RSA Step by Step

Schlüsselerzeugung

Öffentlicher Schlüssel

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, die teilerfremd zu $\varphi(n)$ ist (Teilerfremd = größter gemeinsamer Teiler beider Zahlen ist 1). Wir wählen für unser Beispiel $e=3$

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

Privater Schlüssel

Um den privaten Schlüssel zu erhalten, benötigt man eine natürliche Zahl d mit $d \cdot e = 1 (mod\;\varphi(n))$. Für unser Beispiel genügt $d=2011$ diesen Bedingungen, denn $2011\cdot 3 = 1 (mod\;\varphi(n))$

Damit ist der **private Schlüssel**: (n;d) → (3127;2011)

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`

(A1)

Verwende das Cryptool um das RSA Verfahren selbst schrittweise nachzuvollziehen und verschlüssle den Text `Informatik ist wichtig` mit den dort von dir gewählten Parametern.

- Notiere den öffentlichen Schlüssel
- Notiere den geheimen Schlüssel
- Halte fest wie du den Text codierst
- Halte Klartext und verschlüsselten Text fest
- Entschlüssle die Nachricht