**Studienarbeit T3\_3101 von Aaron Lacks und Luc Forster:**

Aufteilung:

1. Ziele und Vorgehensweise

1 1.1. Ziel der Arbeit . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

1 1.2. Geplante Vorgehensweise . . . . . . . . . . . . . . . . . . . . . . . . .

2. Grundlagen

2.1. Primzahlen . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . (Aaron)

2.1.1. Definition und Eigenschaften . . . . . . . . . . . . . . . . . . . (Aaron)

2.1.2. Bestimmung von Primzahlen . . . . . . . . . . . . . . . . . . . (Aaron)

2.1.3. Rolle der Primzahlen in der Kryptografie . . . . . . . . . . . . (Aaron)

2.2. Algebraische Strukturen . . . . . . . . . . . . . . . . . . . . . . . . . (Luc)

2.2.1. Monoid . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . (Luc)

2.2.2. Gruppe . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . (Luc

2.2.3. Zyklische Gruppe . . . . . . . . . . . . . . . . . . . . . . . . . (Luc)

2.2.4. Untergruppen . . . . . . . . . . . . . . . . . . . . . . . . . . . (Luc)

2.2.5. Ring . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . (Luc)

2.2.6. Körper . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . (Aaron)

2.3. Das diskrete Logarithmusproblem . . . . . . . . . . . . . . . . . . . . (Luc)

2.3.1. Das verallgemeinerte diskrete Logarithmusproblem . . . . (Luc)

2.3.2. Diffie-Hellman Key Exchange (DHKE) . . . . . . . . . . . . . (Luc)

3. Elliptische Kurven (Luc)

3.1. Arithmetik . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . (Luc)

3.2. Gruppeneigenschaften . . . . . . . . . . . . . . . . . . . . . . . . . . (Luc)

3.3. Punktbestimmung . . . . . . . . . . . . . . . . . . . . . . . . . . . . (Aaron)

3.3.1. Rechnerische Grundlagen . . . . . . . . . . . . . . . . . . . . . (Aaron)

3.3.2. Punktbestimmung: Brute-Force-Methode . . . . . . . . . . . . (Aaron)

3.3.3. Punktbestimmung: Punktaddition und -verdopplung . . . . . (Aaron)

3.3.4. Punktbestimmung: Algorithmische Brute-Force-Methode . . . (Aaron)

3.4. Das diskrete Logarithmusproblem über elliptischen Kurven . . . . . . (Luc)

3.5. Elliptic-Curve-Diffie-Hellman Key Exchange (ECDHKE) . . . . . . . (Luc)

4. Implementierung in Python (Luc)

5. Fazit und Ausblick (Aaron)