TP1 Report

A85272	Jorge Mota
A83840	Maria Silva

This work has the objective to decipher 3 ciphertexts and do the respective cryptanalysis.

The ciphertexts are in uppercase characters and plaintexts in lowercase.

This ciphertexts were encrypted with *affine* , *monoalphatic substitution* and *Vigenère* (not respectively). Alhtough we didn't know which method of encryption was aplied in order, we deduced that the first one wasn't the *Vigenère*, because there was a lot of texts and too few patterns for 3 letter words.

With this we could try to first find the *affine* ciphertext since its the easist one to get the key (only 2 numbers obtained from systems of equations with modular aritmethic).

But instead we decided to decypher the *affine* and the *monoalphatic substitution* at the same time , since the *affine* is a type of *monoalphatic substitution*.

We deciphered this texts with de the `mono_decoder` function we developed in python

This function receives a ciphertext (in uppercase) and optionally a known_letters map and return the plaintext if its possible to decode

```
mono_decoder(txt,kl={})
```

Known Letters Map

It's a python dictionary used as a map to store the mapping of the cipher letters to plain letters, example:

```
known_letters = { 'G':'t', 'U':'a', 'V':'s', 'I':'o', 'T':'r', 'R':'u',
'N':'b', 'O':'l', 'S':'w', 'H':'i', 'J':'p', 'C':'n', 'B':'m', 'M':'c', 'A':'y',
'K':'g', 'F':'v', 'Z':'f', 'L':'d', 'L':'d', 'Y':'q', 'P':'k', }
```

Ciphertext #2 & #3

Ciphertext #1