

Workshop: Codierungstheorie und Kryptographie

In diesem Kurs beschäftigten wir uns mit Grundlagen der Codierungstheorie und der Kryptographie. Unter Codierung versteht man die Darstellung von Information in anderer Form. Die Gründe für die Wahl einer anderen Form können vielfältig sein. Einerseits können Informationen durch Codierungen überhaupt erst technisch verarbeitbar oder für bestimmte Personengruppen verständlich werden, andererseits kann Codierung die Geheimhaltung von Information bewirken. Gerade in der heutigen Zeit spielt die Sicherheit bei der Informationsübertragung eine immer größere Rolle.

Immer mehr Menschen sind weltweit über Rechnernetze verbunden und nutzen diverse Möglichkeiten, Daten über Netze auszutauschen. Dabei handelt es sich oft um 'geheime' Daten. Deshalb passiert es, dass zum Beispiel aus Konkurrenzgründen oder einfach aus Neugierde Information von Dritten abgefangen oder auch verfälscht werden. Ziel einer Verschlüsselung ist es, dass abgefangene Information nicht entschlüsselt werden kann oder der Empfänger eine Verfälschung der eigentlichen Nachricht erkennt. Die Kryptologie stellt verschiedene Methoden zur Geheimhaltung von Daten und zur sicheren Nachrichtenübertragung zur Verfügung.

Dauer: Nach Aufgabenstellung und in Absprache

Empfohlene Voraussetzungen: Der Trainingsinhalt ist variabel und lässt sich auf die individuellen Bedürfnisse der Teilnehmer anpassen.

Inhalte:

- **Alltägliche Codes (ISBN, Barcodes, Nummerierung von Geldscheinen)**
- **Mathematische Grundlagen der Codierungstheorie**
- **spezielle Codes**
- **Sicherheit in Rechnernetzen**
- **Grundlagen der Kryptographie**
- **Kryptographische Systeme**
- **Der RSA-Algorithmus**