# Das RSA-Verfahren – Lösung für p=5, q=11

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** = 5 und **q** = 11

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

  **N** = p · q = 5 · 11 = 55

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

  **phi** = (5 -1)·(11 -1) = (4 )·(10 ) = 40

- 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).

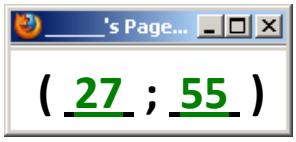
  erster Versuch:

  - Die erste Zahl, die als Rest einer Division durch 40 den Rest 1 läst, ist 41 :
    41 mod 40 = 1 — 41 lässt sich nicht in zwei Faktoren zerlegen, weil sie eine Primzahl ist.
    -> es gibt kein Zahlenpaar (d;e) mit d_e = 41

  zweiter Versuch:

  - Die zweite Zahl, die als Rest einer Division durch 40 den Rest 1 läst, ist 81 :
    81 mod 40 = 1 — 81 lässt sich als 3 _ 27 darstellen. Damit ist ein Zahlenpaar (d;e) mit d_e = 81 gefunden.

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 2 : $c = 2^{27} \bmod 55 = 18$

## 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 18 : $m = 18^3 \bmod 55 = 2$