RSA Verschlüsselung* – Schritt für Schritt (1)

🔐 RSA-Verschlüsselung – Schritt für Schritt

🧭 Überblick: Die 6 RSA-Schritte

1. **Zwei Primzahlen wählen:** p und q
2. **Modulus berechnen:** n = p * q
3. **φ(n) berechnen:** φ(n) = (p - 1) * (q - 1)
4. **Öffentlichen Schlüssel wählen:** e, teilerfremd zu φ(n)
5. **Privaten Schlüssel berechnen:** d, sodass e * d mod φ(n) = 1
6. **Nachricht verschlüsseln und entschlüsseln**

📦 Beispiel: Du willst „Hl“ verschicken

Schritt 1: Zwei Primzahlen wählen

Wir nehmen kleine Zahlen:
p = 3, q = 11

Schritt 2: Modulus berechnen

n = p * q = 3 * 11 = 33

Schritt 3: φ(n) berechnen

φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20

Schritt 4: Öffentlichen Schlüssel wählen

Wähle e = 3, denn 3 ist teilerfremd zu 20
→ Öffentlicher Schlüssel: (e = 3, n = 33)

Schritt 5: Privaten Schlüssel berechnen

Finde d, sodass e * d mod φ(n) = 1
→ 3 * 7 = 21, 21 mod 20 = 1
→ Privater Schlüssel: (d = 7, n = 33)

---

*Erstellt von J. Aeckersberg mit Hilfe von Copilot am 29.10.2025 und https://youtu.be/NvVErwsv76g?si=urRvmeUnJlRHv1vd

RSA Verschlüsselung* – Schritt für Schritt (2)

Schritt 6: Nachricht verschlüsseln und entschlüsseln

🔤 Nachricht: „HI“

Zahlenzuordnung:

- H = 8
- I = 9

🔐 Verschlüsseln mit öffentlichem Schlüssel (e = 3, n = 33)

Formel: Chiffre = Zahl^e mod n

- 8^3 = 512, 512 mod 33 = 17
- 9^3 = 729, 729 mod 33 = 3
  → Verschlüsselte Nachricht: 17, 3

🔓 Entschlüsseln mit privatem Schlüssel (d = 7, n = 33)

Formel: Klartext = Chiffre^d mod n

- 17^7 mod 33 = 8 → H
- 3^7 mod 33 = 9 → I
  → Entschlüsselte Nachricht: „HI“

*Erstellt von J. Aeckersberg mit Hilfe von Copilot am 29.10.2025 und https://youtu.be/NvVErwsv76g?si=urRvmeUnJlRHv1vd