Escola Politècnica Superior **Universitat de Lleida**
Grau en Enginyeria Informàtica

Computational tools for problem solving

Lab list 7 – Due on Friday December 4, 2020 at 6:00 pm

Affine Ceasar Cipher.

The affine Caesar cipher is a generalization of Caesar's cipher, which for a key pair (a, b) in $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$, encrypts a plaintext letter ℓ as

$$c = E_{a,b}(\ell) = (a\ell + b) \bmod 26.$$

The one-to-one property is a requirement in any encryption scheme. That is, an encryption algorithm should encrypt two different plaintext letters to different ciphertext letters. It can be easily seen that the affine Caesar cipher is not one-to-one for all values of a.

Problem

1) Show that for an affine Caesar cipher scheme to be one-to-one or not, does not depend on the choice of b.

2) Determine a necessary and sufficient condition on the value of a for an affine Caesar cipher scheme to be one-to-one.

3) How many one-to-one affine Caesar cipher schemes do there exist.

4) Write a program that receives as input a key pair $(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ and a ciphertext message C (of arbitrary length), and outputs the corresponding plaintext message that has been encrypted with the affine Caesar cipher scheme $E_{a,b}$.

5) Suppose that a long ciphertext message has been generated with an affine Caesar cipher scheme and the most frequent letter in the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U'. Find the key pair of this scheme.

6) Use the key pair found in 5) to decrypt the following ciphertext

$$LTJQBPTCDC.$$