INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Lab 3: Product ciphers *March 22, 2024*

Please do the following exercises in pairs. Choose ONLY ONE of the following programming languages TO DO ALL THE EXERCISES: C, C++, Python, Java or C#.

1. Programming exercises

A product cipher combines the substitution and permutation encryption mechanisms. An example of this kind of cipher does the following:

- First we take each character of the message, find it in the following matrix and then we substitute the character with the characters in the row and column

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

- Then we use transposition. We choose a key word, this will be the first row in a matrix, then we write the ciphertext of the previous step. Then we alphabetically sort the characters of the key and rearrange the columns. Finally we took the letters of each column from top to down. This will be the final ciphertext C.

1. Design and implement a function to encipher the previous product cipher. Your function must receive the plaintext M and the keyword K, and it must return C
2. Design and implement a function to decipher the previous product cipher. Your function must receive the plaintext C and the keyword K, and it must return M.

2. Report

Every student must write her/his own document to present the programs. **It is mandatory** that your document fulfill the following:

- You can use English or Spanish to write it, but pay attention to spelling.
- Include your full name, number and title of the lab session, date.
- Briefly indicate how to run your programs and how are they organized.
- Include in your report ONLY the functions in section 1, a small paragraph in your own words explaining how each function works and the screenshots of your runs.
- Write down the values that you used to prove every function in point 1.
- Include screenshots of your program running.