Άσκηση 5 Dai16067 Κρυπτογραφία

In [34]:
```
def str2lst(s):
    return [ord(x) for x in s]

def lst2str(lst):
    return ''.join([chr(x) for x in lst])



p=2621
e=7
plaintext="SWEETDREAMS"
plaintext2=str2lst(plaintext)


X=[x%p for x in plaintext2]
X2=[power_mod(x,e,p) for x in X]

print X
print "The puclic information is ", X2


R=[x for x in range(1,p+1) if gcd(x,p)==1]
phi_n=len(R)
print "Φ(p)=Φ(2621)=",phi_n

d=inverse_mod(e,phi_n)
print "d = ",d

print (e*d)%phi_n == 1

print "The public key is the modulus: ", p, "and the public exponent:", e
print "The private key is:", d

X3=[power_mod(x,d,p) for x in X2]
print X3
print "The encrypted text is " ,lst2str(X3)
```

```
[83, 87, 69, 69, 84, 68, 82, 69, 65, 77, 83]
The puclic information is  [886, 670, 1252, 1252, 1329, 2392, 2496, 1252, 1618, 1417, 886]
Φ(p)=Φ(2621)= 2620
d =  1123
True
The public key is the modulus:  2621 and the public exponent: 7
The private key is: 1123
[83, 87, 69, 69, 84, 68, 82, 69, 65, 77, 83]
The encrypted text is  SWEETDREAMS
```

Στο 1ο ερώτημα μετατρέπουμε το κείμενο σε αριθμούς μετα το κάνουμε encryption υπολογίζουμε το R για να βρούμε το φ(ν) και για να βρούμε ύστερα το d υπολογίζουμε την σχέση μας ότι ισχύει το

e*d%φ(v) ==1 και τελικά με το X3 κάνουμε το τελικό decryption για να βρούμε πάλι τους αρχικούς αριθμούς και να το μετατρέψουμε σε γράμματα.

```
In [5]: def str2lst(lst):
            return ''.join([chr(x+65) for x in lst])
        p=29
        #p1=

        X2=[4,19,19,11,4,24,9,15,15]
        flag=False;

        #from fractions import gcd
        #print reduce(gcd, [p1])

        print "The puclic information is ", X2

        R=[x for x in range(1,p+1) if gcd(x,p)==1]
        phi_n=len(R)
        print "Φ(p)=Φ(2621)=",phi_n
        print chr(65+25)
        Z26=IntegerModRing(26)
        while True:
            try:
                e = ZZ.random_element(1,p-1)
                d=inverse_mod(e,phi_n)

                X3=[power_mod(x,d,p) for x in X2]


                if(X3[5]==20):
                    if(all(i < 26 for i in X3)):
                        break;

            except ZeroDivisionError:
                flag=False

        print "d = ",d
        print (e*d)%phi_n == 1
        print "The public key is the modulus: ", p, "and the public exponent:", e
        print "The private key is:", d
        X3=[power_mod(x,d,p) for x in X2]
        print X3
        print "The encrypted text is " ,str2lst(X3)

        The puclic information is  [4, 19, 19, 11, 4, 24, 9, 15, 15]
        Φ(p)=Φ(2621)= 28
        Z
        d =  17
        True
        The public key is the modulus:  29 and the public exponent: 5
        The private key is: 17
        [6, 14, 14, 3, 6, 20, 4, 18, 18]
        The encrypted text is  GOODGUESS
```

Στο 2ο ερώτημα έγραψα ουσιαστικά μέσα σε μια ατέρμονη while την αναζήτηση του e και του d, η συνθήκη για να σταματήσουν είναι πρώτα από όλα το 5ο γράμμα να είναι το U στο decryption και όλα τα νούμερα

να είναι μικρότερα του 26 καθώς παίρνουμε τιμές από 0 έως 25, η λύση είναι πάντα ίδια και το κείμενο που είχε κρυπτογραφηθεί είναι το GOODGUESS.

In [119]:

```
def lst2num(lst):
    number=[]
    for i in range(len(lst)):
        number.append(lst[i]//100)
        number.append(lst[i]%100)


    return number
def lst2str2(lst):
    return ''.join([chr(x+65) for x in lst])

p=2591

X2=[1213, 902 ,539 ,1208 ,1234, 1103, 1374]
R=[x for x in range(1,p+1) if gcd(x,p)==1]
phi_n=len(R)
print "Φ(p)=Φ(2621)=",phi_n
while True:
    try:
        e=ZZ.random_element(1,p-1)
        d=inverse_mod(e,phi_n)
        X3=[power_mod(x,d,p) for x in X2]
        if(X3[1]==1314):
            X4=lst2num(X3)
            if(all(i < 26 for i in X4)):
                break;
    except ZeroDivisionError:
        q=1; #do smthing

print X
print "The puclic information is ", X2

print "Φ(p)=Φ(2621)=",phi_n

d=inverse_mod(e,phi_n)
print "d = ",d

print (e*d)%phi_n == 1

print "The public key is the modulus: ", p, "and the public exponent:", e
print "The private key is:", d



print X3
print X4
print  lst2str2(X4)
```

```
Φ(p)=Φ(2621)= 2590
[1213, 902, 539, 1208, 1234, 1103, 1374]
The puclic information is  [1213, 902, 539, 1208, 1234, 1103, 1374]
Φ(p)=Φ(2621)= 2590
d =  797
True
The public key is the modulus:  2591 and the public exponent: 13
The private key is: 797
[314, 1314, 1917, 400, 319, 708, 1823]
[3, 14, 13, 14, 19, 17, 4, 0, 3, 19, 7, 8, 18, 23]
DONOTREADTHISX
```

Το κόλπο στο 3ο ερώτημα είναι και αυτό μέσα στην while όπου τον τετραψήφιο αριθμό τον κάνω διψήφιο και με αυτόν τον τρόπο βρίσκω τα γράμματα με τον ASCII