cap_sage_rsa

```
def digit(string):
    return map(lambda x: ord(x), string)
```

```
def letters(num_list):
    return ''.join(chr(i) for i in num_list)
```

```
def rsa_encrypt(message,key):
    message = digit(message)
    cipher = []
    for mess in message:
        cipher.append(power_mod(mess,key[0],key[1]))
    #cipher = list_to_ascii(cipher)
    return cipher

def rsa_decrypt(cipher,key):
    #cipher = digit(cipher)
    plain = []
    for ciph in cipher:
        plain.append(power_mod(ciph,key[0],key[1]))
    print plain
    #plain = list_to_ascii(plain)
    return letters(plain)
```

```
def init_rsa():
    #random primes for the modulus
    p = ZZ.random_element(10**100,10**101); p = next_prime(p)
    q = ZZ.random_element(10**100,10**101); q = next_prime(q)
    m = q*p
    #euler phi
    phi = (p-1)*(q-1)
    # choosing e
    e = phi
    while not gcd(phi,e) == 1:
        e = next_prime(ZZ.random_element(10**100,10**101))%m
    d = power_mod(e,-1,phi)
    print d*e%phi
    return [[d,m],[e,m]]
```

```
priv_key,pub_key = init_rsa()
```

```
1
```

```
priv_key
```

```
[156158695177945444786452394035114873441185749806520708816924
532093418680191416514738180759196179197442351263690171058495 2
713755080232823646295601699535510554656713914812434342999260 8
336885206426104159756383608106718732468380057780743689380715 3
979891981109646337652266566522159957070979375339179152309399 9
127027876277460878920011267776909939633355292625427635076388 7
```

```
pub_key
```

```
[114507250259023443834187889238705322692546030103981053449923
564149283479013527629778801310526 1,
336885206426104159756383608106718732468380057780743689380715 3
979891981109646337652266566522159957070979375339179152309399 9
127027876277460878920011267776909939633355292625427635076388 7
```

```
message = 'Dies ist meine Nachricht!'
```

```
cipher_text = rsa_encrypt(message,pub_key)
print cipher_text
plain_text = rsa_decrypt(cipher_text,priv_key)
print plain_text
```

```
[862520770413612543980527933573032738609192354051667870211312
192605984415047139777373956379871617380494728277073066681937 4
964315215067587404759586983115175806751634234161998240096022 1
155919203733077872213410926534900307013868840500446539360389 5
307339510613624340791349504760696131798968406437487679996787 1
186369402184200331059613407584730388739018205102534916858555 6
364938773695482599186803227081594764070346327466294929610153 4
146114016834999029592121545394437535476274746972470184919446 7
753902570958535605008326213285036797596355280923102539724113 7
260973559358723002234452825729488566847102744847401623379307 9
792395205625996010943099325231718254330672211332688778767370 2
447875140159591886953233940346490096533616533351727016474960 1
120172634390636803334656015615444625005952845230516044419776 0
822815123732736087339979824063430735826644604533213257143792 3
223463131012248129517477178387585942972276528142463695254446 0
155919203733077872213410926534900307013868840500446539360389 5
307339510613624340791349504760696131798968406437487679996787 1
186369402184200331059613407584730388739018205102534916858555 6
260973559358723002234452825729488566847102744847401623379307 9
792395205625996010943099325231718254330672211332688778767370 2
447875140159591886953233940346490096533616533351727016474960 1
913388086057926071812534272449328620892233076276282641481255
767703529569059792110368189895049488021698248475729746323964 0
436171275158477533631750445023668249945566844122572317043791 9
120172634390636803334656015615444625005952845230516044419776 0
822815123732736087339979824063430735826644604533213257143792 3
223463131012248129517477178387585942972276528142463695254446 0
163443300619032504512127262707036772302499614987391758078906 3
```

```
456737747640962149825828083175919331933211780439950119997555644565409888261440520730763692913127862479261066029226449722736493877369548259918680322708159476407034632746629492961015341461140168349990295921215453944375354762747469724701849194467753902570958535605008326213285036797596355280923102539724113715591920373307787221341092653490030701386884050044653936038953073395106136243407913495047606961317989684064374876799967871186369402184200331059613407584730388739018205102534916858555618839354173754662727893277893911896612422090620366467079936524905950595275306835715854958144989082027476157662502039890940554184245079861446210472643847185969812910123437801896991620536493877369548259918680322708159476407034632746629492961015341461140168349990295921215453944375354762747469724701849194467753902570958535605008326213285036797596355280923102539724113712017263439063680333465601561544462500595284523051604441977608228151237327360873399798240634307358266446045332132571437923223463131012248129517477178387585942972276528142463695254446024886786634139367791941926878569392792582326270736288368610173113744146048821443252638130380737999928894527682556111827939990445706130965722884612478607823041306133200095066069958751463699672441250639446368874249855329754447618863808875762005740264355626205999210038129242881937765306226069973484903338530184643677392920930288577207470201294599464383732664045685542675922171270463248292933784779748345493454639114351310096098474432045143338779236802671314420298151670709582269830991702691993097987300289060527668637225158367223503931078117981776835692980495274209700398421008067057810979083272563284367818547014637901521542331725271196574768034684516005799391115783773801463790152154233172527119657476803468451600579939111578377380150679912742986404341148671090431792223912991281861224268247585801272388100107701295050515517796936067422652892789453467227997290825783730412441578528545713796122152996080479761391947587248995562027039043763892015923094418482853456668607201916155919203733077872213410926534900307013868840500446539360389530733951061362434079134950476069613179896840643748767999678711863694021842003310596134075847303887390182051025349168585556267592217127046324829293378477974834549345463911435131009609847443204514333877923680267131442029815167070958226983099170269199309798730028906052766863722515836722350393107811798177683569298049527420970039842100806705781097908327256328436781854701463790152154233172527119657476803468451600579939111578377380150679912742986404341148671090431792223912991281861224268247913388086057926071812534272444932862089223307627628264148125558476770352956905979211036818989504948802169824847572974632396404361712751584775336317504450236682499455668441225723170437919331049631079946335385057160540326482189701952407539490838029106510993988920282259994382143258168394327303905007878418526193594341382629841267311594025485766988790063887953546565609094[68, 105, 101, 115, 32, 105, 115, 116, 32, 109, 101, 105, 11032, 78, 97, 99, 104, 114, 105, 99, 104, 116, 33]
```

```
Dies ist meine Nachricht!
```