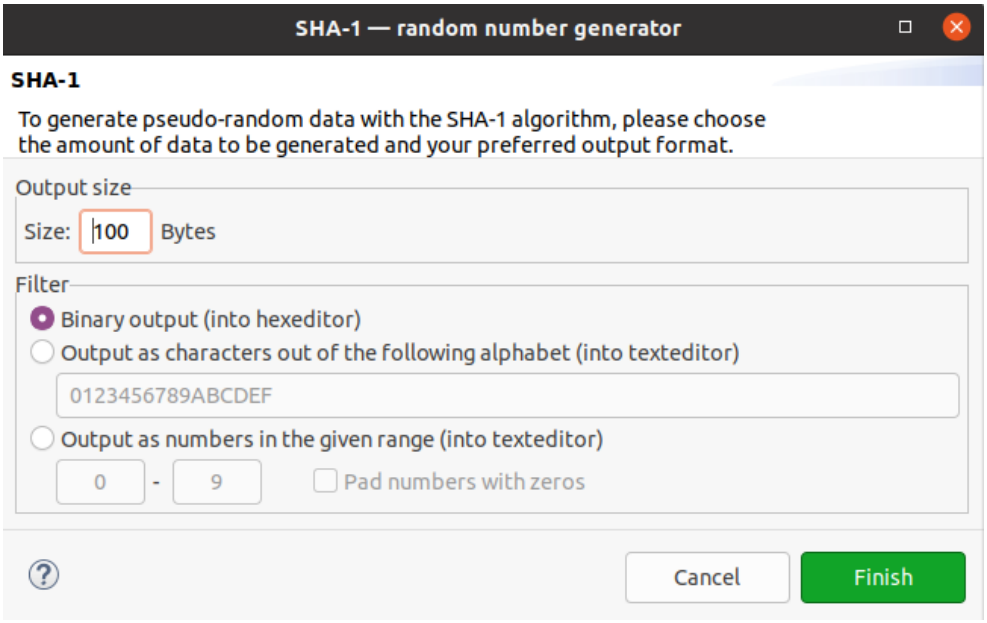


Figure 26: Ventana generación de números aleatorios

Y una vez clickamos en Finish se nos aparece la salida, en este caso 100 bytes de forma binario pero dumpeada en hexadecimal.

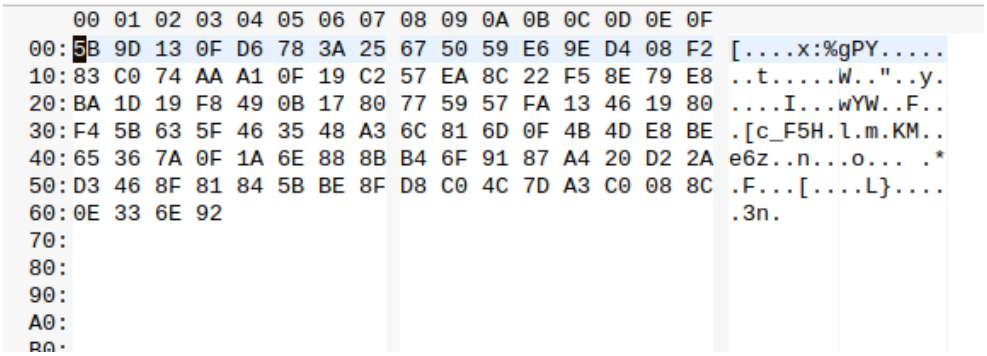


Figure 27: Resultado de la generación de números aleatorios

`JCryptTool` nos ofrece multitud de algoritmos para poder realizar operaciones criptográficas, en esta práctica hemos contemplado los algoritmos más sencillos y los primeros que se idearon para cifrar mensajes, sin embargo en las próximas prácticas observaremos la fortaleza que tiene esa herramienta a la hora de realizar algoritmos más complejos.