

PRÁCTICA: CRIPTOGRAFÍA CLÁSICA

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)



HERRAMIENTAS

Esta práctica está pensada para realizarse con la herramienta 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.

EJERCICIOS

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:

Solución:

Al cifrar con “a” las mayúsculas pasan a minúscula y viceversa. Esto ocurre porque la “a” no es el primer carácter, sino el primero tras todas las mayúsculas

(de ahí que el desplazamiento no sea 1, sino 27 [A..(26)..Z a]). Esto no ocurre con la "Z" (el desplazamiento es de 26 en este caso). Con la A no se produce desplazamiento.

Con esa configuración, todos los símbolos que no están en el alfabeto (minúsculas, espacios y signos de puntuación) se filtran y por ello se pierden.

Ejercicio 2:

Considere el siguiente texto en claro:

References

(1) Tuomas Aur. Modelling the Needham-Schröder 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?

Solución:

- a) Desaparecen los espacios, los signos de puntuación y los números. También desaparece la "ö" de Schröder. Si se utiliza 6X6 sí se conservan los números. Por ello hay que considerar la importancia del alfabeto en temas criptográficos.
- b) Sí, aparecen "X" entre las letras repetidas (RE FE RE NC ES TU OM AS AU RM OD EL LI NG TH EN EX ED...)

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 05hhgMZZI YjO 6Skm 5SQTb0mV4 7h 162TUg YfN T0i96WP1m
0g12S5hd8. uV76j MZ5k243YSIg a2 N5n0aKW Thf IRP 6rglOX6 ngaXR 7a2a1
3SkjaMP6, 3b5 3SSk27Y2S jia3P O ecl YQ S83g14 6acmVO P7 ikOO 7h YfKWcs2
IRPWk 0g12S5hfO36. y6fS4S-lh23P OgYd83Wl a63S26g 9K6S 426X 3850623Tn9d8
5671 IY 6Sk678 SOk1oK2S 62kSR1l YfN N2famXTQ3haYY 3kclYN2eg. zY7So2j
M2cihgQ2Oi5aM 05hhgMZZI 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-6mYIO L139q2T6, 3b5 3SS e6eS4Om6gX3
7a2q SY7kc54NS 8cj 3SS o2jSQW5YISZ1. GcnOXP7f UH, CN2W

- 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)
- Calcule las estadísticas asociadas al criptograma, esto es: distribución de monogramas más frecuentes (histograma) y la relación de digramas y trigramas más frecuentes.
- Los resultados del apartado anterior podrían ser útiles para criptoanalizar el texto. ¿Para qué tipos de criptosistemas utilizaría cada uno de esos resultados?
- Descifre el criptograma utilizando los métodos automáticos en el menú de Análisis.
- Calcule la Entropía del criptograma. ¿Sería razonable que la entropía del texto claro original fuera mayor que la del cifrado?

Solución:

- a) Señalar Numeral y Lowercase en Options/Text Options.
- b) En menu/Analysis/General/N-Gram utilizar la herramienta para determinar los monogramas más frecuentes: 2, 6, S, 5, 3; los digramas más frecuentes: 3S, 62, 7h, Sk, a2, y los trigramas más frecuentes: 3SS, %aM, 6Sk, O5h, Og1.
- c) El histograma sería útil para un cifrado monoalfabético, mientras que la relación de digramas y trigramas podría emplearse para realizar el método de Kasiski para Vigenere (e.d. polialfabético).
- d) Entropía:
 - del texto en claro: 4.25
 - del texto cifrado: 5.16

A través del cifrado se ha llevado a cabo un efecto de difusión que se refleja en la entropía.
- e) Lo normal es que un texto cifrado tenga mayor entropía que un texto en claro. De hecho, lo deseable es que los cifradores proporcionen resultados con alta entropía.

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

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

```

03VTV UUV5B 4Q9BU B8V4Y BJ3VB VUUVE BOVLF BLBTY
FUU9N BE9L9 YOVL9 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 UVOF5 BTVUU V59BU BE3VO YBQVU
B8V4Y BN8F9 BUBTQ 9TQVT YOBFO 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 BTVBV VUU9T TVOVL
95V4N BUF4T YB4YV TVUVO VEOVT V4Y9B Q94J3 FK9YV
U9J3V QVTVB GBJ3V VOB3J VBU53 4V4B4 9ABLF BTVBV
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 YOB0V 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
    
```

Solución:

Los símbolos del criptograma son mayúsculas y números, sin contar la ñ. Esto se puede deducir porque analizando el texto cifrado la ñ no aparece. El alfabeto entonces será de 36 caracteres (mod 36).

Se sabe que la sustitución es monoalfabeto.

Se intenta César con varios desplazamientos. No se consigue nada.

Se supone afín ($am+b=c \pmod{36}$).

Letras más frecuentes: V, B

Suponemos la correspondencia entre texto cifrado-texto en claro V-E B-A

$$b = 1$$

$21 = 4 \cdot a + 1 \pmod{36}$; $4 \cdot a = 20 \pmod{36}$; Se puede resolver ya que $\text{mcd}(4,36) = 4$ y 20 es múltiplo de 4. Tendrá 4 soluciones

$$y = 1 ; a = x_k = 5 + 9k \pmod{36} \text{ con } k = 0,1,2,3$$

Los posibles valores de $a = 5, 14, 23, 32$. Descartamos $a = 14, 32$ porque $\text{mcd}(a,36) \neq 1$ para que la sustitución afín se puede realizar y eso lo cumplen $a = 5, 23$

Primer intento: $a=5, b=1$

Se hace una sustitución manual con cryptool u otra herramienta como black chamber.

Cifrador:

Cifrador Tipo Afín, clave $(a,b) = (5,1)$

Alfabeto: castellano y números sin la ñ ($\pmod{36}$)

Texto en claro:

Fuese llegando a la venta, que a él le parecía castillo, y a poco trecho della detuvo las riendas a Rocinante, esperando que algún enano se pusiese entre las almenas a dar señal con alguna trompeta de que llegaba caballero al castillo. Pero, como vio que se tardaban y que Rocinante se daba prisa por llegar a la caballeriza, se llegó a la puerta de la venta, y vio a las dos distraídas mozas que allí estaban, que a él le parecieron dos hermosas doncellas o dos graciosas damas que delante de la puerta del castillo se estaban solazando. En esto, sucedió acaso que un porquero que andaba recogiendo de unos rastrojos una Nombre del planeta-- UA--Millones de kilometros al sol Mercurio 0.387 57 millones de kil. Venus 0.723 107 -- Júpiter 5.203 770 -- Neptuno 30.035 4.428 -- manada de puercos -que, sin perdón, así se llaman- tocó un cuerno, a cuya señal ellos se recogen, y al instante se le representó a don Quijote lo que deseaba, que era que algún enano hacía señal de su venida; y así, con extraño contento, llegó a la venta y a las damas, las cuales, como vieron venir un hombre de aquella suerte, armado y con lanza y adarga, llenas de miedo, se iban a entrar en la venta; pero don Quijote, coligiendo por su huida su miedo, alzándose la visera de papelón y descubriendo su seco y polvoroso rostro, con gentil talante y voz reposada, les dijo: