Asymmetrische Verschlüsselung

Beispiel mit Zahlen für die berechnung von Public- und Private Key:

Es sei:

- e der Public Key
- d der Private Key
- M ein Zeichnen der zu verschlüsselnden Nachricht.
- C ist das verschlüsselt Zeichen der Nachricht
- N ist die Basis für die Moduloberechungen

- p und q sind Primzahlen

Public Key berechnen:

1. Zwei Primzahlen wählen:
   p = 17
   q = 11

2. N = p*q = 187

3. Eine weitere Zahl e wählen.
   Voraussetzung: ggT[e,(p-1),(q-1)] = 1 (ggT grösster gemeinsamer Teiler)
   Das heisst e ist *teilerfremd* zu N oder anders gesagt, N darf nicht durch e teilbar sein.

   e = 7

4. Der Public Key besteht aus e und aus N.

Private Key berechnen:

5. Wir müssen nun den Private-Key **d** bestimmt.
   Dazu können wir diese Formel verwenden:

   1 = e*d mod ((p-1)*(q-1))

   Wir können diese Formel nicht nach d auflösen, kennen jedoch e, p und q.
   Nun probieren wir mittels Brute-Force alle Zahlen beginnend von 1, bis wir ein d finden für das die Formel gilt.

   ➔ Es geht noch weiter

1 = 7*d mod ((17-1)*(11-1)) = 7*d mod(160)

d = 1 ➔ 7*1 mod(160) = 7 mod(160) = 7

d = 2 ➔ 7*2 mod(160) = 14 mod(160) = 14

d = 3 ➔ 7*3 mod(160) = 21 mod(160) = 21

… wir sind viel zu tief

d = 22 ➔ 7*22 mod(160) = 154 mod(160) = 154

d = 23 ➔ 7*23 mod(160) = 161 mod(160) = 1 ➔ **also ist d = 23**

Nachricht verschlüsseln:

$C=M^{\wedge e}$ mod(N)

Buchstabe X in ASCII = 88

C = 88^7 mod(187) = 11

Nachricht entschlüsseln:

$M=C^{\wedge d}$ mod(N)

Buchstabe X in ASCII = 88

M = 11^23 mod(187) = 88 ➔ X