uc3m | Universidad Carlos III de Madrid

LAB ASSIGNMENT: CLASSIC CRYPTOGRAPHY

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | COMPUTER SECURITY LAB (COSEC) GROUP

TOOLS

This assignment is intended to be executed in Cryptool 1.4.XX

INTRODUCTION

Please take a few minutes to familiarize with the menu of the application.

The application shows a text which can be used as a clear text sample.

All cipher/decipher functions are applied to the window which is active at the time.

EXERCISES

Exercise 1:

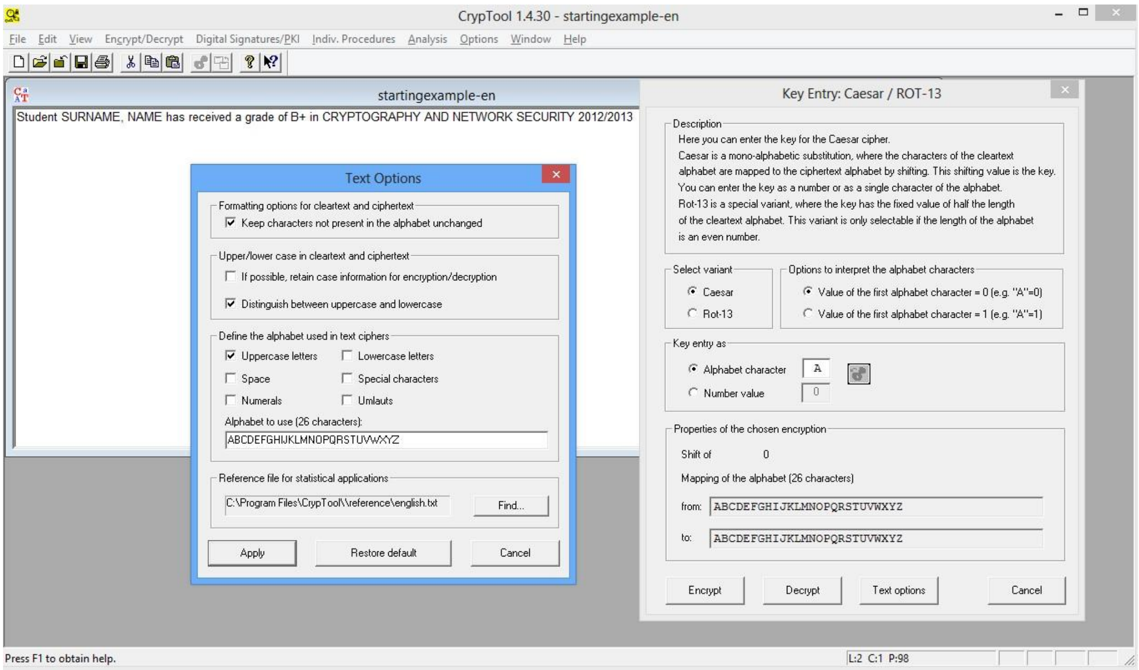
Consider the following clear text:

```
Student SURNAME, NAME has received a grade of B+ in
CRYPTOGRAPHY AND NETWORK SECURITY 2012/2013
```

Copy and paste the former text into the Cryptool environment.

a) Use the alphabet that contains upper- and lowercase. What happens if the keys “a”, “A”, “Z” are used? Taking into account these results and those obtained from your own experiments, how does this cipher work?

b) Explain and justify what happens when encrypting using this configuration:


CrypTool 1.4.30 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Apply
Restore default
Cancel
Find...
Encrypt
Decrypt
Text options
Cancel
Press F1 to obtain help.
L:2 C:1 P:98

Student SURNAME, NAME has received a grade of B+ in CRYPTOGRAPHY AND NETWORK SECURITY 2012/2013

Text Options

Formatting options for cleartext and ciphertext
☑ Keep characters not present in the alphabet unchanged

Upper/lower case in cleartext and ciphertext
☐ If possible, retain case information for encryption/decryption
☑ Distinguish between uppercase and lowercase

Define the alphabet used in text ciphers
☑ Uppercase letters ☐ Lowercase letters
☐ Space ☐ Special characters
☐ Numerals ☐ Umlauts
Alphabet to use (26 characters): ABCDEFGHIJKLMNOPQRSTUVWXYZ

Reference file for statistical applications
C:\Program Files\CrypTool\\reference\english.txt

Key Entry: Caesar / ROT-13

Description
Here you can enter the key for the Caesar cipher.
Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key.
You can enter the key as a number or as a single character of the alphabet.
Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.

Select variant
● Caesar
○ Rot-13

Options to interpret the alphabet characters
● Value of the first alphabet character = 0 (e.g. "A"=0)
○ Value of the first alphabet character = 1 (e.g. "A"=1)

Key entry as
● Alphabet character A
○ Number value 0

Properties of the chosen encryption
Shift of 0
Mapping of the alphabet (26 characters)
from: ABCDEFGHIJKLMNOPQRSTUVWXYZ
to: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Solution:

Encrypting with “a” capital letters turn to lower case letters and vice versa. It happens because “a” is not the first character, but the first one after capital letters (thus, shift is not 1 but 27). It does not happen with “Z” (the shift is 26 in this case). Using “A” no sift is identified.

With this configuration symbols not included in the alphabet (lower case letters, spaces and punctuation marks) are filtered and lost.

Exercise 2:

Consider the following clear text:

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.

Use the Playfair cipher with the key “ABETOS” and a matrix of size 5x5, and perform an encryption and decryption operations. Repeat the process with a 6x6 matrix.

a) Is the message fully recovered? What is the difference between using each matrix?

b) Are new characters present in the message? If so, why?

Solution:

a) Spaces, punctuations maks and numbers disappear. Also “ö” of Schröeder disappear. If you use 6x6 matrix, numbers are preserved. This is the reason why the encryption/decryption alphabet is essential in cryptography.

b) Yes, “X” appear in between repeated letters (RE FE RE NC ES TU OM AS AU RM OD EL LI NG TH EN EX ED…)

Exercise 3:

The following cryptogram is the result of the encryption of a text written in English:

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) As the cryptogram contains numbers, lowercase and uppercase symbols, change the text options in Cryptool to include those characters. (Beware of the order: first numbers and then lowercase)

b) Study the frequencies of single characters, and groups of two and three letters. Store the results.

c) Decrypt the cryptogram using automatic tools in menu Analysis and calculate entropy.

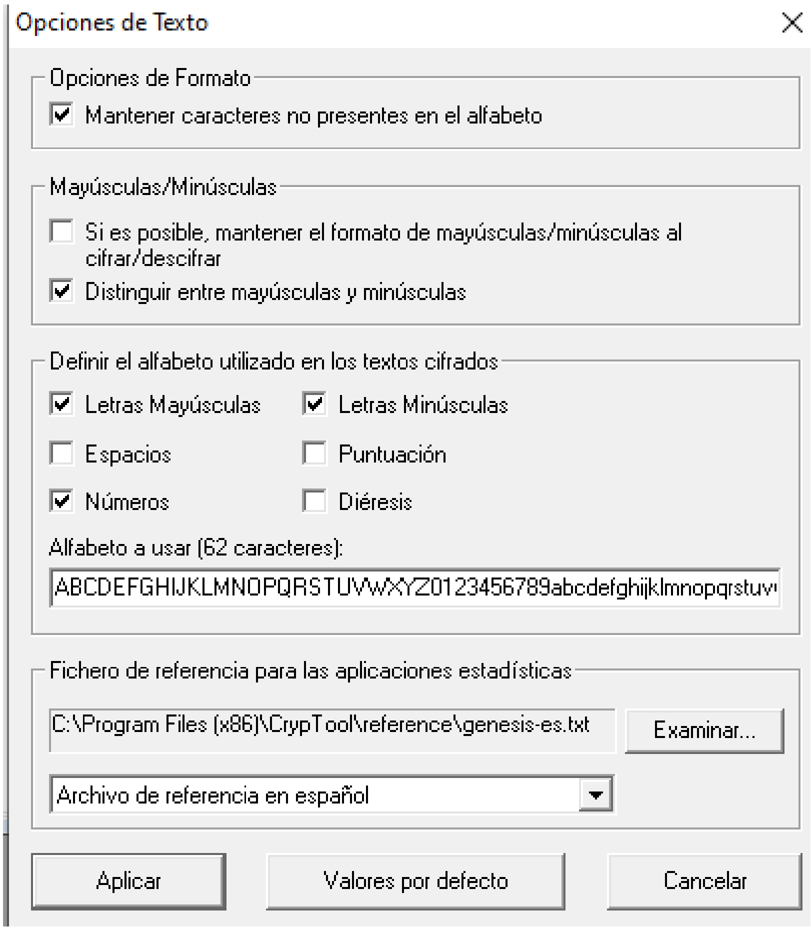
d) Is sensible to have higher entropy in the cleartext than in the ciphertext?

Solution:

a) Choose Numeral and Lowercase in Options/Text Options.

b) In menu/Analysis/General/N-Gram use the tool to choose most frequent monograms: 2, 6, S, 5, 3; most frequent digrams: 3S, 62, 7h, Sk, a2, y los most frequent trigrams: 3SS, %aM, 6Sk, O5h, Og1.

c) The alphabet to do the decryption is:



Opciones de Texto

Opciones de Formato

☑ Mantener caracteres no presentes en el alfabeto

Mayúsculas/Minúsculas

☐ Si es posible, mantener el formato de mayúsculas/minúsculas al cifrar/descifrar

☑ Distinguir entre mayúsculas y minúsculas

Definir el alfabeto utilizado en los textos cifrados

☑ Letras Mayúsculas ☑ Letras Minúsculas

☐ Espacios ☐ Puntuación

☑ Números ☐ Diéresis

Alfabeto a usar (62 caracteres):

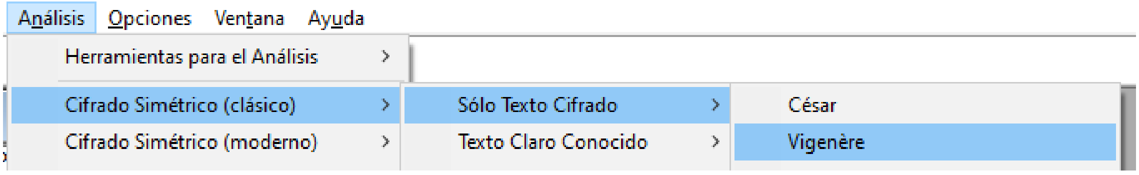
ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuv

Fichero de referencia para las aplicaciones estadísticas

C:\Program Files (x86)\CrypTool\reference\genesis-es.txt

Archivo de referencia en español

Then, decrypt automatically with Vigenere as depicted in the following:


Análisis
Opciones
Ventana
Ayuda
Herramientas para el Análisis
Cifrado Simétrico (clásico)
Cifrado Simétrico (moderno)
Sólo Texto Cifrado
Texto Claro Conocido
César
Vigenère

The key is “abetos”

d) Entropy:

- cleartext: 4.25
- ciphertext: 5.16

Encryption increases diffusion effect and entropy is affected.

It is expected to have higher entropy in ciphertexts. Indeed, ciphers should generate outputs with high entropy.

Exercise 4:

Cryptanalyze the following ciphertext considering the following:

- The text is in Spanish.

- The cipher is a monoalphabetic substitution.

Decrypt the following text.

CRYPTOGRAM. What is the average distance from Jupiter to the sun in kilometers?

```
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
```

Solution:

Cryptogram symbols are capital letters and numbers, without ñ. You can identify this because ñ does not appear in the ciphertext. Then, the alphabet will be composed of 36 characters (mod 36).

We know that it is a monoalphabetic substitution.

We can try Cesar with different shifts, but it does not work.

We assume that it is an affine cipher (am+b=c mod36)

Most frequent letters: V, B

We assume ciphertext-cleartext: V-E and B-A

b = 1

21 = 4·a+1 mod 36 ; 4·a = 20 mod 36; It can be solved because gcd(4,36)= 4 and 20 is multiple of 4. There are 4 solutions

$y = 1$; $a = x_k = 5 + 9k \bmod 36$ with $k = 0,1,2,3$

Possible values of a= 5, 14, 23, 32. However, 14 and 32 are discarded because gcd (a,36) =1 for affine substitution to work and then a should be 5 and 23.

First attempt: a=5, b=1

Manual substitution can be performed with Cryptool or any other tool like Black chamber.

Cipher:

Affine cipher, key (a,b) = (5,1)

Alphabet: Spanish with numbers and without ñ (mod 36)

Cleartext:

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 priesa por llegar a la caballeriza, se llegó a la puerta de la venta, y vio a las dos destraídas 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 estraño 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: