Angewandte Kryptographie
SoSe 2024

Prof. Dr.-Ing. Kerstin Lemke-Rust
Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 5

Hinweis: Verwenden Sie eine existierende Langzahlbibliothek mit ihren Hilfsroutinen, unter JAVA kann BigInteger genutzt werden.

C.1 (a) Implementieren Sie eine zufallsgesteuerte Generierung einer 1500-Bit Primzahl gemäß BSI/NIST Vorgaben (vgl. Folie 24 der Vorlesung zu Public-Key Kryptosystemen). Messen Sie die Zeitdauer von Primzahlgenerierungen unter Nutzung der Systemzeit. Welche Zeitmessungen beobachten Sie im Mittel und in Extremfällen?

(b) Erzeugen Sie einen eigenen 3000-Bit RSA-Schlüssel gemäß der Vorgehensweise beginnend auf Folie 19 der Vorlesung zu Public-Key Kryptosystemen. Geben Sie alle verwendeten RSA-Schlüsselparameter aus.

(c) Prüfen Sie durch Berechnung der Hintereinanderausführung einer RSA-Verschlüsselung und RSA-Entschlüsselung einer von Ihnen gewählten Zahl x, dass der neu erzeugte RSA Schlüssel funktioniert.

C.2 (a) Implementieren Sie den Chinesischen Restsatz und prüfen Sie auf die Korrektheit des Ergebnisses einer RSA-Entschlüsselung verglichen Ihrer Implementierung aus C.1.

(b) Führen Sie einen Performanzvergleich auf der Basis der Systemzeit durch. Schlüsselabhängige Konstanten des Chinesischen Restsatz sollen vorberechnet werden und damit nicht in die Zeitmessung eingehen. Verwenden Sie denselben 3000-Bit RSA-Schlüssel und dieselben 3000-Bit Eingangsdaten in die RSA-Entschlüsselung für die zwei folgenden Tests. Prüfen Sie, ob die Zeitmessungen zuverlässige Ergebnisse bringen, ansonsten bestimmen Sie den Mittelwert mehrerer Zeitmessungen für dieselben Daten.

i. Messen Sie die (mittlere) Zeitdauer einer Entschlüsselung ohne Chinesischen Restsatz.

ii. Messen Sie die (mittlere) Zeitdauer einer Entschlüsselung mit dem Chinesischen Restsatz.

Wie groß ist der praktische Performanzgewinn des Chinesischen Restsatzes?