Das RSA-Verfahren

Das RSA-Verfahren wurde 1978 von **R**ivest, **S**hamir und **A**dleman entwickelt.

1. Geeignete Schlüssel wählen

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

  p = ____ und **q** = ____

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

  N = p · q = ____ · ____ = ____

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

  phi = (___-1)·(___-1) = (___)·(___) = ____

- Bestimme zwei natürliche Zahlen **d** und **e** so, dass gilt: $(d \cdot e) \bmod phi = 1$
  (Für Interessierte: da der Rest der Division (d · 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 ____ den Rest 1 läst, ist ___:
    ____ mod ____ = 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 ____: $c = \_\_^{\_\_} \bmod \_\_ =$ ____

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 ____: $m = \_\_^{\_\_} \bmod \_\_ =$ ____