Übung 4

**An RSA encryption scheme has the set-up parameters p = 31 and q = 37.**

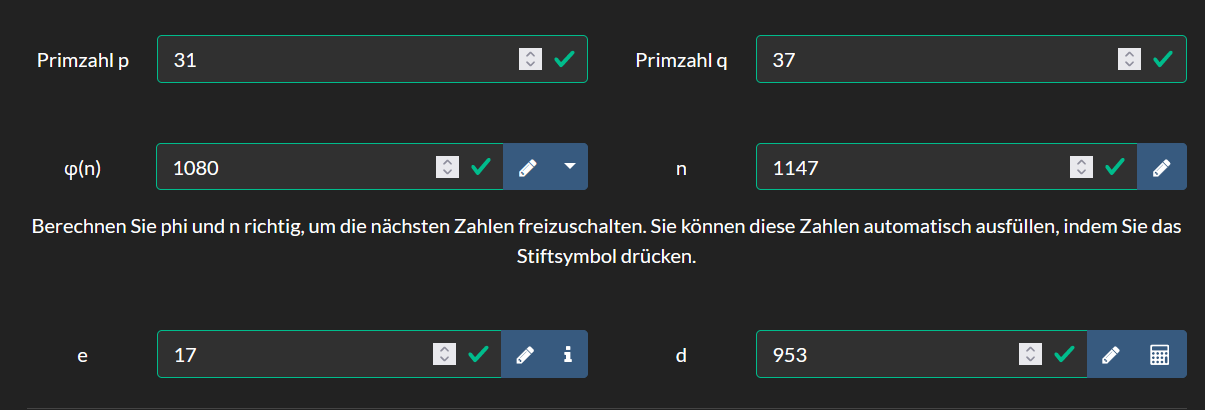
**The public key is e = 17.**

1. **Decrypt the ciphertext y = 2 using the Cryptool or a pocket calculator!**



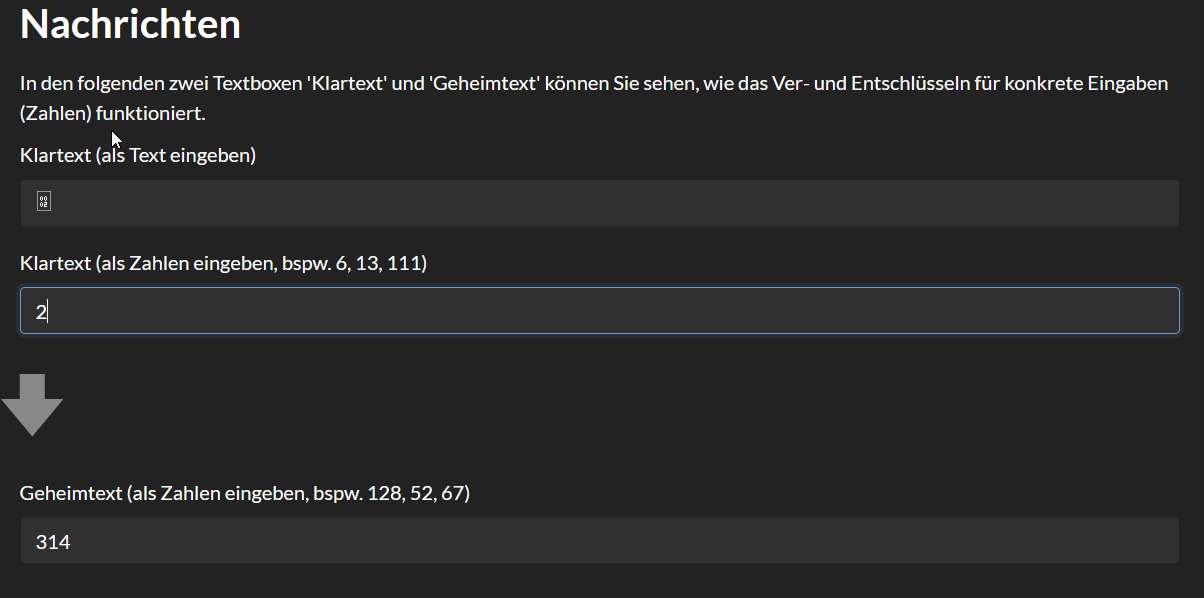
**d = 953**

**Nachgerechnet mit Crypttool:**

****

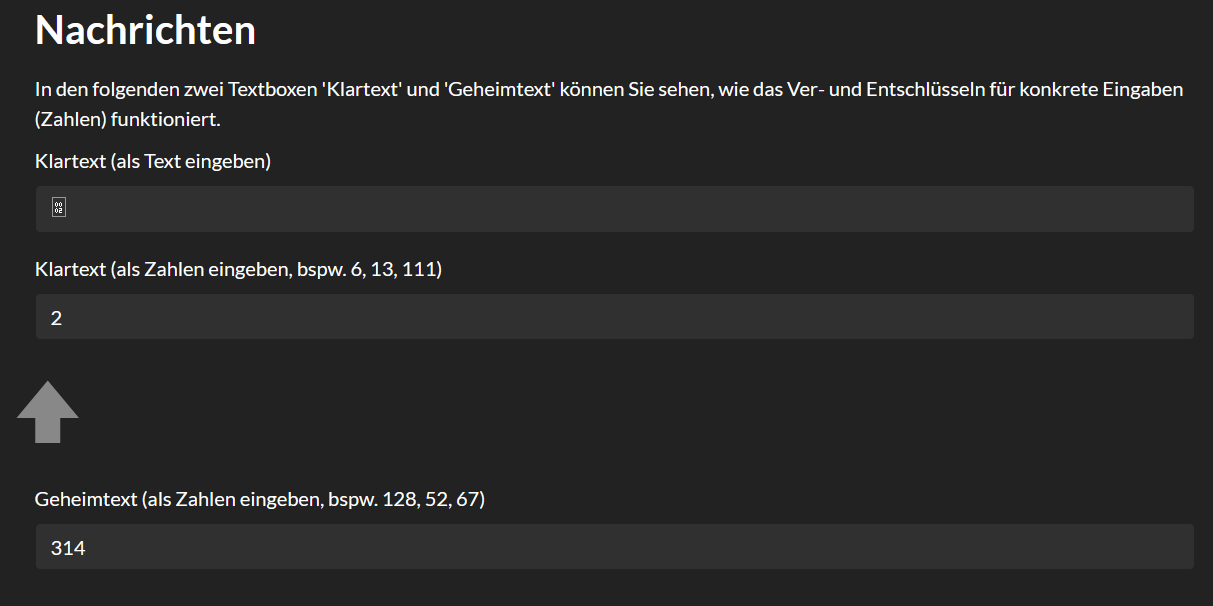
**Mit** [**Cryotool**](https://www.cryptool.org/de/cto/rsa-step-by-step)**:**

**Verschlüsseln:**

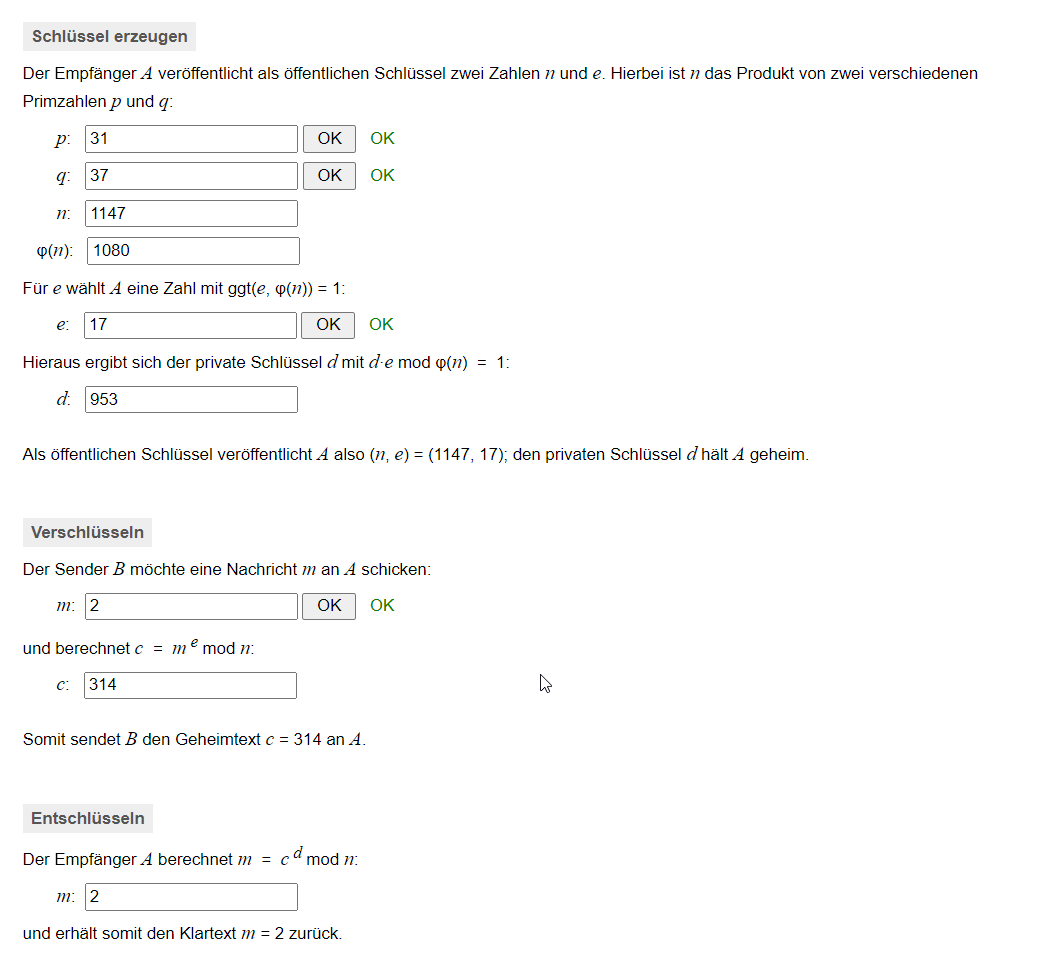
****

1. **Verify your result by encrypting the plaintext!**

**Entschlüsseln:**

****

**Mit anderem** [**Cryptorechner**](https://www.inf.hs-flensburg.de/lang/krypto/protokolle/rsa.htm)**:**

****

**Eine händische Verschlüsselung erweist sich als unpraktikabel aufgrund der großen Zahlen. Daher erfolgte die Verschlüsselung und Entschlüsselung über die Cryptools.**