Prof. Dr. Andreas Aßmuth
Rechnernetze und Mathematik

OTH Amberg-Weiden
Kaiser-Wilhelm-Ring 23
92224 Amberg
☎ +49 (9621) 482 - 3604
✉ a.assmuth@oth-aw.de
https://www.andreas-assmuth.de

Kryptologie I

Zielsetzung:

Die Studierenden kennen die Grundlagen ausgewählter moderner Verschlüsselungs- und Signaturschemata, Hashfunktionen und Message Authentication Codes. Sie können ausgewählte Verfahren anwenden und deren kryptographische Stärke bewerten, sie kennen praktische Anwendungen von kryptographischen Primitiven und Protokollen.

Inhalte:

Grundbegriffe, Einführung in die Mathematik-Software SAGE, historische Verschlüsselungsverfahren, modulare Arithmetik, Sicherheitsbegriffe in der Kryptologie, Stromchiffren, Blockchiffren, kryptographische Hashfunktionen, Message Authentication Codes und Public Key-Kryptographie.

Hintergrund/Motivation:

Moderne Kryptographie ist die Wissenschaft, die sich mit Methoden und Verfahren zur Sicherung digitaler Informationen, Transaktionen und verteilten Berechnungen beschäftigt. Während früher der Schutz vertraulicher Daten durch Verschlüsselung die Hauptaufgabe der Kryptologie war, hat sie in Zeiten des Internets und der elektronischen Kommunikation an Bedeutung gewonnen und muss darüber hinaus weitere Aufgaben erfüllen: z. B. Authentifizierung, Identifikation, digitale Signaturen, elektronisches Geld oder auch das sichere Abspeichern von Benutzerpasswörtern. In jüngerer Vergangenheit bekamen einige Internetnutzer jedoch auch negative Auswirkungen der Kryptographie zu spüren: Ransomware oder „Krypto-Trojaner" sind Schadsoftware, die die Dateien eines Benutzers verschlüsseln, um diesen zu erpressen. Gegen die Bezahlung eines bestimmten Betrags in Bitcoins erhält er/sie (angeblich) die benötigten Schlüssel, um wieder Zugriff auf die eigenen Dateien zu erhalten.

In der Lehrveranstaltung „Kryptologie I" steht die moderne Kryptographie im Vordergrund. Strom- und Blockchiffren werden im Wesentlichen zur Verschlüsselung von Massendaten eingesetzt. Public-Key-Verfahren dienen der Vereinbarung von Sitzungsschlüssel oder der Erzeugung und Verifikation von elektronischen Signaturen. Die für das Verständnis moderner kryptographischer Primitive benötigten mathematischen Verfahren werden im Rahmen der Lehrveranstaltung anhand einfach nachvollziehbarer historischer Verfahren anschaulich eingeführt.

Die Vorlesungen finden im Rechnernetze-Labor (EMI 205) statt und sind so angelegt, dass die Studierenden mit den besprochenen Lerninhalte unmittelbar am Computer arbeiten sollen. Das praktische Anwenden der kryptographischen Primitive und Protokolle bzw. das selbständige Berechnen führt zu einem besseren Verständnis der Thematik. Die begrenzte Anzahl von Sitzplätzen/PCs führt allerdings auch zu einer Beschränkung der Teilnehmeranzahl.

Umfang:

4 SWS, 5 LP

Voraussetzungen:

Grundkenntnisse der Programmierung (vorzugsweise in Python) sind hilfreich. Keine Sorge wegen der Mathematik! Es wird außer den Grundrechenarten nichts vorausgesetzt, alles weitere wird anhand konkreter Beispiele erklärt.

Prüfung:

Die Prüfungsleistung wird in Form einer mündlichen Prüfung am letzten Vorlesungstermin des Semesters erbracht.