CE340 –HW1

Serdar Haliloğlu

26.10.2015

Contents

```
s = random_prime(2^512)
r = random_prime(2^512)

n = s * r

phi = (s-1) * (r - 1)

e = ZZ.random_element(phi)

while gcd(e,phi) != 1:
 e= ZZ.random_element(phi)

bezout = xgcd(e,phi)

d = Integer(mod(bezout[1],phi))

#mod(d*e,phi)

PublicKey = (e,n)

PrivateKey = (d,n)

#PublicKey; PrivateKey;

myFile = open("MyPlainText.txt")

read_data = myFile.read()

read_data.encode("utf-8")

myFile.close()

read_data = map(ord,read_data)

read_data = ZZ(list(reversed(read_data)),100)


Cip = power_mod(read_data,e,n)
```

```
power_mod(Cip,d,n)

power_mod(Cip,d,n,) == read_data

Cip = str(Cip)
file = open("encryptedFile.txt", 'w')

file.write(Cip)

file.close()

file = open("encryptedFile.txt" ,'r')
```

```
'Plain Text RSA Algorithm Example'
8108980610328502211632828365326609041215061705093270209810130901
True
```