

# RSA Step by Step

## Schlüsselerzeugung

Wähle zwei Primzahlen und berechne ihr Produkt:

P = 53 und Q = 59.  
n = P\*Q = 3127.

außerdem berechnet man  $\varphi(n) = (p-1)(q-1)$ :  $\varphi(n) = 3016$  Nun benötigt man eine kleinere Zahl e mit folgenden Eigenschaften: \* Eine positive Ganzzahl \* Darf kein Faktor von n sein ( $\text{ggT}(n,e)=1$ ) \* Darf kein Faktor von  $\Phi(n)$  mit  $\Phi(n)=(P-1)*(Q-1)$  sein ( $\text{ggT}(\Phi(n),e)=1$ ) \*  $1 < e < \Phi(n)$ . wir nehmen für unser Beispiel e=3 Damit ist der **öffentliche Schlüssel**: 3127,3 (n,e) **Privater Schlüssel**: \* Um den privaten Schlüssel zu erhalten, benötigt man eine natürliche Zahl d mit  $d = (k*\Phi(n) + 1)/e$ . 'k' ist dabei eine beliebige natürliche Zahl - **man kann aber nur solche k-s verwenden, bei denen d eine natürliche Zahl (>0) ergibt!** \* Wählt man für k=2 ergibt sich d=2011. Damit ist der **private Schlüssel**: 3127,2011 (n,d) ===== Verschlüsselung ===== Der Algorithmus kann nur Zahlen zwischen 0 und n ver- und entschlüsseln, man muss also zunächst Informationen als Zahlen codieren, zum Beispiel H=8,A=1,I=9. Damit wird HAI zur Zahl 819. Verschlüsseln:  $\text{geheimtext} = \text{klartext}^e \bmod n$  also  $819^3 \bmod 3127 = 1899$  ===== Entschlüsseln ===== \* Zu entschlüsseln:  $\text{geheimtext}=1899$ . \* Vorgehen:  $\text{klartext} = \text{geheimtext}^d \bmod n$  also  $1899^{2011} \bmod 3127 = 819$

From:  
<https://info-bw.de/> -

Permanent link:  
<https://info-bw.de/faecher:informatik:oberstufe:kryptographie:rsa:start?rev=1648810438>

Last update: **01.04.2022 10:53**

