ΚΡΥΠΤΟΓΡΑΦΙΑ. DAI16067. ΑΣΚΗΣΗ 2

1. Κάθε μηχάνημα κοστίζει 10^6/100=10.000 κυκλώματα (100% επιβάρυνση άρα 100 ευρώ για κάθε κύκλωμα). Οπότε η ταχύτητα του παράλληλου συστήματος μας είναι 5*10^8*10^4=5*10^12 keys/second. Συνήθως βρίσκουμε το σωστό κλειδί στην μέση περίπτωση δηλαδή 2^127. Οπότε θα βρούμε το κλειδί στην μέση περίπτωση με αυτόν τον τρόπο: 2^127keys/5*10^12 keys/second= 3.4*10^25 seconds /(60 * 60* 24*365)= 1.08 * 10^18 χρονιά άρα 10^8 φορές μεγαλύτερο από την ηλικία του σύμπαντος.

2. Έστω i τα iterations του Moore's law οπότε έχουμε την εξής σχέση:

   1.08*10^18 χρονιά * (365/2^i) =1 day =>2^i=1.08*10^18 years *365 days οπότε

   i=68,42 περίπου 69 άρα 1,5 χρονιά * 69 iterations =103.5 χρονιά.

In [16]:
```
# A τρόπος με a,b ακεραίους
message = 'UNIVERSITY';


Z26 = IntegerModRing(26)
a=Z26(11)
b=Z26(4)



def str2lst(s):
    return [ord(x)-65 for x in s]

def lst2str(lst):

    return ''.join([chr(x+65) for x in lst])


def affine_enc(m,k1,k2):
 plaintextList = str2lst(m)

 ciphertextList = [(k1*x+k2) for x in plaintextList]
 n=1
 m=2
 if m == n:
    print m


 r=[];
 for md in range(len(ciphertextList)):
   for pico in range(27):
    if pico == ciphertextList[md]:
        r.append(pico)


 ciphertext = lst2str(r)


 return ciphertext


print("The plaintext message: " + message + " becomes --> " + affine_enc(message,a,b))
```

```
The plaintext message: UNIVERSITY becomes --> QROBWJUOFI
```

n [20]:
```
# A τρόπος με a, b ακεραίους
ciphertext='QROBWJUOFI'
Z26= IntegerModRing(26)
t=Z26(11)
r=Z26(4)


def affine_dec(c,k1,k2):
    k1=k1.inverse_of_unit()

    ciphertextList = str2lst(c)
    plaintextList = [(k1*(x-k2)) for x in ciphertextList]

    r=[];
    for md in range(len(plaintextList)):
     for pico in range(27):
      if pico == plaintextList[md]:
        r.append(pico)

    plaintext = lst2str(r)

    return plaintext

print("The ciphertext message: " + ciphertext + " becomes --> " + affine_dec(ciphertext,t,r))
```

```
The ciphertext message: QROBWJUOFI becomes --> UNIVERSITY
```

Στον κώδικα στην 1η εικόνα δηλαδή στην κρυπτογράφηση , όρισα τα α και β στο Z26 οπότε και κάνουν αυτόματα mod όταν βγαίνουν εκτός ορίων και έτσι η λίστα ciphertextList δεν χρειάζεται πλέον το %26 που είχε μέσα, το πρόβλημα ήταν ότι επειδή είναι τύπου Integermodring και όχι απλό integer η συνάρτηση μου επέστρεφε άσπρα κουτάκια αντί για το κρυπτοκειμενο, οπότε με την σειριακή αναζήτηση ανίχνευσα τα ίδια νούμερα με τον λίστα και έθεσα σε μια 2η λίστα το pointer όταν αυτός θα είναι ίσος με τη λίστα (άρα απλό integer), αυτή τη λίστα την στέλνω μετα για το τη συνάρτηση lst2str και επιστρέφεται σαν κείμενο κανονικά . με την ίδια λογική έκανα και το decryption 2η εικόνα απλά στο inversion του κ1 χρησιμοποίησα μια άλλη συνάρτηση της python και όχι αυτή που δίνονταν.