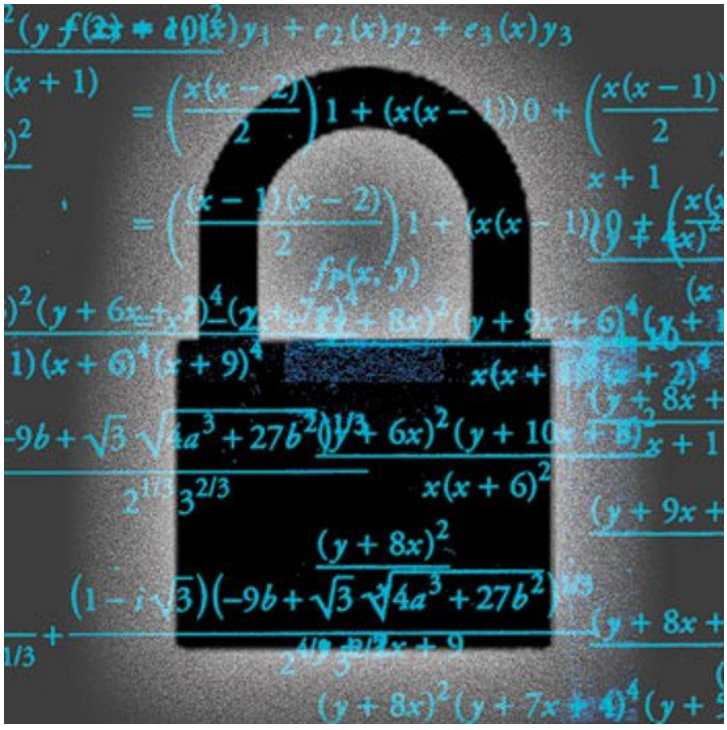
Name: Bernal Leocadio Josué Eduardo.
Teacher: Nidia Asunción Cortez Duarte.
Group: 3CM9.

Cipher affine.



Introduction

Classical cryptography we have the affine encryption which is a derivation of the cipher cease, both encryption algorithms are known as monoalphabetic, this means that there is a valid alphabet for encryption, commonly the alphabet is used in English.

Like all encryption algorithms, this method consists of an encryption function and a decryption function. The decryption function must meet certain requirements to be valid, since there may be an infinity of encryption functions for which there is no function of encryption. deciphered

Literature review.

As I mentioned before the encryption consists of an encryption function and a decryption function, the following formula is used to encrypt.

$$E(x)=\alpha(x)+\beta \bmod n$$

α, β : are integers.

x : is the position of the character to encrypt.

n :is the cardinality of the set of symbols.

This is how using this formula you can substitute a symbol for another, if we wanted to decipher a symbol we would only have to do modular algebra.

$$E(x)=\alpha(x)+\beta \bmod n :$$

$$E(x)-\beta=\alpha(x) \bmod n$$

$$\alpha^{-1}[E(x)-\beta]=\alpha^{-1}\alpha(x) \bmod n$$

$$x=\alpha^{-1}[E(x)-\beta]\,mod\,n$$

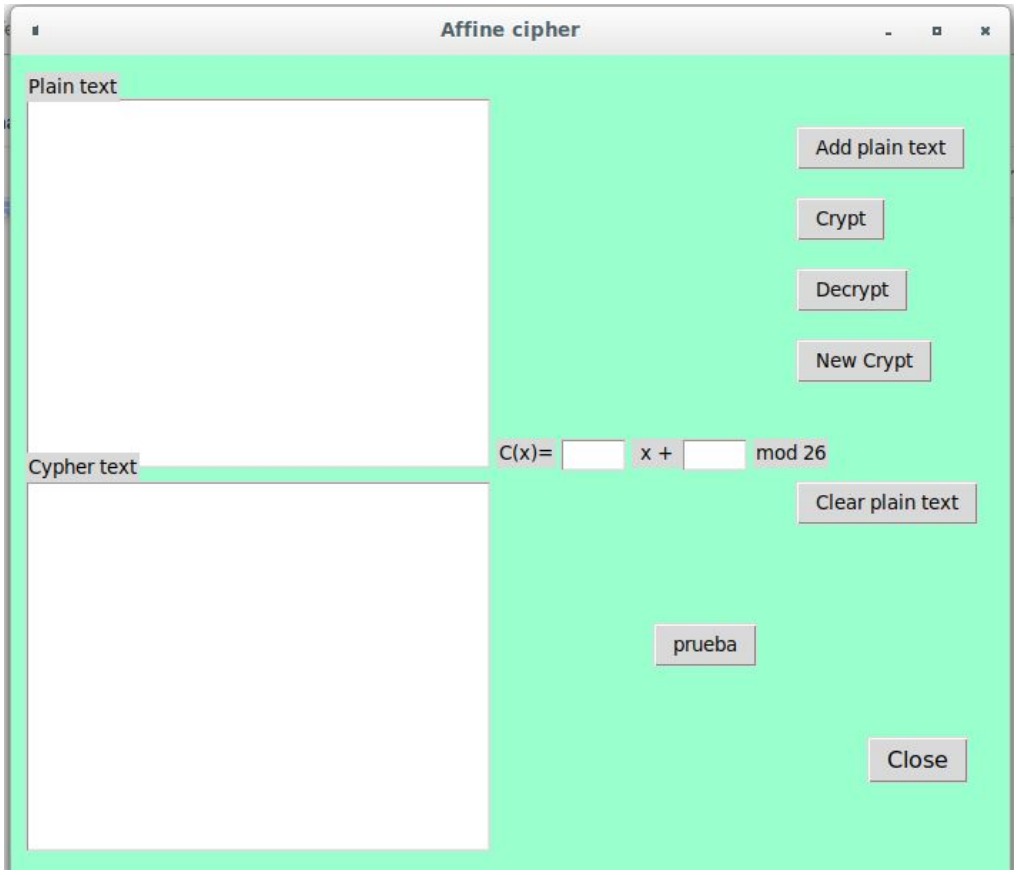
Software.

Python 2.7.15rc1

Tkinter (GUISś python)

Procedure.

We started a simple graphical user interface, with the following components.



Inputs:

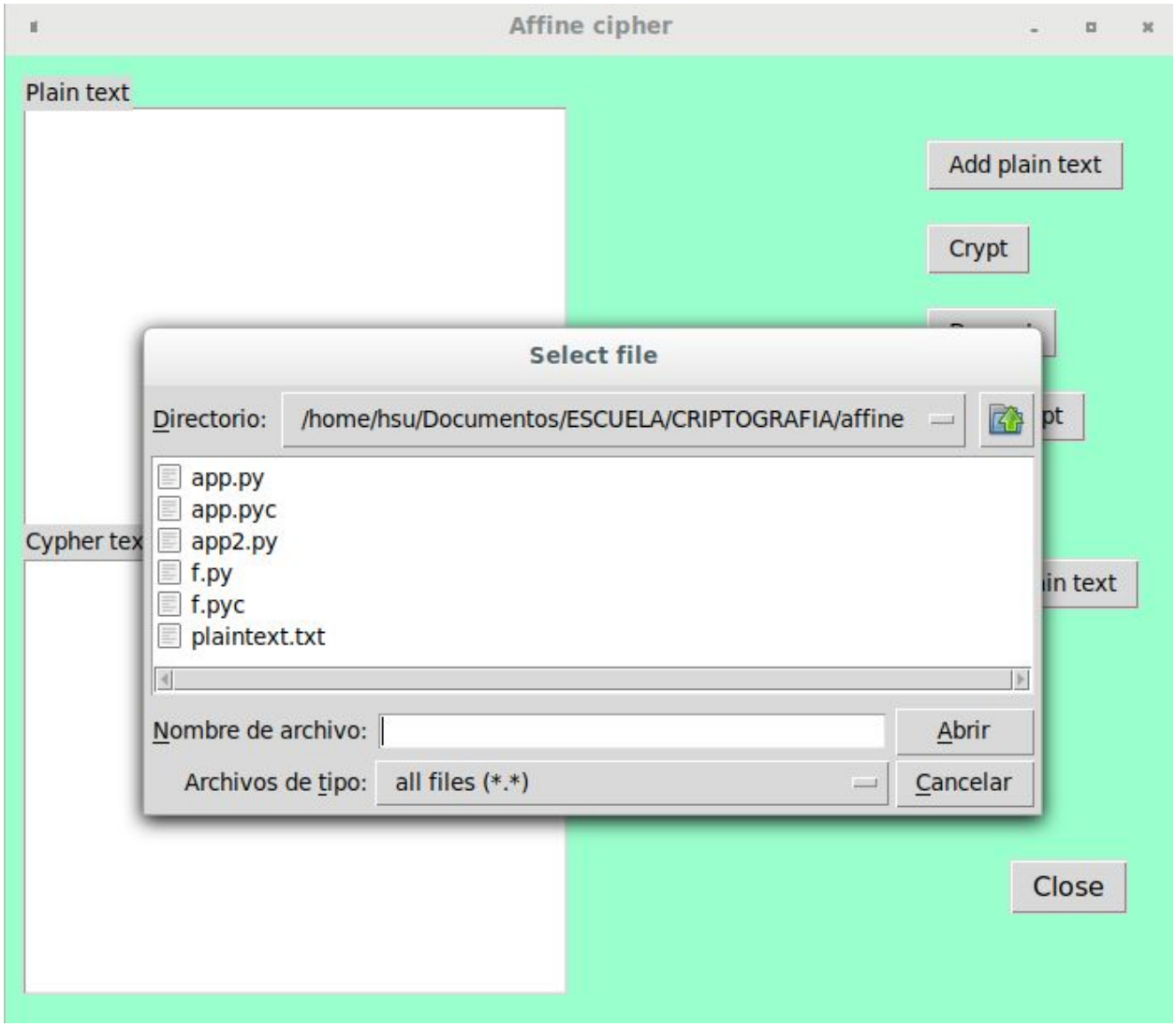
- TextArea1: Text Area to upload the plain text.
- TextArea2: Text Area to show the plaintext encrypted.

Buttons:

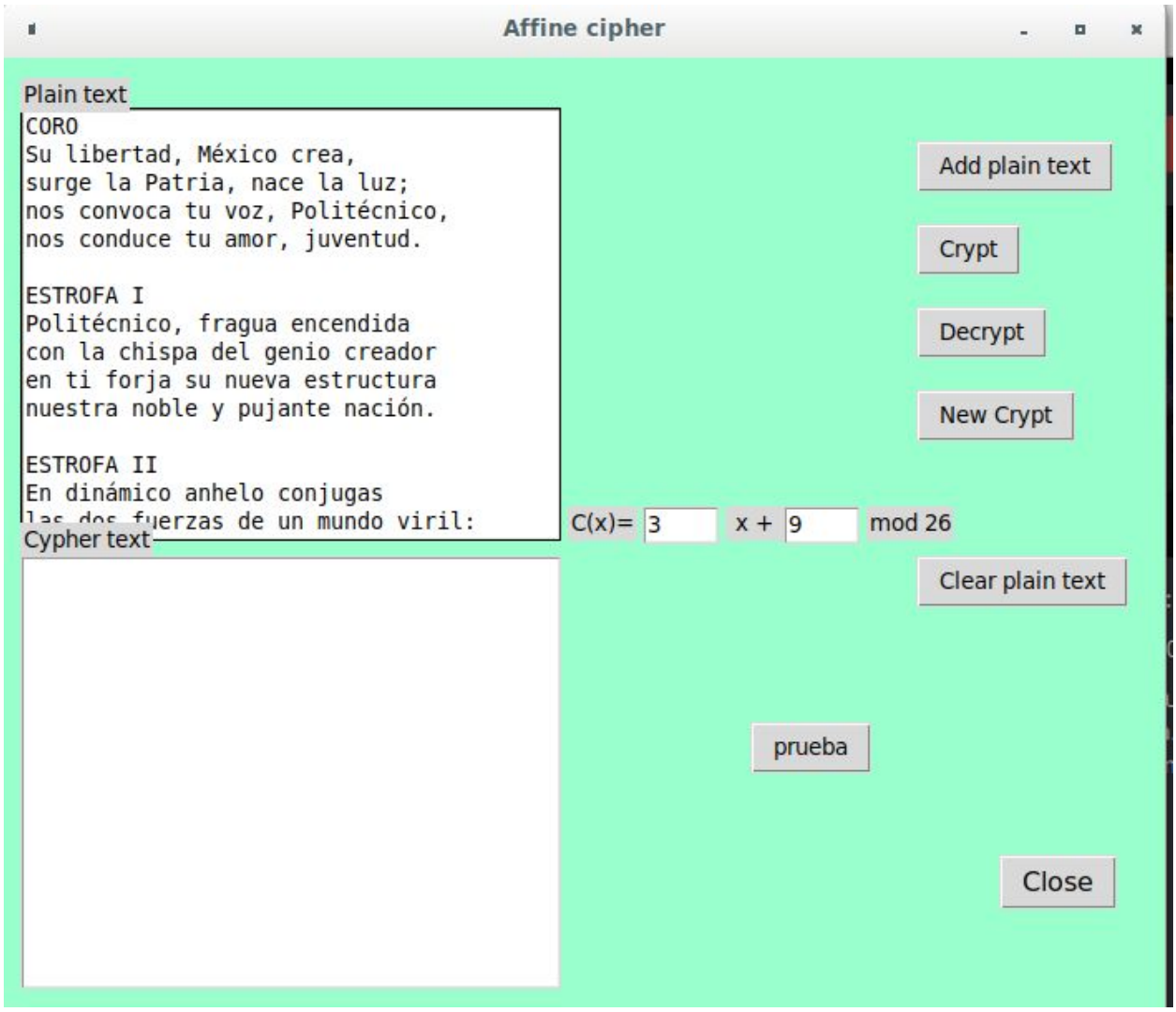
- Add plain text: Open a file browser to search the a file.
- Crypt: Process the plaintext previously upload with the cipher affine.
- Decrypt: Process the encrypted text became in the original plain text.
- New Crypt: Clear both text areas.
- Clear Plain Text: Clear only the text area.
- Close: Close the app.

Results (encrypt).

We load the file to encrypt.



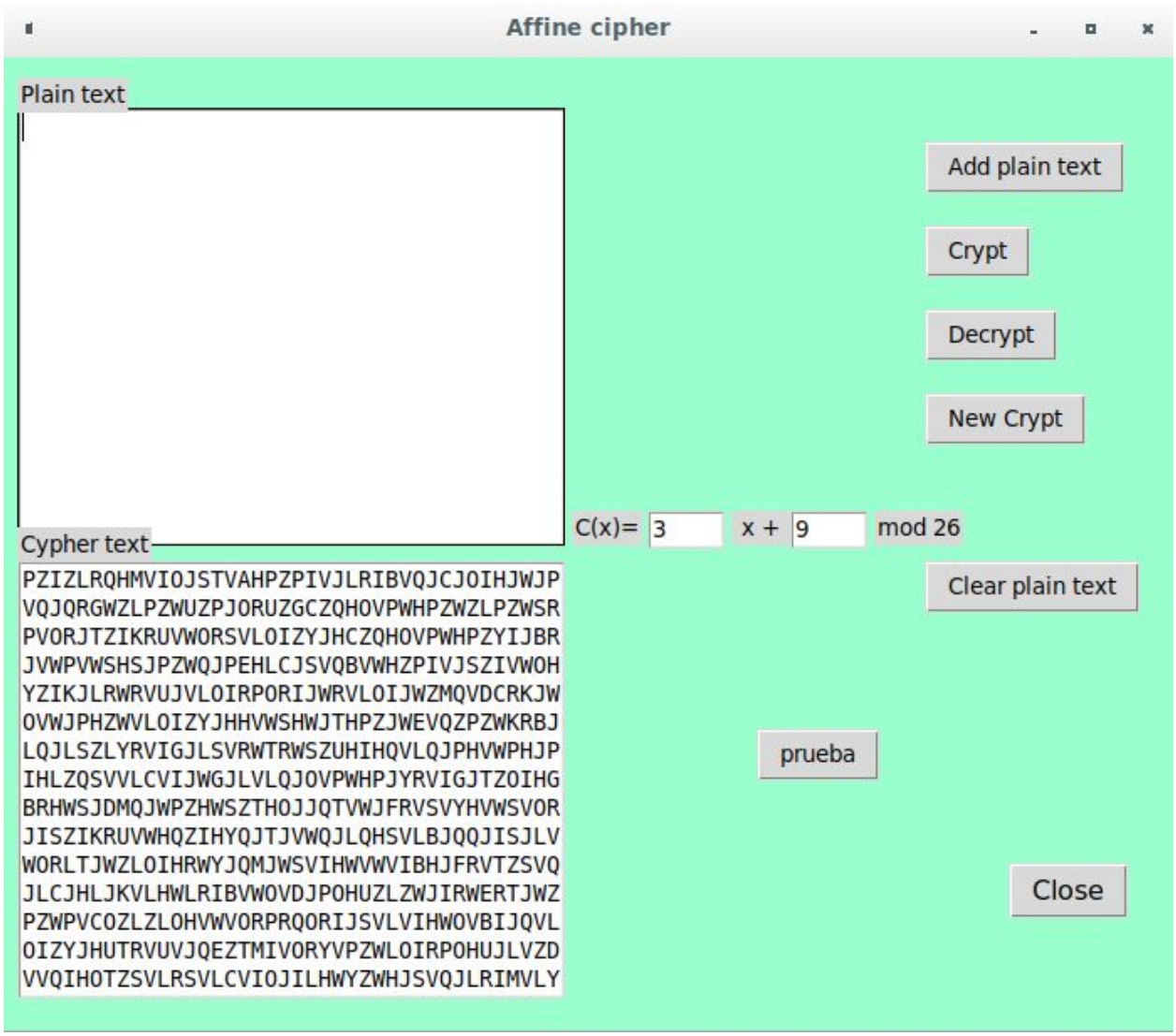
We enter the values of alpha and betha.



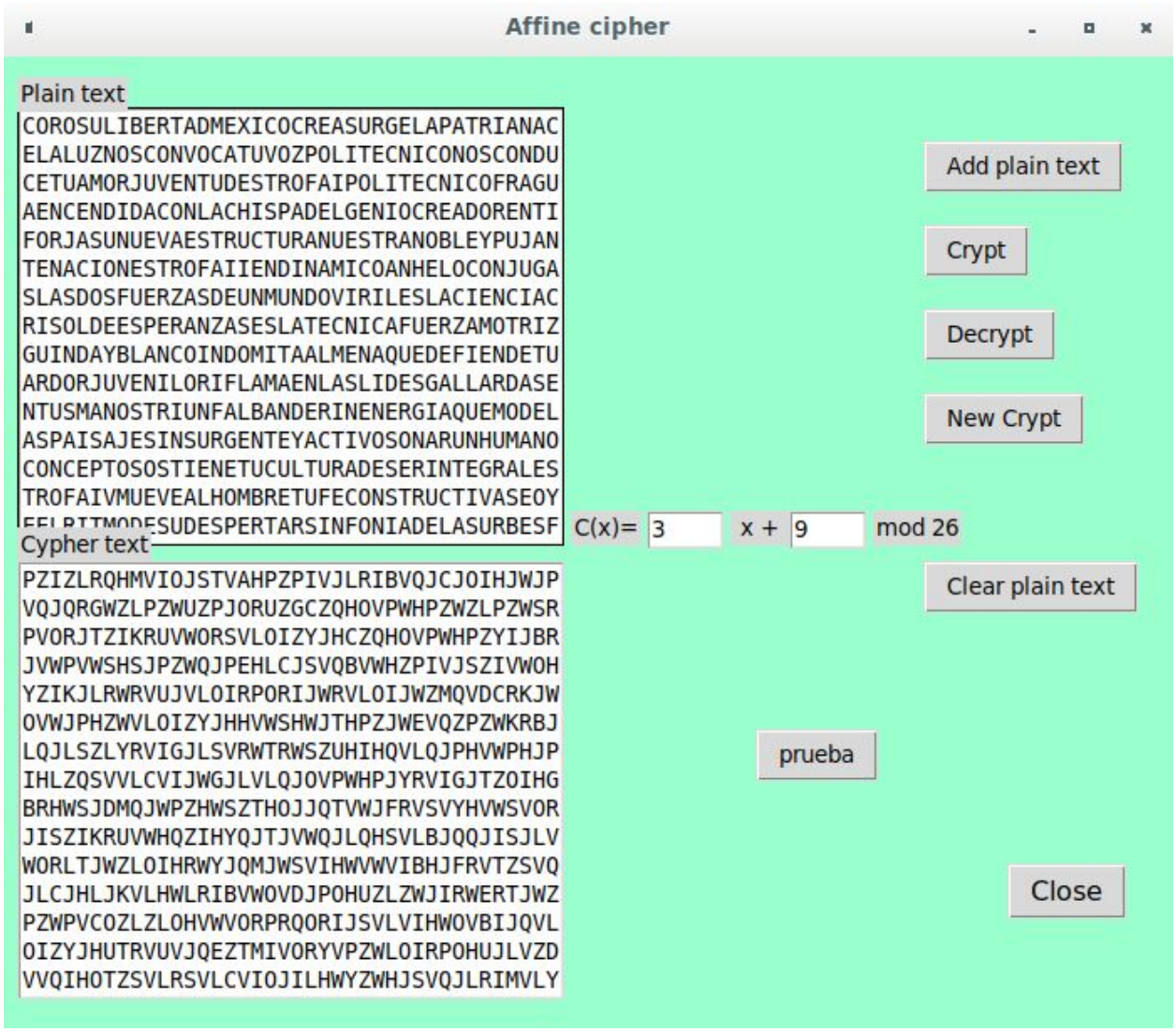
After we press the button crypt and the result is showed at the second test area.

Results (decrypt).

To decrypt first we must to clear the text area of the plain text.



We press the button decrypt, the application catch the encrypted text and process it to obtain the original plain text, buth in this case with capital letters.



To finalize we press the button close.

Important functions.

```
def decryptText(encryptedText):
     inverse=int(f.inverse( int(alfa.get()),26 ))
     be=int(beta.get())


     alfabeto=['A','B','C','D','E','F','G','H','I','J','K','L','M','N',
     'O','P','Q','R','S','T','U','V','W','X','Y','Z']
     list2=[]
     for i in encryptedText:
          if i=='\n':
               list2.append('\n')
          else:
               position=alfabeto.index(i)
               aux=inverse*(position-be)
               newPosition=aux%26
               list2.append(alfabeto[newPosition])

     #list2.pop()
     salida=''.join(list2)
     return salida
```

```

def encryptText(plaintext):


    alfabeto=['A','B','C','D','E','F','G','H','I','J','K','L','M','N',
    'O','P','Q','R','S','T','U','V','W','X','Y','Z']
    list2=[]
    for i in plaintext:

        if i=='\n':
            list2.append('\n')

        else:
            actualPosition=alfabeto.index(i)

            al=int(alfa.get())
            be=int(beta.get())
            aux=(al*actualPosition)+be
            newPosition=aux%26
            list2.append(alfabeto[newPosition])

    salida=''.join(list2)



    return salida
```

Conclusions.

The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which.

The whole process relies on working modulo m (the length of the alphabet used). In the affine cipher, the letters of an alphabet of size m are first mapped to the integers in the range 0 … m-1.

The 'key' for the Affine cipher consists of 2 numbers, we'll call them a and b. The following discussion assumes the use of a 26 character alphabet (m = 26). a should be chosen to be relatively prime to m (i.e. a should have no factors in common with m).

í tu texto Escribe aquí tu texto Escribe aquí tu texto Escribe aquí tu texto Escribe aquí tu texto Escribe aquí tu texto.