

1	1	9	9	Prüfe, ob e zulässig ist.	Vergiß L .
1	1	9	9		
2	2	10	10	Verschlüssele die Zahl x mit Hilfe des öffentlichen Schlüssels. (Für später als Kommentar: Verschlüsselte Nachricht verschicken.)	Eine kleine Probe: Ist $de - 1$ durch L ohne Rest teilbar?
2	2	10	10		
3	3	11	11	Vergiss die beiden Primzahlen.	Entschlüssele die Zahl y mit Hilfe des geheimen Schlüssels. (Für später als Kommentar: Mail prüfen und einlesen.)
3	3	11	11		
4	4	12	12	Übersetze die Zahl in einen Text.	Speichere den öffentlichen Schlüssel. (Für später als Kommentar: den öffentlichen Schlüssel an Money-penny schicken und den geheimen sichern.)
4	4	12	12		
5	5	13	13	Speichere den geheimen Schlüssel.	Würfele einen zufälligen Exponenten e für den öffentlichen Schlüssel.
5	5	13	13		
6	6	14	14	Berechne die Wiederholffrequenz L .	Berechne die Ringgröße N .
6	6	14	14		
7	7	15	15	Bestimme den Entschlüsselungsexponenten d .	Prüfe, ob die beiden Primzahlen verschieden sind.
7	7	15	15		
8	8	16	16	Wähle zwei Primzahlen p und q .	Übersetze den Text „Hi“ in eine Zahl x und prüfe, ob diese nicht zu groß ist.
8	8	16	16		

```

9
delete L:
if igcd(e,L)>1 then
    error("e schlecht, versuch's nochmal.");
else print("Ok.");
end_if:

9
10
test := (d*e-1)/L;
if testtype(test, DOM_INT) then
    print("Probe ok!");
else error(Arrrg!); end_if:

10
11
// checkmail():
// y := readmail();
z := powermod(y, d, N);

11
12
public := [N,e];
//mailto("moneypenny@mi6.gov.uk",
// "von Bilbo", N, e, y ):

12
13
e := random(3..L-2)();

13
14
N := p*q;

14
15
if p=q then error("p = q ist verboten!");
else print("OK. (p!=q)");
end_if:

15
16
x := text2num("Hi");
if x>=N then error("Nachricht zu lang!");
end_if:

9 1
10 2
11 3
12 4
13 5
14 6
15 7
16 8

1
2
3
4
5
6
7
8

if igcd(e,L)>1 then
    error("e schlecht, versuch's nochmal.");
else print("Ok.");
end_if:

y := powermod(x, e, N);
//mailto( "sk06-z8-77@bit.uni-bonn.de",
// "von Frodo", N, e, y );

delete p,q:

v := num2text(z);

secret := [N,d];

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

d := 1/e mod L;

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

```