LEHRSTUHL FÜR RECHNERARCHITEKTUR UND PARALLELE SYSTEME

Aspekte der systemnahen Programmierung bei der Spieleentwicklung

Gruppe Team 103 – Abgabe zu Aufgabe 504: RSA
Wintersemester 2022/23

Guo Linfeng Özakay, Baris Zheng, Julian

1 Einleitung

Das Praktikum Aspekte der systemnahen Programmierung bei der Spieleentwicklung beschäftigt sich mit dem Programmieren von Prozessen auf niedriger Ebene. Dabei ist es wichtig die Schnittstellen zwischen Hardware and Software effectiktive zu nutzen. Man lernt außerdem bei dem Praktium das Umgehen vom Optimieren von Programmen sowie die Programmiersprache Assembler, AArch64. Assembler ermöglicht die Assemblersprache in Maschinensprache zu übersetzten und das Programmieren in Assembler ermöglicht eine bessere Leistung für das Programm. Diese Verbesserung spielt in vielen Bereciehen der Informatik eine wichtige Rolle.
Das Praktikum beinhaltet viele Themengebiete. Eines davon ist die Kryptographie. Kryptographie ist ein essentieller Bestandteil unserer heutigen Kommunikation. Unsere Aufgabe ist es mit dem RSA-Algorithmus zubeschäftigen. Der RSA-Algorthmus ist nach seinen Erfindern Rivest, Shamir and Adleman ernannt und hat in der heutigen Zeit seine Relevants nicht nachtgelassen. Er wird in Bereichen wie zum Beispiel bei Banken, Webservern oder E-Mails, für Sicherheit und Datenschutz verwendt. Wir werden uns mit der Implementierung in Assembler und C beschäftigen, die Funktionsweise von RSA auseinandersetzen, die Korrekheit der Implementierung zu überprüfen und die Performanz der Implementierung analysieren. Die Bearbeitung dieser Teilberecihe wird im Folgenden beschrieben.

2 Lösungsansatz

2.1 Funktionsweise von RSA

Der RSA-Algorithmus gehört zu dem Public-key cryptography, Asymmetrisches Kryptosystem. Dies bedeutet für die Verschlüsselung der Nachricht wird der Public Key verwendet und bei der Entschlüsselung den Private Key. Ein Schlüssel ist ein Tupel, der aus Variablen besteht. Der öffentliche Schlüssel ist aus dem Tupel (e, N) und der private Schlüssel aus dem Tupel (d,N). Für die Wahl diese Variabeln gibt es bestimmten mathematischen Bedingungen.
Nach dem man die Schlüssel generiert hat, kann man die Nachricht mit der Formel verschlüsseln

$$c{=}m^2 \mod N \tag{1}$$

2.2 Primzahl Generierung

Für die Wahl von N werden zwei Primezahl verwendet, p und q.

2.3 Wahl für e

2.4 Der erweiterte Euklidische Algorithmus

2.5 Sicherheit von RSA

3 Korrektheit/Genauigkeit

4 Performanzanalyse

5 Zusammenfassung und Ausblick