

RSA Step by Step

Schlüsselerzeugung

Wähle zwei Primzahlen und berechne ihr Produkt:

$$\begin{aligned} P &= 53 \text{ und } Q = 59. \\ n &= P \cdot Q = 3127. \end{aligned}$$

außerdem berechnet man $\Phi(n) = (P-1)(Q-1)$ (eulersche Φ -Funktion):

$$\Phi(n) = 3016$$

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 $\Phi(n)=(P-1) \cdot (Q-1)$ 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 $\Phi(n) = 3016$
- Für unser Beispiel:
- Außerdem benötigt man eine Zahl 'd' mit $d = (k \cdot \Phi(n) + 1) / e$. 'k' ist dabei eine beliebige ganze Zahl.
- 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://wiki.qg-moessingen.de/> - **QG Wiki**

Permanent link:
<https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:kryptographie:moderneverfahren:rsa:start?rev=1578146057>

Last update: **04.01.2020 14:54**

