**erstellt von**Alec Schitzkat & Karl R. Jahn

**Dresden, der 03. Januar 2022**

Dokumentation zur Informatikabschlussarbeit der

25. Oberschule „Am Pohlandplatz“ Dresden

**mit den Namen**„RSA-Tool“

# Idee

Im Zeitalter der Digitalisierung wird die Sicherheit dieser digitalen Daten zunehmend wichtiger. Deshalb ist es sinnvoll, sich mit ebendieser zu beschäftigen und so kam uns die Idee zum einen anderen dabei behilflich zu sein und zum anderen selber natürlich dazuzulernen, indem wir dies mit dem „RSA-Tool“ ermöglichen.

Das RSA-Tool soll in der Lage sein, das RSA-Verfahren durchzuführen (und dies nach heutigen Standard) und dies gleichzeitig zu visualisieren, sodass der Benutzer in der Lage ist dieses augenscheinlich trockene Verschlüsslungsverfahren nachvollziehen und verstehen zu können. Und als letztes möchten wir uns in der Kryptographie ausspielen und einige Verfahren zu unseren „eigenen“ vereinen.

# Das RSA-Verfahren

Das RSA-Verfahren, welches nach dessen Entwicklern Rivest, Shamir und Adlema bennant wurde basiert auf Zahlentheoretischen Problemen (die Ineffizienz der Faktorisierung großer Zahlen) und ist ein asymmetrisches Verfahren, d.h. es gibt einen privaten und einen öffentlichen Schlüssel (oder in den Fall sogar zwei).

## Schlüsselerzeugung

1. Wähle zwei unterschiedliche riesige (min. 600 Dezimalstellen, also 2048 Bytes) Primzahlen und.
2. Berechne das RSA-Modul aus und .
3. Berechne die Eulersche -Funktion aus .

Eulersche -Funktion:

da und und

1. Wähle eine zu teilerfremde Zahl .
2. Berechne , welches das multiplikative Inverse zu bezüglich darstellt. Dies geht über den erweiterten euklidischen Algorithmus.
3. Fertig! Die öffentlichen Schlüssel sind nun und das private Schlüsselpaar besteht aus . , und werden nun nicht mehr gebraucht.