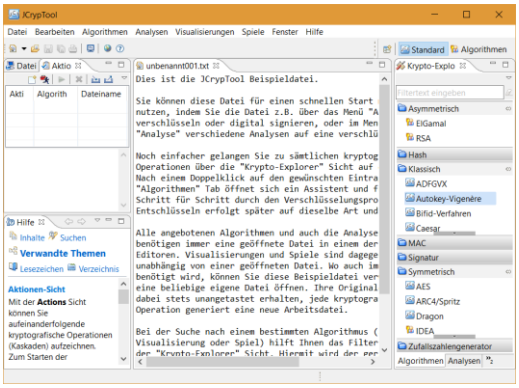
Integration von SUNSET/FFAPL in JCrypTool

JCrypTool (https://www.cryptool.org/de/jcryptool) ist ein modernes, mächtiges und leicht erlernbares eLearning-Werkzeug für das (Selbst-)Studium von Kryptographie. Das System ist Plugin-basiert, und bietet per Menü Zugriff auf eine Vielzahl kryptographischer Algorithmen, deren Funktionsweise und Verhalten schnell und leicht anhand eigener Beispiele untersucht und verstanden werden kann.

SUNSET/FFAPL[1] ist eine integrierte Entwicklungsumgebung, welche der schnellen Implementierung von kryptographischen Basismechanismen dient. Hierfür wurde die Programmiersprache „FFapl“ (Finite Field Application Language) geschaffen, welche kryptographisch relevante Strukturen (Restklassengruppen, Ringe, endliche Körper) als first-class Datentypen unterstützt, wodurch der sonst übliche Rückgriff auf Bibliotheken hinfällig wird. Die Manipulation von Daten geschieht unabhängig vom Typ in der gewohnten Infix-Notation (etwa Division in endlichen Körpern, Addition von Punkten auf elliptischen Kurven[2], o.ä.).



Funktionalitäten der Erweiterung im Einzelnen:

- Einbindung des Sunset/FFapl Skript-Interpreters in JCrypTool
- Konzeptionierung und Implementierung von Ein- und Ausgabefunktionen für Benutzer/innen-Eingaben.

Das SUNSET/FFAPL System ist unter GPL-3 lizenziert und frei verfügbar in github[3]. Die Aufgabenstellung besteht primär in der Integration des Skript-Interpreters für FFapl in JCrypTool; eine Integration von „Sunset“ als Entwicklungsumgebung für die FFapl Sprache ist nach Maßgabe der Möglichkeiten möglich.

Der Kreativität sind keine Grenzen gesetzt. Der/m Studierenden steht es nach Absprache mit dem Betreuer frei, das Funktionen-Repertoire der Software zu erweitern. Das Projekt ist in enger Kooperation mit der JCrypTool-Community abzuwickeln, d.h. der ständige Kontakt und Austausch mit der Community (insbes. *Prof. Bernhard Esslinger*, Universität Siegen) ist ausdrücklich erwünscht; die Betreuung der Master-Arbeit an der Universität Klagenfurt übernimmt *Prof. Dr. Stefan Rass*.

Projektverlauf und Aufgaben:

- Einarbeitung in JCrypTool und SUNSET/FFAPL
- Konzeption der Software und Erweiterungen
- Implementierung, Beschreibung und Tests

Rahmenbedingungen:

- Projektstart: Ab sofort!
- Projektende: 6-8 Monate nach Beginn (excl. Einarbeitungszeit)

Voraussetzungen:

- Ausgezeichnete Kenntnisse der Programmiersprache Java
- (programmiertechnische) Kreativität

Ansprechpartner und Betreuer:

- Prof. Dr. Stefan Rass (Universität Klagenfurt, E.1.52, DW 3715, e-Mail: stefan.rass@aau.at)
- Bezüglich JCrypTool: Prof. Bernhard Esslinger, Universität Siegen

Literatur

[1] A. O. Ortner: *Eine Umgebung zum vereinfachten Prototyping von Krypto-Verfahren*, Master-Arbeit, Universität Klagenfurt, 2012.

[2] S. Rass, J. Winkler: *Computer Aided Teaching of Elliptic Curve Cryptography*, Proc. of the 17th Int. Conference on Interactive Collaborative Learning, ICL2014, ISBN 978-1-4799-4438-5, pp. 180-175.

[3] SUNSET/FFAPL github repository: https://github.com/stefan-rass/sunset-ffapl