Wichtige Basiskonzepte moderner Kryptographie werden vorgestellt. Hierzu gehören Verschlüsselungsverfahren, digitale Signaturen, Identifikationsprotokolle und Mehrparteienberechnungen. In allen Fällen werden formale Sicherheitsdefinitionen vorgestellt und, ausgehend von mathematisch präzisen Annahmen, beweisbar sichere Konstruktionen entwickelt. Der Fokus der Veranstaltung liegt auf der Vorstellung der Techniken die modernen Kryptosystemen und deren Sicherheitsbeweisen zugrunde liegen.

Der Kurs hat eine starke mathematische Prägung. Hauptbestandteil sind die mathematischen Formulierungen diverser Konzepte aus der Kryptographie und die Korrektheitsbeweise kryptographischer Verfahren.

Empfohlene Voraussetzungen:
- Grundkenntnisse in Komplexitätstheorie
- Grundkenntnisse in Wahrscheinlichkeitstheorie

Kenntnisse in Algebra, IT-Sicherheit und Kryptographie sind hilfreich aber nicht notwendig.

Lernziel:

Studierende kennen und verstehen etablierte Konzepte und Methoden moderner Kryptographie. Sie sind in der Lage Sicherheitsanforderungen formal zu definieren, kennen die etablierten Standard-Definitionen sowie deren Grenzen und sind in der Lage die Eigenschaften und Wechselwirkungen dieser Definitionen formal zu analysieren.

Vorgehen:

Die Vorlesung besitzt einen integrierten Übungsanteil. Hierfür haben die Teilnehmer in Heimarbeit Übungsaufgaben zu bearbeiten. Die Lösungen werden anschließend in der Vorlesung an der Tafel von den Studenten präsentiert und zusammen diskutiert. Die Bearbeitung der Übungsaufgaben sowie deren Präsentation und Diskussion sind Teil der Studienleistung.

Seminar
Das zum Modul gehörende Seminar findet geblockt gegen Ende des Semesters statt. Der genaue Termin wird mit den Studierenden abgestimmt. Weitere Details zum Ablauf des Seminars werden in der ersten Vorlesungseinheit besprochen.

Literatur:

Der Kurs basiert großteils auf dem Buch "Lindell, Yehuda and Katz, Jonathan. Introduction to Modern Cryptography. Chapman and Hall/CRC, 2014.". Weitere Literatur wird gegebenenfalls in der Vorlesung bekannt gegeben.

Zusätzliche Hinweise zu Prüfungen:

Die Modulprüfung findet voraussichtlich als mündliche Prüfung statt. Sollte die Anzahl der Teilnehmer unerwartet hoch sein, wird gegebenenfalls auf eine schriftliche Klausur zurückgegriffen. Dies wird in der ersten Vorlesungsstunde besprochen.