

# Das RSA-Verfahren

Das RSA-Verfahren wurde 1978 von Rivest, Shamir und Adleman entwickelt.

## 1. Geeignete Schlüssel wählen

- Wähle zwei Primzahlen **p** und **q** !

$$p = \boxed{\phantom{00}} \text{ und } q = \boxed{\phantom{00}}$$

- Berechne das Produkt **N** der beiden gewählten Primzahlen p und q !

$$N = p \cdot q = \underline{\phantom{00}} \cdot \underline{\phantom{00}} = \boxed{\phantom{00}}$$

- Berechne das folgende Produkt **phi** = (p-1)·(q-1) !

$$phi = (\underline{\phantom{00}} - 1) \cdot (\underline{\phantom{00}} - 1) = (\underline{\phantom{00}}) \cdot (\underline{\phantom{00}}) = \boxed{\phantom{00}}$$

- Bestimme zwei natürliche Zahlen **d** und **e** so, dass gilt:  $(d \cdot e) \bmod phi = 1$   
(Für Interessierte: da der Rest der Division  $(d \cdot e) : phi$  den Wert 1 ergibt sind die Zahlen d und e „modular invers“ bezüglich der Division durch phi).

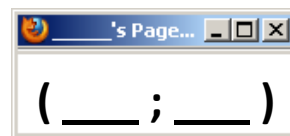
erster Versuch:

- Die erste Zahl, die als Rest einer Division durch  $\underline{\phantom{00}}$  den Rest 1 lässt, ist  $\underline{\phantom{00}}$ :  
 $\underline{\phantom{00}} \bmod \underline{\phantom{00}} = 1$

Nun sind ein **geheimer** Schlüssel **d**



und ein **öffentlicher** Schlüssel **(e;N)** gefunden.



## 2. Verschlüsseln

Die Verschlüsselung einer natürlichen Zahl  $m < N$  durch einen beliebigen Teilnehmer erfolgt mit Hilfe des öffentlichen Schlüssels  $(e;N)$  :

$$c = m^e \bmod N$$

Bsp.: Verschlüsselung der Zahl  $\underline{\phantom{00}}$  :

$$c = \underline{\phantom{00}}^{\underline{\phantom{00}}} \bmod \underline{\phantom{00}} = \boxed{\phantom{00}}$$

## 3. Entschlüsseln

Die Entschlüsselung einer verschlüsselten Zahl c durch den Empfänger erfolgt mit Hilfe des geheimen Schlüssels d und dem öffentlichen N:

$$m = c^d \bmod N$$

Bsp.: Entschlüsselung der Zahl  $\underline{\phantom{00}}$  :

$$m = \underline{\phantom{00}}^{\underline{\phantom{00}}} \bmod \underline{\phantom{00}} = \boxed{\phantom{00}}$$