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

Classic cryptography

Proposed exercises

Note. In these exercises, consider the Spanish alphabet (that is, including 'ñ' between 'n' and 'o', 27 symbols) unless otherwise stated.

Exercise 1 :
Considering the encryption function E(m)=7m+3 mod 27, answer the following questions

a) Which are the values of the decimation and shift constants?
b) Encrypt "TERCERA"
c) Decrypt "DID ÑOE"

Key:

a) Decimation constant = 7; Shift constant =3
b)

E("T") = E(20) = 20 · 7 + 3 (mod 27) = 8 = "I"
E("E") = E(4) = 4 · 7 + 3 (mod 27) = 31 (mod 27) = 4 ="E"

This process is repeated until getting the final message: "IEUQ EUD"

c) First we get the decryption equation:

7^{-1} (mod 27) = 4. Thus, the decryption equation is as follows
D(c) = 4(c − 3) (mod 27) = 4c − 12 (mod 27) = 4c + 15 (mod 27)
D("D") = E(3) = 4 · 3 + 15 (mod 27) = 0 = "A"
D("I") = E(8) = 4 · 8 + 15 (mod 27) = 20 = "T"
This process is repeated until getting the final message: "ATAQUE"

Exercise 2:
Given the key "LUCI" encrypt the message M= "CAMINERO" using Vigenère.

Key:

NUÑPXYTW

Exercise 3:
Given the key “PLUS" decrypt the message C= “LSAW COMW” given that it was encrypted using Vigenère.

Key:

VIGENERE

Exercise 4:
Given the key “ALA" decrypt the message C= “EDVI KVQG” given that it was encrypted using Vigenère with autokey

Key:
Given that we are dealing with the autokey variant, it is needed to decrypt it step by step as follows:

EDVI KVQG
ALA

ESV

EDVI KVQG
ALA**E SV**

ESVE RA

EDVI KVQG
ALAE SV**ER**

ESVE RANO

Exercise 5:
Given the key “MARTES", encrypt M= “FALSO PUENTE” using Playfair

Key:

BE GF PQ ZF QM RZ

Consider that the matrix is the following one:

M A R T E
S B C D F
G H I/J K L
N/Ñ O P Q U
V W X Y Z

Exercise 6:
Given the key “MARTES" decrypt C= “FOMUMB ZFTERZ” given that it was encrypted using Playfair

Key:
BUENA SUERTE X

The matrix is the same is in the previous exercise.

Exercise 7:
Given the matrix $K = \begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix}$ answer the following questions:

a) Determine if it is suitable as key for Hill ciphers.

b) Encrypt M=”RECORDAR” using Hill cipher.

Key:

a) $\det(K)=10 \neq 0$ and $\gcd(\det(K), 27) =1$, this is suitable to be used in Hill.

b) We need to work on the message in pairs of characters as follows:

Encrypt (RE) = $\begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix} * \begin{pmatrix} 18 \\ 4 \end{pmatrix} = (62\ 96) \bmod 27 = (8\ 15) =$ “IO”

Repeating the process for the remaining pairs, it leads to: C=“IOJQ GJJA”

Exercise 8:
Given the matrix $K = \begin{bmatrix} 7 & 6 \\ 3 & 11 \end{bmatrix}$ answer the following question:

a) Decrypt C=”J8D6” considering the English alphabet with numbers in the following order {A,…,Z}+{0,…,9}..

Key:

a) First, we need to compute the inverse matrix:

Given that $\text{Det}(K) = |K| = 23$, and that $\gcd(23,36)=1$, we can compute the inverse $\text{Det}(K)^{-1} = |K|^{-1} = 11$. This result can be used to compute the inverse of the matrix,

$K^{-1} = |K|^{-1} \cdot \text{adj}(A)^T \bmod 36 = \begin{bmatrix} 13 & 6 \\ 3 & 5 \end{bmatrix}$

Now we operate the ciphertext in pairs, as follows:

$K^{-1} \cdot$ "J8" mod 36 = $\begin{bmatrix} 13 & 6 \\ 3 & 5 \end{bmatrix} * \begin{bmatrix} 9 \\ 34 \end{bmatrix} = \begin{bmatrix} 33 \\ 17 \end{bmatrix}$ = "7R"

We repeat the process for "D6". The final result is: "7RPZ"

Exercise 9:
Consider the permutation K_P= (642135). Decrypt the message C= "OOEMTD IACSLS EEOCSE" which has been encrypted using that permutation.

Key:
OOEMTD IACSLS EEOCSE
1 234 5 6 123456 123456 →Re-ordering based on the permutation:

M= "METODOS CLASICOS"

Exercise 10:
Encrypt the following message M="FIESTA NACIONAL" using a 4-column transposition

Key:

It should be transposed as follows:

F I E S
TA N A
C I O N
A L X X

Thus, the result is C="FTCAI AILENO XSANX" (that is, reading the matrix by columns)