

RSA-Verschlüsselung

Beispiel-Eingaben zur RSA-Simulation unter media.kswillisau.ch > IN > Verschlüsselung

The screenshot shows a simulation of the RSA encryption process between Alice and Bob. Alice's side (left) shows her choosing prime numbers $p=5$ and $q=11$, calculating $n=pq=55$ and $m=(p-1)(q-1)=40$. She then chooses $a=27$ and finds $b=3$ such that $ab \equiv 1 \pmod{m}$. Finally, she decrypts Bob's message $x=39$ to get $y=19$. Bob's side (right) shows him receiving the message $x=39$ and encrypting it to $y=19$ using Alice's public key $n=55$ and $a=27$.

Quelle: <http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/RSA.swf>

★ Hinweis zur Berechnung von a und b:

Die Bedingung ist $(a * b) \pmod{m} = 1$. Man sucht also eine Zahl, welche bei der ganzzahligen Division durch m einen Rest 1 ergibt und sich in zwei ganzzahlige Faktoren a und b zerlegen lässt. In unserem Beispiel ist $m = 40$.

1. Versuch:

Die erste Zahl die bei der Division durch 40 Rest 1 ergibt ist 41: 41 ist eine Primzahl und lässt sich nicht in Faktoren zerlegen.

2. Versuch:

Die zweite Zahl die bei der Division durch 40 Rest 1 ergibt ist 81: 81 lässt sich als $27 * 3$ darstellen. Wir haben also eine mögliche Lösung für a und b gefunden. Dabei wird b geheim gehalten.

◎ Hinweis zu den Modulo-Berechnungen:

Hier lässt sich der im Betriebssystem integrierte Rechner einsetzen. Unter Windows ist er im Startmenü unter Zubehör zu finden. Aktivieren Sie unter Ansicht den Modus „wissenschaftlich“. Nun stehen Ihnen Mod und x^y zur Verfügung.

