# Konzeptdokument „Kryptologie“

**Motivation**

Wir interessieren uns beide stark für das Thema Kryptologie und hatten bis jetzt keine Möglichkeit, uns auf diesem Gebiet sinnvoll zu vertiefen.
Da wir momentan für das Hauptstudium hin zu den Themen „Informationssicherheit und Kryptografie“ und „Netzwerktechnik“ tendieren, möchten wir die Chance nutzen, uns schon im Vorfeld intensiv mit den Grundlagen der Informationssicherheit zu befassen.
Der Einstieg in die Grundlagen der Kryptologie und deren Anwendung auf ein fundamentale Fallbeispiele erachten wir als gute Basis.

**Scope**

Erarbeitung der theoretischen Grundlagen zu den klassischen Verschlüsselungsverfahren

- Monoalphabetische Chiffrierung
- Polyalphabetische Chiffrierung

und deren Schwachstellen. Zudem möchten wir visuell demonstrieren, wie diese Schwachstellen für die Entschlüsselung ausgenutzt werden können.

**Meilensteine / Ziele**

1. Iteration
    - Projektplanung (User stories, Tasks, Meilensteine definieren)
    - Erarbeiten der wissenschaftlichen Grundlagen
    - Aufteilung der Tasks
    - Beginn der Programmierung (Klassendiagramm und Grundstruktur/UML fertig)

2. Iteration
    - Programm-Grundfunktionen funktionsfähig und getestet (primär Konsolenausgaben)
    - Dokumentation inhaltlich abgeschlossen

3. Iteration
    - GUI Ausgabe
    - Finalisierung der Dokumentation (inkl. Code-Review)
    - Ausarbeitung der grafischen Demonstration
    - Erstellung der Präsentation

**Resultat**

Am Ende des Projekts möchten wir einerseits ein lauffähiges Programm präsentieren können, welches die Grundlagen der Verschlüsselung und Ausnutzung der jeweiligen Schwachstellen veranschaulicht.
Zudem soll die Dokumentation einen fundierten theoretischen Unterbau liefern, damit andere interessierte Personen den Einstieg in die Kryptologie einfach nachvollziehen können.

**Betreuung**

| | | |
|---|---|---|
| Kursverantwortlicher | Philippe Nahlik | xnah@zhaw.ch |
| Scrum-Master | Jens-Christian Fischer | jens-christian.fischer@simplificator.com |
| Kunde | Lars Kruse | larspeterkruse@gmail.com |

**Verwendete Techniken**

Programmiersprache: Java (1.6)
Es ist die Programmiersprache, welche wir (als „Nicht-Applikationsentwickler“) am besten beherrschen. Zudem ist die Applikation so auf mehrere Plattformen ohne grosse Anpassungen portierbar und bietet sehr viele integrierte Funktionen (Unit-Testing, Code-Dokumentation, externe Libraries, etc.), welche uns die Arbeit enorm erleichtern werden.

Software-Versionskontrolle: Git / Github https://github.com/MLjubicic/Algohol
Wir haben im Verlauf des Studiums bereits sehr gute Erfahrungen gesammelt, zudem ist die Dokumentation des Projektfortschritts relativ einfach nachzuvollziehen

Projektplanung: Pivotal https://www.pivotaltracker.com/projects/501933
Auch mit diesem Tool haben wir im Rahmen von „Methoden der Programmierung“ sehr gute Erfahrungen sammeln können.