Practica 2. La herramienta *Cryptool*. Uso de herramientas con cifrados clásicos.

1. Instalar la herramienta **Cryptool 1.4.3**. para máquinas con Windows de 32 bits. Instalar la versión **Cryptool 2** para máquinas de 64 bits.

2. Generar un texto suficientemente grande (con al menos 1000 caracteres) de prueba. Escoger el texto preferentemente de entre obras literarias de elección personal, de manera que la probabilidad de coincidencia con el texto escogido por algún otro compañero sea casi nula.

3. Familiarizarse con los menús de ***Cifrar/Descifrar → Simétrico(clásico)*** y ***Simétrico(moderno)*** y los de ***Procedimientos Individuales → Visualización de Algoritmos***, ***Análisis → Herramientas para el Análisis***, ***Análisis → Cifrado Simétrico(clásico)*** *y* ***Ayuda → Escenarios***.

Tareas a realizar:

4. Escoger 3 métodos distintos de cifrado simétrico clásico y comprender como cifran. Explicarlo y añadir ejemplos con textos llanos en castellano.

5. Realizar un análisis del cifrado con ***Entropía, Histogramas, Frecuencias*** y ***N-gramas***. Calcular la ***Autocorrelación*** y la ***Periodicidad*****.**

6. Describir la llave que usa cada sistema, la Distancia de Unicidad (número total de llaves posibles) y las ventajas e inconvenientes del mismo.

7. Realizar un análisis a los textos de los ejemplos dados en Teoría sobre cifrados monoalfabéticos (**Cifrado Mono_ejemplo_1**) y polialfabéticos (**Cifrado Poli_ejemplo_2**), hasta conseguir descifrarlos. Para ello utilizar las herramientas de ***Análisis → Cifrado Simétrico(Clásico) → Sólo Texto Cifrado → Sustitución / Vigenere (según Schroedel)***

8. Tomar el texto llano generado en 2. y cifrarlo con 4 algoritmos clásicos: Uno monoalfabético, otro polialfabético, otro Enigma y el último a elegir de entre los no dados en clase y distinto de los anteriores. Para estos textos cifrados hacer una comparación de las medidas del mismo para determinar una medida comparativa de la fortaleza de los cifrados: *Entropía, Distribución de Frecuencias, Número de 3-gramas, 4-gramas, Frecuencias por 64 bytes, Autocorrelación, Medida de Vitanyi, Distancia de Unicidad, Número de Llaves*, …

Dar una interpretación de todos los resultados obtenidos y elaborar una lista ordenada de la fortaleza de los mismos en función de los anteriores parámetros.

9. Realizar un análisis al *"Texto cifrado que venció a Poe"* (**Cifrado Poe_ejemplo_3**), usando esta herramienta.

    a) Hacer un Análisis de Trigramas repetidos con CrypTool y determinar cuáles son.
    b) Calcular el periodo mediante el **método de Kasiski** aplicado al apartado anterior.
    c) Modificar el periodo obtenido por la **autocorrelación** con los datos de b).
    d) Obtener resultados parciales para intentar arreglar el problema grave anunciado en el texto cifrado.

Práctica para entrega 2:

10. Descifrar el texto dado en el "**Cifrado ejemplo_4**". Para ello:

    a) Determinar el tipo de cifrado aplicado. Determinar información sobre entropía, N-gramas, Autocorrelación, periodicidad, … y confirmar con toda esta información el tipo de cifrado.
    b) Descifrarlo con la herramienta de análisis adecuada de CrypTool.

11. Resolver el triple reto de **Mystery Twister C3** contenido en el fichero **mtc3-wacker-01-classicalciphers3-en** usando la herramienta CrypTool y dando las 3 palabras código pedidas.

12. Resolver el reto de **Mystery Twister C3** contenido en el fichero **mtc3-simon-02-adfgvx-en** cifrado con el algoritmo ADFGVX, usando también esta herramienta.