Universidad
Carlos III de Madrid

***Grupo COSEC**· Dpto. Informática*

Universidad Carlos III de Madrid

Práctica Cryptool

COSEC
Curso 2019/2020

Un experto en la resolución de problemas debe estar dotado de dos cualidades incompatibles: una imaginación inquieta y una paciente obstinación. – Howard W. Eves

Esta práctica está pensada para ejecutarse en Cryptool 1.4.XX

INTRODUCCIÓN

Antes de comenzar la práctica visite todas las opciones del menú y familiarícese con cada una de las herramientas de que consta la aplicación.

La herramienta presenta una ventana de inicio con un texto ejemplo con el que puede ser utilizado como texto en claro.

Las funciones de cifrar, descifrar etc. del menú se aplican siempre sobre la ventana que se encuentre en ese momento seleccionada.

CRIPTOGRAFÍA CLÁSICA:

Ejercicio 1 :

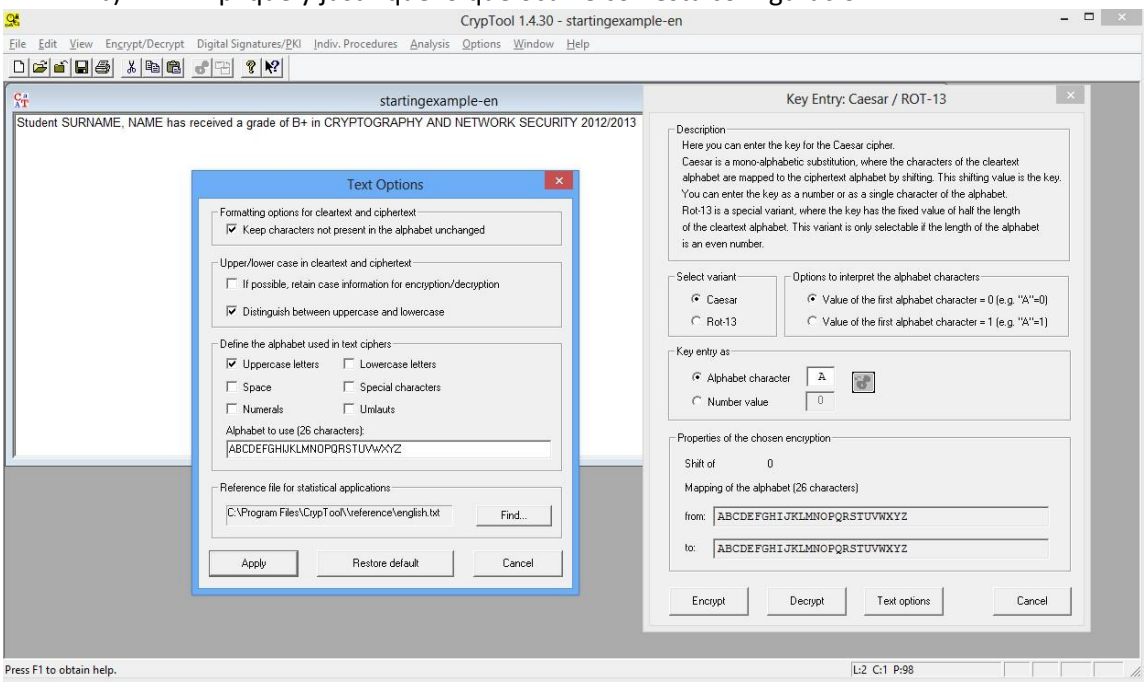
Considere el siguiente texto en claro:

```
El alumno: APELLIDO1 APELLIDO2, NOMBRE ha obtenido la calificación de
SOBRESALIENTE en la asignatura STI/CSI.
```

Copie y pegue le texto dado en un documento nuevo en el entorno de la aplicación Cryptool. Utilice el método Caesar de cifrado sobre el texto en claro utilizando distintas claves y las siguientes configuraciones:

a) Utilizando el alfabeto que contiene mayúsculas y minúsculas, ¿Qué ocurre si utiliza las claves “a”, “A” y “Z”? A la vista de esos resultados y de utilizar otras claves, ¿cómo funciona este cifrado?

b) Explique y justifique lo que ocurre con esta configuración:



Ejercicio 2:

Considere el siguiente texto en claro:

References

(1) Tuomas Aur. Modelling the Needham-Schröeder authentication protocol with high level Petri nets. Technical Report B14, Helsinki University of Technology, Digital Systems Laboratory, Espoo, Finland, September 1995. <http://www.tcs.hut.fi/pub/reports/B14.ps.Z>

(2) M. Burrows, M. Abadi, and R. Needham. A logic of authentication. In Proceedings of the Royal Society, Series A, 426(1871):233-271, 1989.

(3) John A. Clark and Jeremy Jacob. A survey of authentication protocol literature. manuscript, August 1996.

(4) Richard Kemmerer, Catherine Meadows, and Jonathan Millen. Three systems for cryptographic protocol analysis. Journal of Cryptology 7(2):79-130, 1994.

Cifre y descifre el texto dado mediante el método de Playfair y la clave "ABETOS", usando las matrices de 5x5 y 6x6.

a) ¿Se recupera todo el mensaje? ¿Hay alguna diferencia en la ejecución con distintas matrices?
b) ¿Han aparecido nuevos caracteres?

Ejercicio 3:

El siguiente criptograma corresponde al cifrado clásico de un texto en inglés, aunque se desconoce qué tipo de cifrado se utilizó. Copie y pegue este texto en un documento en blanco en el entorno de Cryptool:

c2cihgQ2Oi5aM 05hhgMZZl YjO 6Skm 5SQTb0mV4 7h 162TUg YfN T0i96WP1m 0g12S5hd8. uV76j MZ5k243YSlg a2 N5n0aKW Thf lRP 6rglOX6 ngaXR 7a2a1 3SkjaMP6, 3b5 3SSk27Y2S jia3P O ecl YQ S83g14 6acmVO P7 ikOO 7h YfKWcs2 lRPWk 0g12S5hfO36. y6fS4S-lh23P OgYd83Wl a63S26g 9K6S 426X 3850623Tn9d8 5671 lY 6Sk678 SOk1oK2S 62kSR1l YfN N2famXTQ3haYY 3kclYN2eg. zY7So2j M2cihgQ2Oi5aM 05hhgMZZl 525P 6ha6 4YWji6 MSOkY43P5bglSN6 p5aMS 0386 3SSbf 2XLZrga2 X2k2 5SQTb0mV4 7aYf 3SOm c7 XZ5fYd Z22mc4YW6. M56 6Z5d 1gXP 2g YhZWcbb8 PT1bh6-24Om2 2XLZrga2 XSm5gN3 7h 0j807h4jK0Vb0 h1Z7h0gV 6Sk67SNOm6gX T6 66kM56l25. s0S562V P0i522T6 bg h44 2g h9O L6lieZ4Whbk XPS625 3Z SgY3VP Tbba3P-6mYlO L139q2T6, 3b5 3SS e6eS4Om6gX3 7a2q SY7kc54NS 8cj 3SS o2jSQW5YlSZ1. GcnOXP7f UH, CN2W

a) Se observa que en el criptograma aparecen no sólo letras mayúsculas, sino también minúsculas y números. Abra el cuadro de diálogo en Options/Text Options y señale las opciones para ampliar el alfabeto incluyendo números y letras minúsculas (importante en este orden)

b) Calcule las estadísticas asociadas al criptograma, esto es: distribución de monogramas más frecuentes (histograma) y la relación de digramas y trigramas más frecuentes.

c) Los resultados del apartado anterior podrían ser útiles para criptoanalizar el texto. ¿Para qué tipos de criptosistemas utilizaría cada uno de esos resultados?

d) Descifre el criptograma utilizando los métodos automáticos en el menú de Análisis.

e) Calcule la Entropía del criptograma. ¿Sería razonable que la entropía del texto claro original fuera mayor que la del cifrado?

Ejercicio 4:

Efectúe el criptoanálisis de este texto tomando en cuenta las siguientes consideraciones:

- Se sabe que es un texto en castellano.
- El cifrador consiste en una sustitución monoalfabética

Se pide que descifre el texto siguiente y responda a la pregunta que se le plantea.

CRIPTOGRAMA. ¿Cuál es la distancia media de Júpiter al sol medida en millones de kilómetros?

```
 03VTV UUV5B 4Q9BU B8V4Y BJ3VB VUUVE BOVLF BLBTY FUU9N
 BE9L9 YOVLA 9QVUU BQVY3 89UBT OFV4Q BTBO9 LF4B4 YVVTE
VOB4Q 9J3VB U534V 4B49T VE3TF VTVV4 YOVUB TBUZV 4BTBQ
 BOTVB UL94B U534B YO9ZE VYBQV J3VUU V5BGB LBGBU UVO9B
 ULBTY FUU9E VO9L9 Z98F9 J3VTV YBOQB GB4NJ 3VO9L F4B4Y
 VTVQB GBEOF VTBE9 OUUV5 BOBUB LBGBU UVOFS BTVUU V59BU
BE3VO YBQVU B8V4Y BN8F9 BUBTQ 9TQVT YOBFQ BTZ9S BTJ3V
BUUFV TYBGB 4J3VB VUUVE BOVLF VO94Q 9TAVO Z9TBT Q94LV
 UUBT9 Q9T5O BLF9T BTQBZ BTJ3V QVUB4 YVQVU BE3VO YBQVU
 LBTYF UU9TV VTYBG B4T9U BSB4Q 9V4VT Y9T3L VQF9B LBT9J
 3V34E 9OJ3V O9J3V B4QBG BOVL9 5FV4Q 9QV34 9TOBT YO9K9
T34B4 9ZGOV QVUEU B4VYB 3BZFU U94VT QVPFU 9ZVYO 9TBUT
9UZVO L3OF9 XC1WM WZFUU 94VTQ VPFU8 V43TX W7C2X WK3EF
 YVOM7 XCWWX 4VEY3 49CXX CMHH7 1ZB4B QBQVE 3VOL9 TJ3VT
 F4EVO Q94BT FTVUU BZB4Y 9L934 L3VO4 9BL3N BTVBU VUU9T
 TVOVL 95V4N BUF4T YB4YV TVUVO VEOVT V4Y9B Q94J3 FK9YV
U9J3V QVTVB GBJ3V VOBJ3 VBU53 4V4B4 9ABLF BTVBU QVT38
V4FQB NBTFL 94VTY OB9L9 4YV4Y 9UUV5 9BUB8 V4YBN BUBTQ
 BZBTU BTL3B UVTL9 Z98FV O948V 4FO34 A9ZGO VQVBJ 3VUUB
 T3VOY VBOZB Q9NL9 4UB4S BNBQB O5BUU V4BTQ VZFVQ 9TVFG
 B4BV4 YOBOV 4UB8V 4YBEV O9Q94 J3FK9 YVL9U F5FV4 Q9E9O
T3A3F QBT3Z FVQ9B USB4Q 9TVUB 8FTVO BQVEB EVU94 NQVTL
3GOFV 4Q9T3 TVL9N E9U89 O9T9O 9TYO9 L945V 4YFUY BUB4Y
VN89S OVE9T BQBUV TQFK9
```