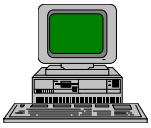

Arbeitsblatt RSA

Bob möchte Alice eine geheime Nachricht übermitteln. Der Einfachheithalber nehmen wir an, dass diese Nachricht nur aus dem Buchstaben "X" besteht.

Alice's erstellt den öffentlichen Schlüssel

Alice wählt 2 Primzahlen p und q

p = **17** q = **11**

N = p*q = **187**

Alice wählt eine Zahl e

e = **7**

Voraussetzung: ggT[e,(p-1),(q-1)] = 1

Klartextnachricht "X"

Öffentlicher Schlüssel von Alice:

N = **187**
e = **7**

Bob verschlüsselt

ASCII-Code von X = **1011000**
Als Dezimalzahl = **88** = M

Geheimcode C aus M berechnen
$C = M^e \pmod N = \mathbf{11}$

Alice erstellt den privater Schlüssel

$e*d = 1 \ [\mathrm{mod}(p-1)*(q-1)]$

Die Zahl d ist der private Schlüssel! Die Gleichung kann mit dem euklidischen Algorithmus aufgelöst werden.

d = **23**

Alice entschlüsselt den Geheimtext

Geheimtext C = **11**

$M = C^d \pmod N = \mathbf{88}$

Binärzahl von M = **1011000**

ASCII-Code **1011000** = **X**