RSA-Demonstration

Einige wichtige Sage-Funktionen für das Rechnen in Restklassen:

- Grösster gemeinsamer Teiler: **gcd**
- Erweiterter Euklidscher Algorithmus: **xgcd**
- Chinesischer Restsatz: **CRT_list**
- Eulersche Phi-Funktion: **euler_phi**
- Rechnen in $\mathbf{Z}_m$: **Mod**, oder **Zmod**
- Lösen von Gleichungen, oder Gleichungssystemen in $\mathbf{Z}_m$: **solve_mod**
- Primzahlen: **is_prime**, **next_prime**, **random_prime**, ...
- Primfaktorzerlegung: **factor**

```
def encode_str(s):
   length = 20
   c = 0
   c_list = []
   if len(s) % length != 0:
       s += (len(s) % length) * " "
   index = Mod(0, length)
   for i in range(len(s)):
       c *= 256
       c += ord(s[i])
       index += 1
       if index == 0:
           c_list.append(c)
           c = 0
   return c_list
```

```
def decode_str(c_list):
   s_list = []
   for c in c_list:
       temp = []
       while c != 0:
           c, r = ZZ(c).quo_rem(256)
           temp.append(chr(r))
       s_list += reversed(temp)
   return reduce(lambda x,y: x+y, s_list)
```

```
text = """In cryptography, RSA is an algorithm for public-key
cryptography. It is the first algorithm known to be suitable for
```

```
signing as well as encryption, and one of the first great advances
in public key cryptography. RSA is widely used in electronic
commerce protocols, and is believed to be secure given sufficiently
long keys and the use of up-to-date implementations. The algorithm
was publicly described in 1977 by Ron Rivest, Adi Shamir, and
Leonard Adleman at MIT, the letters RSA are the initials of their
surnames, listed in the same order as on the paper.
"""
```

```
print text
```

```
"In cryptography, RSA is an algorithm for public-key cryptography.
It is the first algorithm known to be suitable for signing as well
as encryption, and one of the first great advances in public key
cryptography. RSA is widely used in electronic commerce protocols,
and is believed to be secure given sufficiently long keys and the
use of up-to-date implementations. The algorithm was publicly
described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at
MIT, the letters RSA are the initials of their surnames, listed in
the same order as on the paper.
```

```
encoded_text = encode_str(text)
encoded_text
```

```
[19574323398017947091615178437177490746654486177 9,
37180720991543876204040857559298525283165093233 5,
65154836824015922175882884110935013573217146864 7,
65299791228464178113470203663384197236954853617 8,
65912364583240419576346652522487925597310904741 2,
63442017082347433005011178845191433410276703933 7,
59048831572485564925104917909534459597994101513 9,
65353313423186635020902079986731348678489403548 8,
66457101628225618695478706101425504583604322057 7,
63020559608171090371991776715546581302309874083 5,
65353313423980026516236035856274352029500607363 2,
68172022571518040366022415397819468708853929662 8,
65330994880381736712588136363478649551556860017 5,
56767491634660399953617937055303089889231067299 7,
57162284376829393682826222120516560856177327447 8,
18526251734657779137042505902925506304875214449 1,
57931648695365619030393224946161530198938184101 3,
64042064272305118327993194683824565393447127971 3,
66459421470931060782685428741582748508121860721 3,
18534998241231479953425992542799711431718833008 9,
56174219306355752895568837534156505331572343611 4,
60208435649770063005885517402754521114878437795 3,
63022187289991572361017968418733260856444309513 7,
```

```
662963285860432166486664785568077763006514274386,
475298603168879650436549702656500405342869156640,
635975478776366962146475347250930834486720209004,
602018756161112406365267743413217523738364374898,
573161394166600395094142328490447566724581913134]
```

```
print decode_str(encoded_text)
```

```
"In cryptography, RSA is an algorithm for public-key cryptography.
It is the first algorithm known to be suitable for signing as well
as encryption, and one of the first great advances in public key
cryptography. RSA is widely used in electronic commerce protocols,
and is believed to be secure given sufficiently long keys and the
use of up-to-date implementations. The algorithm was publicly
described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at
MIT, the letters RSA are the initials of their surnames, listed in
the same order as on the paper.
```

```
def rsa(text, r, m):
   return [Mod(t, m)^r for t in text]
```

Wir wählen die Primzahlen p und q:

```
p = random_prime(10^30)
q = random_prime(10^30)
print p
print q
```

```
357205226813155582549552868953
186062662322244480639454240871
```

```
m = p * q
print m
```

```
66462555496276917105434328711869848969507733996820759578063
```

```
phi_m = (p-1) * (q-1)
print phi_m
```

```
66462555496276917105434328711326581080372333933631752468240
```

Wir wählen Zahlen r und s mit $\mathrm{ggt}(r, \varphi(m)) = 1$ und

$$r \cdot s \equiv 1 \bmod \varphi(m).$$

```
d = 0
while d != 1:
   r = ZZ.random_element(10^25, 10^40)
   d = gcd(r, phi_m)
```

```
print r
html('$\\mathrm{ggt}(r, \\varphi(m)) = %d$' %gcd(r, phi_m))
```

```
48619659635672937069549452069235488700 41
```

$\mathrm{ggt}(r, \varphi(m)) = 1$

```
s = Mod(r, phi_m)^(-1)
print s
```

```
39013820261753138488910324737468188199790836281244573493 21
```

```
r * s
```

```
1
```

```
code = rsa(encoded_text, r, m)
code
```

```
[54784408666448985845106896381042214017887225804793614344548,
29649508826232885977157462232847777045888667180176171295973 3,
30064605244271850349748740883082340686812191535349506245356 5,
38205595577624497857498855440110744634957643440596743851052 3,
33947640739066808329265601128553543721488420346380888956281 2,
18969617765407839566364570737233186443386783478758038762785,
81259771701876607835947306167349868141601023696015721969 15,
26842986143700022787161006181581038748979027328273822457965 8,
28298975622889607098827576262544549767186409376272989942964 3,
86286558143101420525689233785855841811600447917372997786090,
10576279388610293373224661644040634392849182808528973235139 5,
14544779015206227229915304954102970625450761345713886601550 5,
19973891023178027972524931618759417534006824875546623268829 7,
31735624377802523395761923152491411420406247370914854734239 5,
23560432263377237161207737452070930359315965934513610012364 6,
14699088804441016133230321805013194930638640006066351256484 8,
31781700953349904233743782174285791257594595069791664869523 0,
24370126140159031623131814986631058657407963519780983261277,
77992828644382637250348348188014549227556099693935138328007,
11621338102059826299358376778842602111121636962405754021086 9,
36086259013908465304546588349159279812177854926421090081331 8,
49799648800726414787326399161767298094077861106579963851288,
33076387497087840894073237674093565661225194110736508605230,
28343063250419862618561783096987052218835873890664900465085 5,
11411485267421530869968172152789095522119214475045734493752 2,
51053600499052609705760247669517940972015025704258262651094,
18102527006803946233932975967037181029332553076559264458709 1,
92731242945950438876772696883487953246693691197989580302474]
```

```
print decode_str(rsa(code, s, m))
```

```
"In cryptography, RSA is an algorithm for public-key cryptography.
It is the first algorithm known to be suitable for signing as well
```

as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. The algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT, the letters RSA are the initials of their surnames, listed in the same order as on the paper.