

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.

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

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

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

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

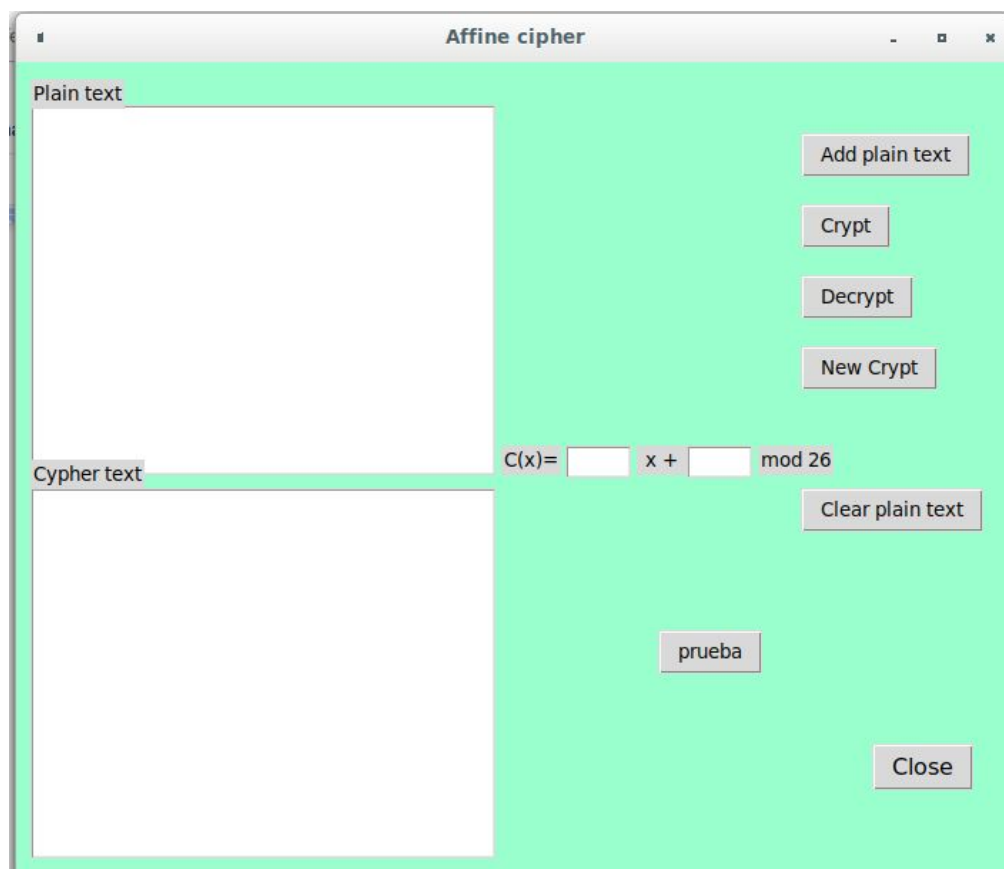
Software.

Python 2.7.15rc1

Tkinter (GUIs python)

Procedure.

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



Inputs:

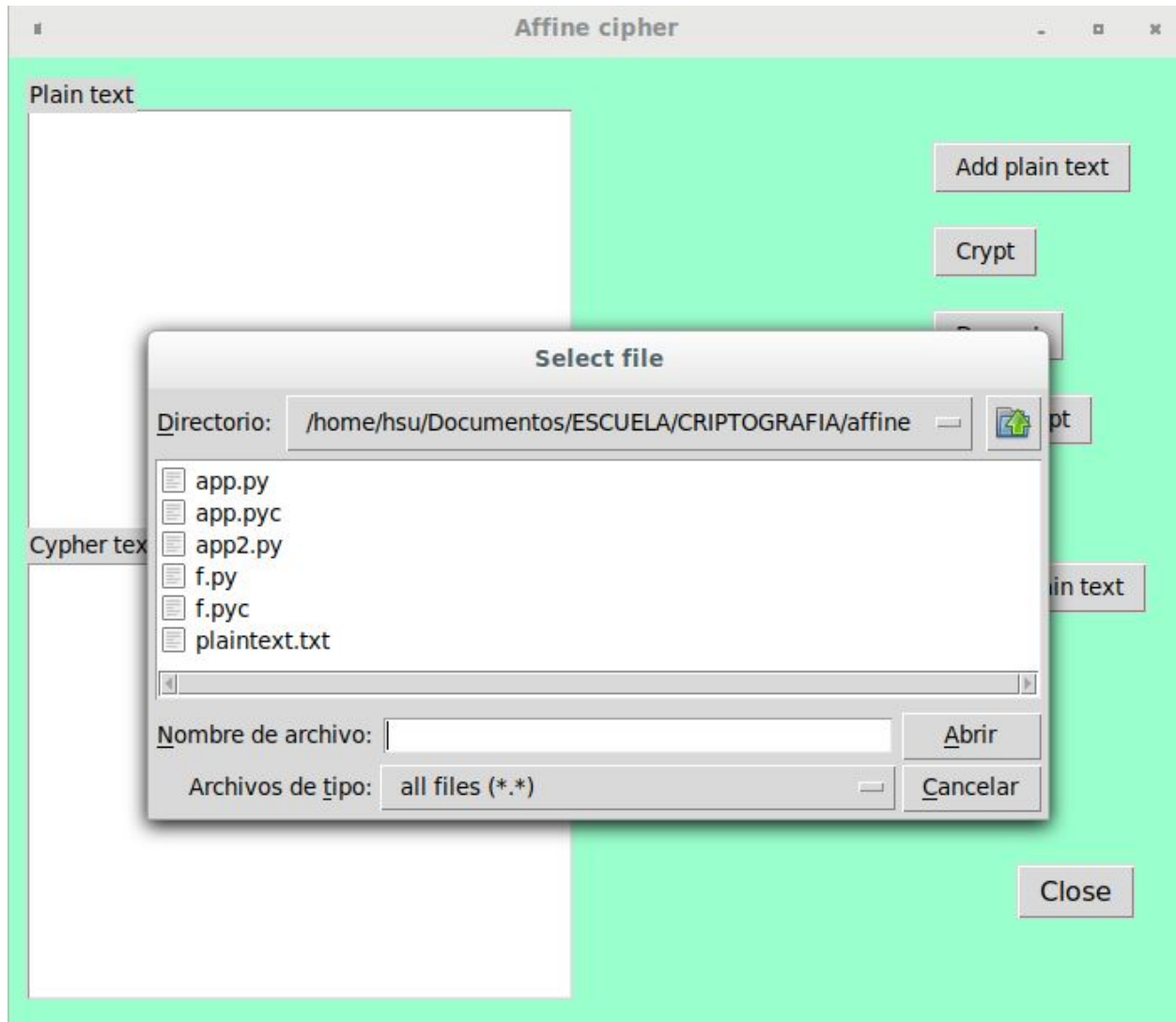
- TextArea1: Text Area to upload the plain text.
- TextArea2: Text Area to show the plaintext encrypted.

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.

Affine cipher

Plain text

CORO
Su libertad, México crea,
surge la Patria, nace la luz;
nos convoca tu voz, Politécnico,
nos conduce tu amor, juventud.

ESTROFA I
Politécnico, fragua encendida
con la chispa del genio creador
en ti forja su nueva estructura
nuestra noble y pujante nación.

ESTROFA II
En dinámico anhelo conjugas
las dos fuerzas de un mundo viril:

Cypher text

Add plain text

Crypt

Decrypt

New Crypt

$C(x) = 3x + 9 \mod 26$

Clear plain text

prueba

Close

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

Affine cipher

Plain text

CORO

Su libertad, México crea,
surge la Patria, nace la luz;
nos convoca tu voz, Politécnico,
nos conduce tu amor, juventud.

ESTROFA I

Politécnico, fragua encendida
con la chispa del genio creador
en ti forja su nueva estructura
nuestra noble y pujante nación.

ESTROFA II

En dinámico anhelo conjugas
las dos fuerzas de un mundo viril:

Cyphertext

PZIZLRQHMVIOJSTVAHPZPIVJLRIBVQJCJOIHJWJP
VQJQRGWZLPZWUZPJORUZGCZQHVPWHPZWZLPZWSR
PVORJTZIKRUVWORSVLOIZYJHCZQHVPWHPZYIJBR
JVWPVWSHSJPZWQJPEHLCJSVQBWHZPIVJSZIVWOH
YZIKJLRWRVUJVLQIRPORIJWRVLOIJWZMQVDCRKJW
OVWJPHZWVLOIZYJHHVWSHWJTHPZJWEVQZPZWKRBJ
LQJLSZLYRVIGJLSVRWTRWSZUHIHQVLQJPHVWPHJP
IHLZQSVVLCVIJWGJLVQJOVPWHPJYRVIGJTZOIHG
BRHWSJDMQJWPZHWSZTHOJJQTVWJFRVSVYHVWSVOR
JISZIKRUVWHQZIHQJTTJVWQJLQHSVLBJQQJISJLV
WORLTJWZLOIHRWYJQMJSVVIHVVVIBHJFRVTZSVQ
JLCJHLJKVLHWRIBVWOVDJPOHUZLZWJIRWERTJWZ
PZWPVCOZLZLOHVWVORPRQORIJSVLVIHWOVBIJQVL
OIZYJHUTRVUVJQEZTMIVORYVPZWLOIRPOHUJLVZD
VVQIHOTZSVLRSVLCVIOJILHWYZWHJSVQJLRIMVLY

Add plain text

Crypt

Decrypt

New Crypt

C(x)=

3

x +

9

mod 26

Clear plain text

prueba

Close

Results (decrypt).

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

Affine cipher

Plain text

Cypher text

Add plain text

Crypt

Decrypt

New Crypt

$C(x) = 3x + 9 \pmod{26}$

Clear plain text

prueba

Close

PZIZLRQHMVIOJSTVAHPZPIVJLRIBVQJCJOIHJWJP
 VQJQRGWZLPZWUZPJORUZGCZQH0VPWHPZWZLPZWSR
 PVORJTZIKRUVWORSVLOIZYJHCZQH0VPWHPZYIJBR
 JVWPVWSHJJPZWQJPEHLCJSVQBWHZPIVJSZIVWOH
 YZIKJLRWRVUJVLOIRPORIJWRVLOIJWZMQVDCRKJW
 OVWJPHZWVLOIZYJHHVWSHWJTHPZJWEVQZPZWKRBJ
 LQJLSZLYRVIGJLSVRWTRWSZUHIHQVLQJPHVWPHJP
 IHLZQSVVLCVIJWGJLVLQJOVPWHPJYRVIGJTZOIHG
 BRHWSJDMQJWPZHWSZTHOJJQTVWJFRVSVYHVWSVOR
 JISZIKRUVWHQZIHQJTTJWVQJLQHSVLBJQQJISJLV
 WORLTJWZLOIHRWYJQMJWSVIHVVWVIBHJFRVTZSVQ
 JLCJHLJKVLHWRIBVWVDJPOHUZLZWJIRWERTJWZ
 PZWVPCOZLZLOHVWVORPRQORIJSVLVIHWVBIJQVL
 OIZYJHUTRVUVJQEZTMIVORYVPZWLOIRPOHUJLVZD
 VVQIHOTZSVLRSVLCVIOJILHWYZWHJSVQJLRIMVLY

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

Affine cipher

Plain text

COROSULIBERTADMEXICOCREASURGELAPATRIANAC
ELALUZNOSCONVOCATUVOZPOLITECNICONOSCONDU
CETUAMORJUVENTUDESTROFAIPOLITECNICOFragu
AENCENDIDAONLACHISPAPDELGENIOCREADORENTI
FORJASUNUEVAESTRUCTURANUESTRA NOBLEYPUJAN
TENACIONESTROFAIENDINAMICOANHELOCONJUGA
SLASDOSFUERZASDEUNMUNDOVIRILESLACIENCIAC
RISOLDEESPERANZASESLATECNICAFUERZAMOTRIZ
GUINDAYBLANCOINDOMITAALMENAQUEDEFIENDETU
ARDORJUVENILORIFLAMAENLASLIDESGALLARDA
NTUSMANOSTRIUNFALBANDERINENERGIAQUEMODEL
ASPAISAJESINSURGENTEYACTIVOSONARUNHUMANO
CONCEPTOSOSTIENETUCULTURADESERINTEGRALES
TROFAIVMUEVEALHOMBRETUFECONSTRUCTIVASEOY
EEI RITMODESUDESPERTARSINFONIADELASURBESF

Cypher text

PZIZLRQHMVIOJSTVAHPZPIVJLRIBVQJCJOIHJWJP
VQJQRGWZLPZWUZPJORUZGCZQHOPWHPZWZLPZWSR
PVORJTZIKRUVWORSVLOIZYJHCZQHOPWHPZYIJBR
JVVPVWSHSPZWQJPEHLCJSVQBWHZPIVJSZIVWOH
YZIKJLRWRVUJVLOIRPORIJWRVLOIJWZMQVDCRKJW
OVWJPHZWVLOIZYJHHVWSHWJTHPZJWEVQZPZWKRBJ
LQJLSZLYRVIGJLSVRWTRWSZUHIHQVLQJPHVWPHJP
IHLZQSVVLCVIJWGJLVQJOVPWHPJYRVIGJTZOIHG
BRHWSJDMQJWPZHWSZTHOJJQTVWJFRVSVYHVWSVOR
JISZIKRUVWHQZIHVQJTVWQJLQHSVLBJQQJISJLV
WORLTJWZLOIHRWYJQMJSVVIHVVWVIBHJFRVTZSVQ
JLCJHLJKVLHWRIBVWOVDJPOHUZLZWJIRWERTJWZ
PZWPVCOZLZLOHVWVORPRQORIJSVLVIHWOVBIJQVL
OIZYJHUTRVUVJQEZTMIVORYVPZWLOIRPOHUJLVZD
VVQIHOTZSVLRSVLCVIOJILHWYZWHJSVQJLRIMVLY

Add plain text

Crypt

Decrypt

New Crypt

C(x) = 3 * x + 9 mod 26

Clear plain text

prueba

Close

To finalize we press the button close.

Important functions.

```

81 def decryptText(encryptedText):
82     inverse=int(f.inverse( int(alfa.get()),26 ))
83     be=int(beta.get())
84
85
86     alfabeto=['A','B','C','D','E','F','G','H','I','J','K','L','M','N',
87             'O','P','Q','R','S','T','U','V','W','X','Y','Z']
88     list2=[]
89     for i in encryptedText:
90         if i=='\n':
91             list2.append('\n')
92         else:
93             position=alfabeto.index(i)
94             aux=inverse*(position-be)
95             newPosition=aux%26
96             list2.append(alfabeto[newPosition])
97
98     #list2.pop()
99     salida=''.join(list2)
100     return salida
101

```

```

43
44 def encryptText(plaintext):
45
46
47     alfabeto=['A','B','C','D','E','F','G','H','I','J','K','L','M','N',
48             'O','P','Q','R','S','T','U','V','W','X','Y','Z']
49     list2=[]
50     for i in plaintext:
51
52         if i=='\n':
53             list2.append('\n')
54
55         else:
56             actualPosition=alfabeto.index(i)
57
58             al=int(alfa.get())
59             be=int(beta.get())
60             aux=(al*actualPosition)+be
61             newPosition=aux%26
62             list2.append(alfabeto[newPosition])
63
64     salida=''.join(list2)
65
66
67
68     return salida
69

```

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 $0 \dots m-1$.

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.