W-Seminar im Fach
Informatik

Lehrkraft: Werner Schmauser **Leitfach: Informatik**

Rahmenthema: Verschlüsselung von Nachrichten

Zielsetzung des Seminars, Begründung des Themas:

K p h q t o c v k m

Diesen Geheimtext kann man vielleicht noch entschlüsseln – wie einst Julius Caesar. Neue Methoden garantieren, dass diese Verfahren viel sicherer sind als Buchstaben immer nur um 2 zu verschieben…

Im Zeitalter digitaler Nachrichtenkommunikation werden Informationen zunehmend über das Internet ausgetauscht. Auf ihrem Weg über die Vermittlungsrechner zum Empfänger sind digitale Nachrichten so unsicher wie Postkarten; sie können unerlaubt gelesen oder sogar verfälscht werden.

In diesem Seminar werden Schutzmechanismen vor derartigen Eingriffen näher beleuchtet. Die Inputphase widmet sich zunächst klassischen Verschlüsselungstechniken, wie z. B. der Cäsar-Verschlüsselung. Anschließend erfolgt eine Einführung in die mathematischen Grundlagen moderner Techniken wie RSA.

Die Sicherheit der modernen Verschlüsselungstechniken beruht auf Ergebnissen der Komplexitätstheorie der theoretischen Informatik: Für Programme, die verschlüsselte Nachrichten angreifen, kann der nötige Rechenaufwand so stark erhöht werden, dass der Versuch einer unberechtigten Entschlüsselung zu (zeit-)aufwändig wird. Die Ergebnisse der theoretischen Informatik belegen, dass auch eine noch so rasante Entwicklung der Rechenleistung eine wirksame Verschlüsselung nicht gefährden kann.

Ein Hauptaugenmerk der Seminararbeiten und insbesondere der Präsentationen liegt auf einer **verständlichen Darstellung** der zugrunde liegenden Informatik- oder Mathematik-Konzepte. In diesem Seminar werden den Schüler(inne)n grundlegende Arbeitstechniken für das Studium von mathematisch-naturwissenschaftlichen Fachrichtungen vermittelt.

Das Seminar eignet sich zur fachübergreifenden Zusammenarbeit mit Mathematik.

Mögliche Themen für die Seminararbeiten:

1. Darstellung historischer Verschlüsselungsverfahren
2. Umsetzung klassischer Verschlüsselungstechniken in Programmen, z. B. Caesar-Verschlüsselung
3. Vigenère-Chiffre und dessen Kryptoanalyse
4. Die Enigma
5. Der RSA-Algorithmus
6. Verschlüsselung und Primzahlen
7. Nachrichtenübermittlung im Internet
8. Wie sicher ist Home-Banking?
9. Die Turingmaschine als einfaches Modell zur Ermittlung der Zeitkomplexität

Gewählte Themen:

- Entschlüsselung alter Sprachen
- Handy-Sicherheit
- Der DES-Algorithmus
- Sicherheit von Online-Banking
- Die Enigma
- Die Digitale Unterschrift
- RFID – Technik, Anwendungen und Risiken
- Der RSA-Algorithmus
- Viren, Würmer und Trojaner
- Kryptographie im Automobil
- Verschlüsselung von WLAN-Netzwerken
- Verschlüsselungssoftware – Funktionsweise und Sicherheit