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:

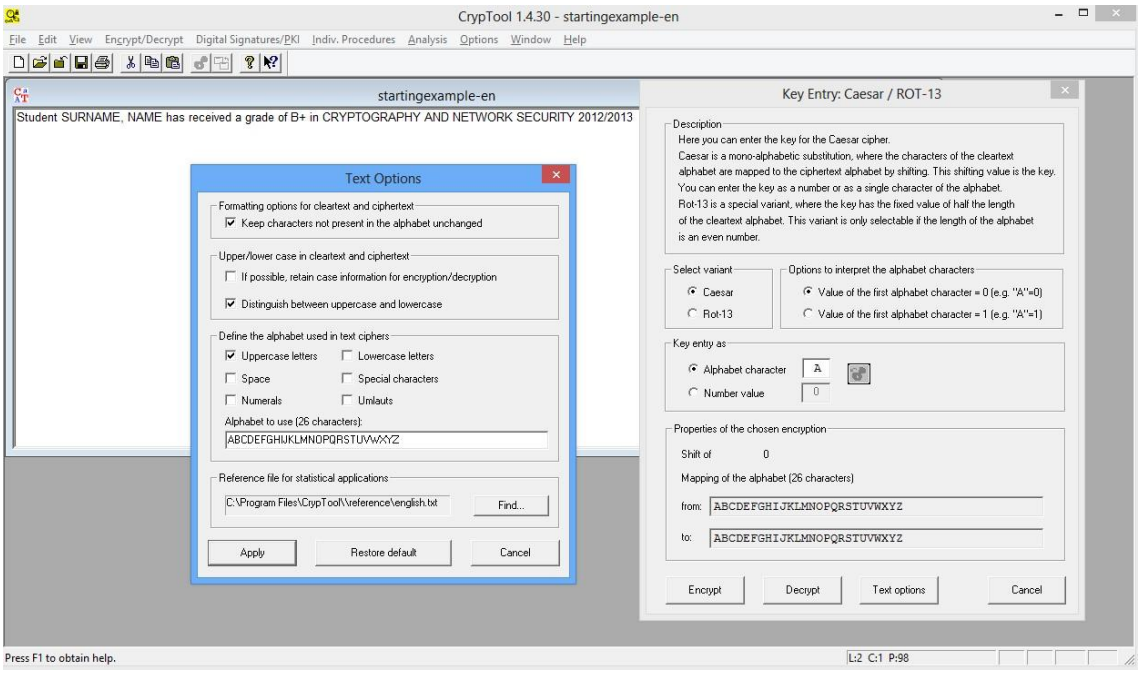
Consider the following clear text:

```
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:



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?

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) Use the automatic tools for the cryptanalysis of the ciphertext above. Give the clear text and explain the steps taken in the process.

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
```