Category:

Cryptography

Name:

Small RSA

Message:

```
from Crypto.Util.number import getPrime
flag="FALG*****************************"
c=""
p=getPrime(12)
q=getPrime(12)
N=p*q
E=65537
for l in flag:
        c+=format(pow(ord(l),E,N), '08X')
print(c)
```

```
>
0015A15A001D7AEA000F663A001A1CFB00127B2D000353B800135A9B001D7AEA00212E6E0015A
15A00064786001D57D6001D7AEA00150F64001A1CFB001D7AEA001D57D60018005E0013EDF200
10858D0015A15A000823E20011654D001D57D6001D7AEA00135A9B002137060011654D0021370
600150F640015A15A000353B8001D7AEA00213706000823E200064786001A1CFB00127B2D0017C
EF80015A15A00150F6400213706001A1CFB000823E2
```

Objective:

Decrypt text.

```
0015A15A001D7AEA000F663A001A1CFB00127B2D000353B800135A9B001D7AEA00212E6E0015A
15A00064786001D57D6001D7AEA00150F64001A1CFB001D7AEA001D57D60018005E0013EDF200
10858D0015A15A000823E20011654D001D57D6001D7AEA00135A9B002137060011654D0021370
600150F640015A15A000353B8001D7AEA00213706000823E200064786001A1CFB00127B2D0017C
EF80015A15A00150F6400213706001A1CFB000823E2
```

Instructions:

The text is encrypted with a key of primary number smaller than 4096.

Hence should not be hard to brute force this. Only 564 prime numbers 318,096 combinations to be calculated!!

Reference:

```
-   L=math.lcm(p-1, q-1)
```

```
-   for D in range(2,L):
-       if (65537*D)%L==1:
-           break
```