07.08.2025 16:01 1/2 start

RSA Step by Step

Schlüsselerzeugung

Wähle zwei Primzahlen und berechne ihr Produkt:

```
P = 53 und Q = 59.

n = P*Q = 3127.
```

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 (ggT(n,e)=1)
- Darf kein Faktor von $\Phi(n)$ mit $\Phi(n) = (P-1)*(Q-1)$ sein $(ggT(\Phi(n),e)=1)$
- 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 ganze Zahl d mit d = (k*Φ(n) + 1) / e. 'k' ist dabei eine beliebige ganze Zahl man kann aber nur solche k-s verwenden, bei denen d eine ganze Zahl ergibt!
- Wählt man für k = 2ergibt 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

07:54

 $Last \\ update: \\ 08.06.2021 \\ faecher: informatik: oberstufe: kryptographie: moderne verfahren: rsa: start https://www.info-bw.de/faecher: informatik: oberstufe: kryptographie: moderne verfahren: rsa: start? rev=1623138893 \\ faecher: informatik: oberstufe: kryptographie: moderne verfahren: rsa: start https://www.info-bw.de/faecher: informatik: oberstufe: kryptographie: moderne verfahren: rsa: start? rev=1623138893 \\ faecher: informatik: oberstufe: kryptographie: moderne verfahren: rsa: start https://www.info-bw.de/faecher: informatik: oberstufe: kryptographie: moderne verfahren: kryptographie: kryptogr$

From: https://www.info-bw.de/ -

Permanent link:

https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:moderneverfahren:rsa:start?rev=1623138893

Last update: **08.06.2021 07:54**



Printed on 07.08.2025 16:01 https://www.info-bw.de/