uc3m | Universidad Carlos III de Madrid

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

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”

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

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

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

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

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

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.

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}..

Exercise 9:

Consider the permutation K_P= (642135). Decrypt the message C= “OOEMTD IACSLS EEOCSE” which has been encrypted using that permutation.

Exercise 10:

Encrypt the following message M=”FIESTA NACIONAL” using a 4-column transposition