

**Kurzbeschreibung zur Information der Schülerinnen und Schüler in der Jahrgangsstufe
10**

Lehrkraft: Martin Franz
Rahmenthema: Kryptographie

Leitfach: Inf / M
(nur mit NTG-Zweig oder grund-
legenden Programmierkenntnissen)

Zielsetzung des Seminars

„**Kryptographie** bzw. **Kryptografie** (altgriechisch κρυπτός *kryptós*, deutsch ‚verborgen‘, ‚geheim‘ und γράφειν *gráphein*, deutsch ‚schreiben‘) ist ursprünglich die Wissenschaft der Verschlüsselung von Informationen. Heute befasst sie sich auch allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.“
(Quelle: de.wikipedia.org/wiki/Kryptographie)

Alle Teilnehmenden bekommen einen Überblick über die verschiedenen Verfahren und deren teilweise unsichtbaren Anwendung im digitalen Alltag von immer mehr Menschen. Die Seminarthemen bieten dabei eine weitere Vertiefung.

Die Mathematik, die in Verfahren steckt, die z.B. in den Weltkriegen und im kalten Krieg von Spionen benutzt wurden, ist weniger schwer zu verstehen. Es lassen sich aber auch Themen finden, die etwas höhere abstrakte Mathematik benötigen und so dem Schüler zu neuem individuellem Erkenntnisgewinn führen werden.

mögliche Arbeitstitel/Themen für die Seminararbeiten:

Klassische Verfahren

- Spionage-Chiffren
- Playfair-Verfahren

Mathematische Vertiefung

- Primzahltests

Asymmetrische Verfahren

- Diffie-Hellman Schlüsselaustausch
- RSA Verfahren

Kryptographie, die nicht zur Geheimhaltung dient

- Digitale Signatur
- Authentifizierung