# Elektronisches Geld Kryptographie mit MuPAD,

Prof. Dr.Dörte Haftendorn, Juli 05 Update Juni 07
Web: http://haftendorn.uni-lueneburg.de www.mathematik-verstehen.de

##########################################################

Mathix will von der Bank von Dagobert eine elektronische Münze zu 2€ bekommen und er will damit einkaufen.
Der Händler will die Münze zur Bank bringen und 2 € auf seinem Konto gutgeschrieben bekommen.
Anforderungen:
Niemand soll festellen können, dass das die Münze von Mathix war.
Jeder soll prüfen können, dass es sich um ein gültiges 2 €-Stück handelt.

---

Es wird mit dem RSA gearbeitet.
Schlüsselerzeugung der Bank von Dagobert
Dagobert wählt zwei große Primzahlen p und q und bildet ihr Produkt n.

```
//p:=numlib::prevprime(floor(sqrt(5*10^200)));
//q:=numlib::prevprime(floor(sqrt(29*10^200)));
//n:=p*q;
```

```
p:=31:  q:=59:  n:=p*q;
```

1829

```
ph:=(p-1)*(q-1);
```

1740

```
repeat
r:= random(2..ph): e:=r():
  until gcd(ph,e)=1 end_repeat:e;
```

989

```
e:=311;
```

311

```
igcdex(ph,e)
```

1, 116, −649

```
ph-649
```

1091

```
d:=op(igcdex(ph,e),3);
  // letztes Element euklid. Algorithmus
if (d<0) then d:=d+ph: end_if:d; //Korrektur bei negativ
```

−649

1091

```
d
```

```
d
```
1091

Probe

```
modp(e*d,ph)
```
1

**Das ist Dagoberts geheimer Schlüssel.**
**Der Öffentlichkeit gibt er e und n bekannt.**

```
e;n
```
311

1829

##########

Nun wählt Mathix

```
v:=17:
w:=1717: //vorläufig hier von Hand eintragen
Er wählt ein C aus Zn*
repeat
r:= random(2..n): c:=r():
  until gcd(n,c)=1 end_repeat:c;
```
1631

```
c:=25
```
25

Mathix berechnet das Inverse von C

```
igcdex(n,c)
```
1, −6, 439

```
cinv:=op(igcdex(n,c),3)
```
439

Probe

```
modp(c*cinv,n);
```
1

Er berechnet

```
powermod(c,e,n)
```
1090

```
powermod(c,e,n)
```
1090
```
s:=modp(powermod(c,e,n)*w,n)
```
463

Nun ist die Dagobert-Bank an der Reihe,
Mathix schickt ihr s.
Erst dadurch wird aus Mathix Berechnungen eine gültige
elektronische Münze. Dagobert rechnet

```
t:=powermod(s,d,n)
```
1176

Von Mathix' Konto werden 2 € abgezogen und die Bank sendet
t an Mathix. Mathix rechnet:

```
z:=modp(t*cinv,n)
```
486

Dies ist das elektronische 2€-Stück
############################################################
Mathix will damit einkaufen.
Der Laden prüft, indem er berechnet:

```
powermod(z,e,n);
```
1717

Dieses Doppelungsmuster ist  "in dieser Lehr-Verkürzung" das
Kennzeichen von 2€-Münzen. Der Laden  nimmt die Bezahlung an.
############################################################
Der Ladenbesitzer kann nun entweder selbst mit dieser Münze einkaufen,
oder er bringt sie zur Bank.
Jedenfalls wird nur geprüft, ob das 2€-Muster vorliegt.
Die Dagobertbank schreibt dem, der die Münze bringt, 2€ gut.
############################################################