Angewandte Kryptographie 2 Prof. Dr.-Ing. Kerstin Lemke-Rust
SoSe 2025 Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 1

Hinweis: Verwenden Sie eine existierende Langzahlbibliothek, bei JAVA kann BigInteger genutzt werden.

C.1 Universelle Fälschung von RSA-Signaturen:

(a) Erzeugen Sie einen eigenen 3000-Bit RSA-Schlüssel (wie auch schon bei der Angewandten Kryptographie 1, Praktikum 5). Geben Sie alle verwendeten RSA-Schlüsselparameter aus.

(b) Implementieren Sie die universelle Fälschung von RSA Signaturen (vgl. Folie 19 der Vorlesung). Wählen Sie hierfür eine beliebige Nachricht. Nehmen Sie bei der universellen Fälschung sowohl die Rolle des Angreifers als auch die des Signierers (Orakel) ein. Prüfen Sie mit dem RSA-Verifikationsalgorithmus, dass die so berechneten RSA-Signaturen korrekt verifiziert werden.

C.2 DSA-Signaturen:

(a) Implementieren Sie die DSA-Schlüsselgenerierung (vgl. Folie 33 der Vorlesung). Geben Sie alle verwendeten DSA-Schlüsselparameter aus.
Hinweis: Verwenden Sie den Algorithmus aus Appendix A.2.1 von `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf` für die Bestimmung eines Generators.

(b) Implementieren Sie den DSA-Signaturalgorithmus mit der Hashfunktion SHA-256. Signieren Sie zufällig gewählte Nachrichten mit dem DSA-Signaturalgorithmus und prüfen Sie, dass der Verifikationsalgorithmus die Signaturen korrekt verifiziert.

(c) Erstellen Sie zwei DSA-Signaturen unter Verwendung derselben Zufallszahl r (vgl. Übungsblatt 1, Aufgabe T.3). Berechnen Sie den privaten DSA-Schlüssel ausgehend von diesen zwei DSA-Signaturen.