RSA Step by Step

Schlüsselerzeugung

Wähle zwei Primzahlen und berechne ihr Produkt:

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

außerdem benötigt man eine kleiner Zahl e mit folgenden Eigenschaften:

- Eine positive Ganzzahl
- Darf kein Faktor von 'n' sein (ggT(n,e)=1)
- `1 < e < Φ(n)` mit `Φ(n)=(P-1)*(Q-1)`

wir nehmen für unser Beispiel e=3

Damit ist der **öffentliche Schlüssel**: 3127,3 (n,e)

Privater Schlüssel:

- Um den privaten Schlüssel zu erhalten berechnet man zunächst `Φ(n) = (P-1)(Q-1)` (eulersche Φ-Funktion).
- Für unser Beispiel: Φ(n) = 3016
- Außerdem benötigt man eine Zahl 'd' mit `d = (k*Φ(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: `geheimtext = klartext^e mod n` also `819^3 mod 3127 = 1899`

Entschlüsseln

- Zu entschlüsseln: geheimtext=1899.
- Vorgehen: `klartext = geheimtext^d mod n` also `1899^2011 mod 3127 = 819`