Kurzbeschreibung zur **Wahl** des **W-Seminars** im Fach Mathematik

Lehrkraft: OStR Horneber — Leitfach: Mathematik

Rahmenthema: Kryptologie

Zielsetzung des Seminars:

„Kryptographie bzw. **Kryptografie** (altgr. κρυπτός *kryptós* ‚verborgen', ‚geheim' und γράφειν *gráphein* ‚schreiben') war ursprünglich die Wissenschaft der Verschlüsselung von Informationen. Heute befasst sie sich allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen unbefugtes Lesen und Verändern sind. Die Kryptographie bildet zusammen mit der Kryptoanalyse (auch: *Kryptanalyse*) die Kryptologie." (Quelle: Wikipedia)

Mobiltelefongespräche werden zumindest schwach verschlüsselt. Emails können je nach Sicherheitsbedürfnis des Senders beliebig stark verschlüsselt werden. Texte können mit einer digitalen Signatur versehen werden. Das sind Beispiele für moderne Anwendungen der Kryptographie. Zur Entwicklung, Implementierung und Testung solcher modernen Verfahren ist höhere und bisweilen sehr schwierige sog. reine Mathematik nötig, von der man vor 100 Jahren noch dachte, dass sie nicht zu Anwendungen zu gebrauchen sei.

Die Mathematik, die in Verfahren steckt, die in Kriegen von der Armee und im kalten Krieg von Spionen benutzt wurden ist weniger schwer zu verstehen.

Es ist also ein Leichtes, Themen zu vergeben, die jeden Schüler an die Grenzen seines mathematischen Verständnisses und deshalb zu individuellem Erkenntnisgewinn führen werden.

Außerdem wird den Schülern klar, dass sogar höhere abstrakte Mathematik nützlich ist, in Technischen Systemen geradezu allgegenwärtig ist und je komplizierter und schwieriger sie ist, desto weniger bemerkt sie der Anwender.

Mögliche Themen für die Seminararbeiten:

Papier und Stift Verfahren
- Spionage-Chiffren
- Playfair-Verfahren

Asymetrische Verfahren
- Diffie – Hellman Verfahren
- RSA Verfahren

Kryptographie, die nicht zur Geheimhaltung von Kommunikation dient
- Digitale Signatur
- Authentifizierung
- Zero-Knowledge-Verfahren

- Die Enigma

…etc., viele weitere Themen nach Absprache.