1 1

2 2

Verschlüssele die Zahl x mit Hilfe des öffentlichen Schlüssels. (Für später als Kommentar: Verschlüsselte Nachricht verschicken.)

2 2

3 3

Vergiss die beiden Primzahlen.

3 3

4 4

Übersetze die Zahl in einen Text.

4 4

5 5

Speichere den geheimen Schlüssel.

5 5

6 6

Berechne die Wiederholfrequenz L.

6 6

7 7

Bestimme den Entschlüsselungsexponenten d.

7 7

8 8

Wähle zwei Primzahlen p und q.

8 8

9 9

10 10

Eine kleine Probe: Ist $de - 1$ durch L ohne Rest teilbar?

10 10

11 11

Entschlüssele die Zahl y mit Hilfe des geheimen Schlüssels. (Für später als Kommentar: Mail prüfen und einlesen.)

11 11

12 12

Speichere den öffentlichen Schlüssel. (Für später als Kommentar: den öffentlichen Schlüssel an Moneypenny schicken und den geheimen sichern.)

12 12

13 13

Würfele einen zufälligen Exponenten e für den öffentlichen Schlüssel.

13 13

14 14

Berechne die Ringgröße N.

14 14

15 15

Prüfe, ob die beiden Primzahlen verschieden sind.

15 15

16 16

Übersetze den Text „`Hi`“ in eine Zahl x und prüfe, ob diese nicht zu groß ist.

16 16

```
test := (d*e-1)/L;
if testtype(test, DOM_INT) then
  print("Probe ok!");
else error("Arrrg!"); end_if:
```

```
// checkmail():
// y := readmail();
z := powermod(y, d, N);
```

```
public := [N,e];
//mailto("moneypenny@mi6.gov.uk",
// "von Bilbo", N, e ):
```

```
e := random(3..L-2)();
```

```
N := p*q;
```

```
if p=q then error("p = q ist verboten!");
else print("OK. (p<>q)");
end_if:
```

```
x := text2num("Hi");
if x>=N then error("Nachricht zu lang!");
end_if:
```

```
else print("Ok.");
end_if:
```

```
y := powermod(x, e, N);
//mailto( "guest-sk08-???@bit.uni-bonn.de",
//        "von Frodo", N, e, y );
```

```
delete p,q:
```

```
num2text(z);
```

```
secret := [N,d];
```

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

```
d := 1/e mod L;
```

```
p := nextprime(2^8);
q := nextprime(2^9);
```