FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2024/25
zu bearbeiten bis
04.12.24

Praktikum 3
zur Vorlesung Kryptologie

Auf meiner Internetseite soll eine kleine RSA-Schlüsselverwaltung entstehen (https://www.hoever-downloads.fh-aachen.de/krypto/ueb/schluessel/index.php).

Dort gibt es ein kleines Programm, das einen Text in eine Zahl und umgekehrt eine Zahl wieder in einen Text umwandeln kann.

Auf der Seite ist schon ein öffentlicher Schlüssel von mir abgelegt.

1. Erzeugen Sie sich mittels zweier ca. 100-stelliger Primzahlen (dezimal) einen RSA-Schlüssel und legen Sie den öffentlichen Teil auf der Internetseite ab.
2. Wählen Sie einen sinnvollen Text (maximal 90 Zeichen), wandeln Sie ihn mittels des Programms in eine Zahl um, und schicken Sie mir diese Zahl verschlüsselt.
3. Sie erhalten von mir eine verschlüsselte Zahl, die Sie entschlüsseln und in einen Text konvertieren können. Schicken Sie mir zur Bestätigung den dechiffrierten Text.
4. Schicken Sie sich gegenseitig verschlüsselte Texte.

Tipp wenn Sie mit Aribas arbeiten: Um Schwierigkeiten beim Einkopieren großer Zahlen nach Aribas zu vermeiden (Aribas akzeptiert häufig nur die hinteren Stellen), kann man in einem Texteditor eine Aribas-Funktion definieren, die die zu kopierende Zahl zurückgibt. Durch Import dieser Funktion kann man dann auf die Zahl zugreifen.