Arbeitsblatt RSA

Bob möchte Alice eine geheime Nachricht übermitteln. Einfachheitshalber 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= q=

N = p*q =

Alice wählt eine Zahl e

e =

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

Klartextnachricht "X"

Öffentlicher Schlüssel von Alice:

N =
e =

Bob verschlüsselt

ASCII-Code von X =
Als Dezimalzahl = = M

Geheimcode C aus M berechnen
$C = M^e \pmod N$ =

Alice erstellt den privater Schlüssel

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

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

d =

Alice entschlüsselt den Geheimtext

Geheimtext C =

$M = C^d \pmod N$ =

Binärzahl von M =

ASCII-Code =