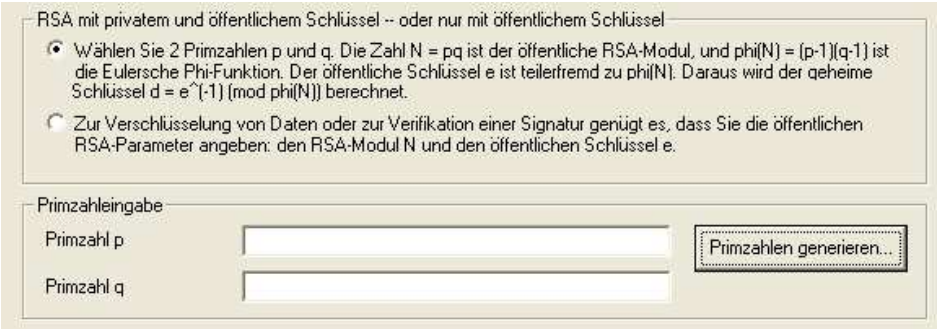
Anleitung: Ver- und Entschlüsseln mit der RSA-Demo von *CrypTool*

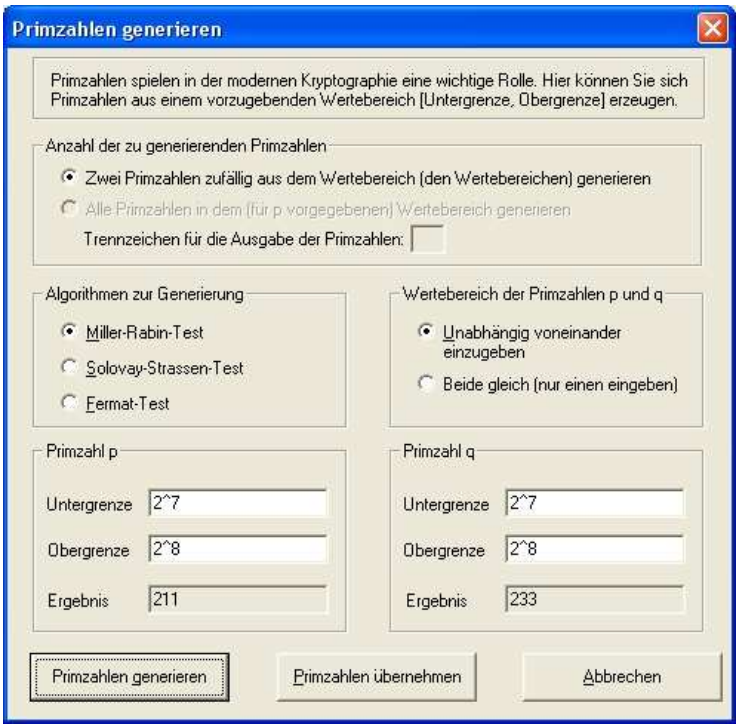
1. RSA-Schlüsselpaar generieren:

Starte *CrypTool* und rufe im Menü *Einzelverfahren* → *RSA-Kryptosystem* → *RSA-Demo...* auf! Es erscheint ein (auf den ersten Blick etwas unübersichtliches) Fenster. Betrachte zunächst nur den oberen Ausschnitt:



Es gibt zwei Möglichkeiten, die Schlüssel **(e; N)** und **d** zu konstruieren:

- zwei Primzahlen in die Felder für p und q eintragen oder
- die Primzahlen von *CrypTool* wie folgt erzeugen lassen: Knopf „Primzahlen generieren“ drücken. Ein neues Fenster erscheint mit den voreingestellten Werten:

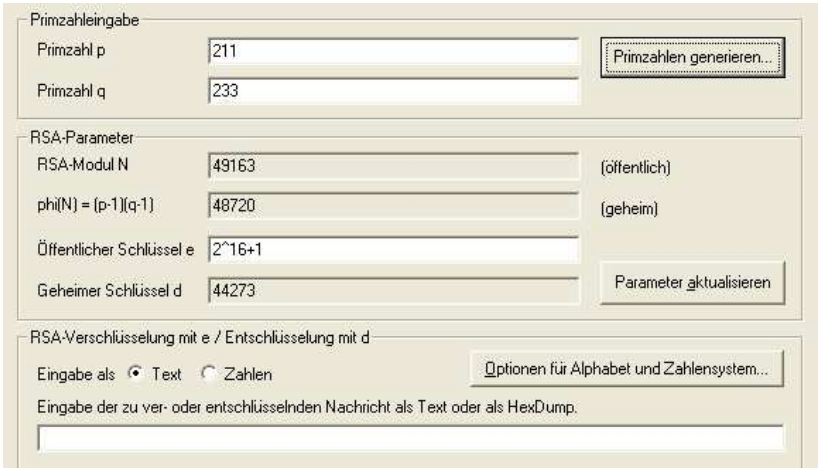


Wir haben also zwei Primzahlen zwischen $2^7 = 128$ und $2^8 = 256$ erhalten. Wenn uns diese Zahlen nicht gefallen sollten, drücken wir ggf. mehrfach „Primzahlen generieren“ und erhalten dann andere Primzahlen aus diesem Bereich, z. B. 227 und 251. *CrypTool* benutzt Pseudozufallszahlen, die stets in der gleichen Reihenfolge auftreten, es macht also Sinn, mehrmals auf den Knopf zu drücken!

Klicke nun auf „Primzahlen übernehmen“. Es erscheint wieder der Ausgangsschirm, aber neben den Primzahlen p und q sind bereits der **RSA-Modul N** und **phi(N) = (p-1)(q-1)** eingetragen. Als öffentlicher Schlüssel e ist immer $2^{16}+1 = 65537$ voreingestellt[1]. Wem diese Zahl nicht gefällt, kann auch hier eine andere eintragen. Diese muss aber teilerfremd zu phi(N) sein!

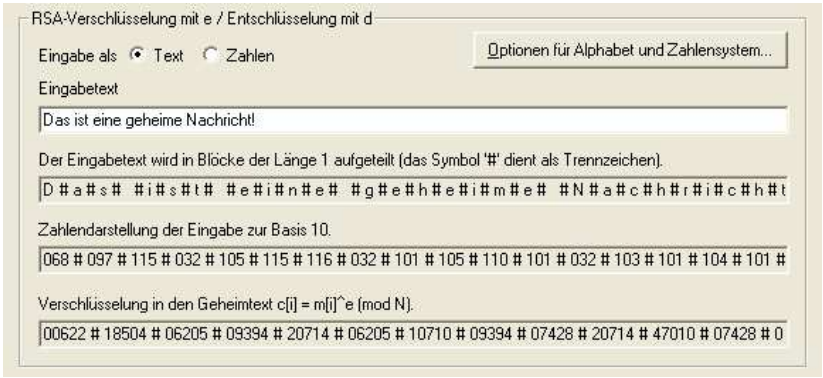
[1] Wer wissen will, warum gerade diese Zahl bevorzugt wird, sollte sich z. B. mit Hilfe des Windows-Taschenrechners ihre Darstellung im Dualsystem anschauen

Der zugehörige geheime Schlüssel wird ebenfalls automatisch erzeugt:



2. Verschlüsseln:

- Gib einen Text in das untere Eingabefeld ein!
- Klicke auf „Verschlüsseln“ um ihn zu **verschlüsseln**!

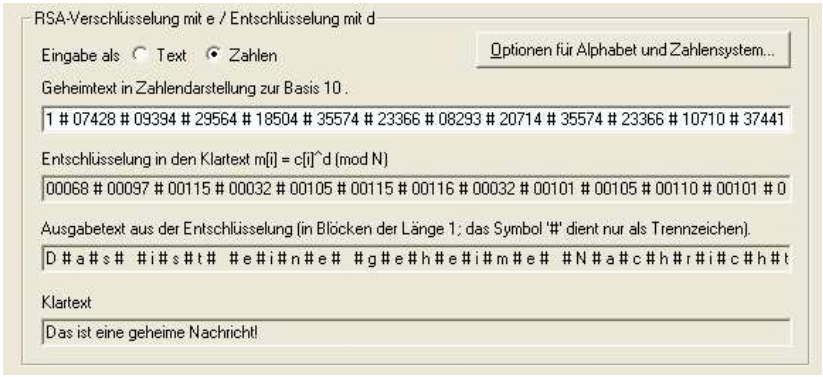


Wegen des relativ kleinen Moduls **N** wird der Text in Blöcke der Länge 1 unterteilt[2] und als Zahlen dargestellt (die entsprechenden ASCII-Nummern). Diese werden dann Block für Block (bei Blocklänge 1 also Zeichen für Zeichen) verschlüsselt.

3. Entschlüsseln:

Trotzdem wollen wir uns überzeugen, dass sich dieser „Geheimtext“ wieder korrekt **entschlüsseln** lässt:

- Kopiere den Geheimtext in die Eingabezeile!
- Klicke auf den Knopf „Zahlen“! (Wenn Du das vergisst, weißt dich *CrypTool* darauf hin.)
- Klicke auf den Knopf „Entschlüsseln“! Ergebnis:



[2] Bei einem so kleinen Modul N handelt es sich um eine schlichte monoalphabetische Verschlüsselung, die ein Knacken per Häufigkeitsanalyse erlaubt. Bei größeren Primzahlen werden jedoch stets mehrere Zeichen in einem Block zusammengefasst.