W-Seminar im Fach
Mathematik

Lehrkraft: **Karl** **Leitfach: Mathematik**

Rahmenthema: Kryptographie im Laufe der Zeit – Von Tontafeln in Linear B bis hin zur public-key-Verschlüsselung im Internet

Zielsetzung des Seminars:

„*Jahrtausende schon verlassen sich Herrscher und Generäle auf schnelle und sichere Nachrichtenwege, um Länder und Armeen zu führen. Und seit jeher wissen sie, welche schwerwiegenden Folgen es haben kann, sollten ihre Botschaften in die falschen Hände geraten. Der Wunsch, bestimmte Nachrichten geheim zu halten, führte dazu, dass Staaten eigene Verschlüsselungsdienste einrichteten, die die bestmöglichen Codes entwickeln sollten und verantwortlich waren für den sicheren Nachrichtenverkehr. Zugleich versuchten die gegnerischen Codebrecher, diese Codes zu entschlüsseln und die Geheimnisse zu stehlen. Die Geschichte der Geheimschriften ist die Geschichte des jahrhunderte alten Kampfes zwischen Verschlüßlern und Entschlüßlern, der in Zeiten von Internetriesen wie google und facebook nichts von seiner Brisanz verloren hat: nie war die Verschlüsselung von Informationen für Privatpersonen so wichtig wie heute*.“ (aus: **Simon Singh**: *Geheime Botschaften*).

In diesem Seminar beschäftigen wir uns mit der Kunst des Verschlüsselns und dem Versuch diese Codes zu knacken. Dabei beleuchten wir einige historische Beispiele für Verschlüsselungen, die wegen ihrer Einfachheit einen guten Einstieg in die Thematik bieten. Anhand der geschichtlichen Entwicklung arbeiten wir uns bis in die Gegenwart vor, die von digitalen Verschlüsselungen geprägt ist. Dabei analysieren wir Codes auf ihre Sicherheit, ihre Tauglichkeit in der nachrichtendienstlichen Praxis und arbeiten Strategien zum knacken der Codes aus.

Somit verbindet das Seminar historische, sprachwissenschaftliche und mathematisch-naturwissenschaftliche Inhalte sowie Gebiete der Informatik in einem spannenden Kontext, was die Möglichkeit für eine sehr individuelle Auswahl des Seminararbeitsthemas bietet.

Neben benötigten fachlichen Kenntnissen aus dem Gebiet der Kryptographie und der Mathematik erarbeiten wir außerdem den korrekten Aufbau einer wissenschaftlichen Arbeit und lernen verschiedene Techniken zur Erstellung eines naturwissenschaftlichen Textes kennen, welche schließlich alle zusammen für die Erstellung der Seminararbeit angewendet werden müssen.

Mögliche Themen für die Seminararbeiten:

1. Entschlüsselung eines Textes mit Hilfe der Häufigkeitsanalyse
2. Das Vignère-Verfahren: Ermittlung eines Schlüsselwortes
3. Der Friedmann Angriff
4. One Time Pad: Erzeugung eines Zufallsschlüssels
5. Funktionsweise einer „Bombe“- Ermittlung des Tagesschlüssels der Enigma
6. Turing und Cribs: Reduzierung der Möglichkeiten
7. Linear B: Entschlüsselung einer alten Schrift
8. Das Diffie-Hellman-Merkle-Verfahren
9. RSA und PGP
10. Quantenkryptographie-Ein Ausblick

Weitere Bemerkungen zum geplanten Verlauf des Seminars: