INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Lab 2: Multiplicative inverse *March 15, 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

1. Write a function to implement the following algorithm, which is similar to the extended euclidean algorithm that we studied on Tuesday. The input will be a positive integer $n \geq 2$, and $a \in \mathbb{Z}_n^*$.

```
xgcd$(a, n)$
 1.    $u \leftarrow a; v \leftarrow n$
 2.    $x_1 \leftarrow 1, x_2 \leftarrow 0;$
 3.    while $u \neq 1$ do
 3.1.      $q \leftarrow \lfloor v/u \rfloor, r \leftarrow v - qu, x \leftarrow x_2 - qx_1;$
 3.2       $v \leftarrow u, u \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x;$
 4.    return $(x_1 \text{ mód } n)$
```

2. Write a function that receives as input any integer $n > 1$, the output must be a list of the elements in $\mathbb{Z}_n^*$ and the multiplicative inverse for each of them. Use the algorithm implemented in point 1. Prove your function with values of $n > 50$.

3. Design and implement a function to do the transposition cipher *scrambling with a key word* (see assignment from March 13, in Teams) . Your function must receive a key word and a message and must return the ciphertext using the transposition cipher mentioned before.

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.