

LU03.L05 - RSA-Verschlüsselungsverfahren

Arbeitsauftrag

- **Schlüsselgenerierung:**

1. Gewählte Primzahlen: $p = 61$ und $q = 53$.
2. Produkt $n: n = p * q = 3233$.
3. Totient Funktion $\phi(n): \phi(n) = (p-1)(q-1) = 3120$.
4. Öffentlicher Exponent $e: e = 17$.
5. Privater Exponent $d: d = 2753$.

- **Öffentlicher Schlüssel (Public Key):** $(n, e) = (3233, 17)$

- **Privater Schlüssel (Private Key):** $(n, d) = (3233, 2753)$

- **Verschlüsselung:**

1. Nachricht $m = 123$.
2. Chiffertext $c: c = m^e \bmod n = 855$.

- **Entschlüsselung:**

1. Chiffertext $c = 855$.
2. Entschlüsselte Nachricht $m: m = c^d \bmod n = 123$.

- **Verifikation:**

1. Die entschlüsselte Nachricht m stimmt mit der ursprünglichen Nachricht überein.

From:
<https://wiki.bzz.ch/> - BZZ - Modulwiki

Permanent link:
<https://wiki.bzz.ch/modul/m183/learningunits/lu03/loesungen/asymmetrischeverfahren?rev=1711631267>

Last update: **2024/03/28 14:07**

