Modulbeschreibung
39-Inf-KRY Kryptographie

Technische Fakultät

Version vom 23.06.2026

Dieses Modulhandbuch gibt den derzeitigen Stand wieder und kann Änderungen unterliegen. Aktuelle Informationen und den jeweils letzten Stand dieses Dokuments finden Sie im Internet über die Seite

https://ekvv.uni-bielefeld.de/sinfo/publ/modul/94014089

Die jeweils aktuellen und gültigen Regelungen im Modulhandbuch sind verbindlich und konkretisieren die im Verkündungsblatt der Universität Bielefeld veröffentlichten Fächerspezifischen Bestimmungen.

39-Inf-KRY Kryptographie

Fakultät

Technische Fakultät

Modulverantwortliche*r

Dr. Dirk Frettlöh

Turnus (Beginn)

Auslaufend

Leistungspunkte

5 Leistungspunkte

Kompetenzen

Es werden Kenntnisse vermittelt, um Methoden aus Informatik und Mathematik zur Implementierung von kryptographischen Verfahren zu verstehen und zu nutzen (Primzahltests, Einwegfunktionen, Hashfunktionen, Zufallszahlen auf dem Computer).
Zudem lernen die Studierenden grundlegende Verschlüsselungs-Protokolle anzuwenden und ihre Schwächen und Stärken nachzuweisen (Passwort, Challenge-and-Response, No-Key-Protokolle, Zero-Knowledge, Multiparty, Signaturen)

Lehrinhalte

- Klassische Codes, RSA, Diffie-Hellman, ElGamal, Zero-Knowledge
- Einwegfunktionen, Zufallszahlen, Primzahltests, Codierungstheorie
- Anwendung auf Multiparty, Anonymität, Signaturen

Empfohlene Vorkenntnisse

–

Notwendige Voraussetzungen

Vorausgesetzte Module:
24-M-INF1: Mathematik für Informatik I
24-M-INF2: Mathematik für Informatik II

Erläuterung zu den Modulelementen

Die Modul(teil)prüfung kann in einigen Studiengängen nach Wahl der Studierenden auch "unbenotet" erbracht werden. Vor Erbringung ist eine entsprechende Festlegung vorzunehmen, eine nachträgliche Änderung (benotet - unbenotet) ist

ausgeschlossen. Wird diese Option gewählt, ist es nicht möglich, dieses Modul zu verwenden, um es in einen Studiengang einzubringen, in dem dieses Modul bei der Gesamtnotenberechnung berücksichtigt wird.

Modulstruktur: 0-1 bPr, 0-1 uPr [1]

Veranstaltungen

Titel	Art	Turnus	Workload [5]	LP[2]
Kryptographie	Vorlesung	SoSe	60 h (30 + 30)	2
Übungen zu Kryptographie	Übung	SoSe	60 h (30 + 30)	2

Prüfungen

Zuordnung Prüfende	Art	Gewichtung	Workload	LP[2]
Modulverantwortliche*r prüft oder bestimmt Prüfer*in *In einigen Studiengängen der Technischen Fakultät kann die Modulteilprüfung nach Wahl der Studierenden auch "unbenotet" erbracht werden (s. Erläuterungen zu den Modulelementen und die jeweilige FsB). Wird die unbenotete Option gewählt, ist es nicht möglich, dieses Modul zu verwenden, um es in einen Studiengang einzubringen, in dem dieses Modul bei der Gesamtnotenberechnung berücksichtigt wird.* *Erläuterungen zu dieser Prüfung siehe unten (benotete Prüfungsvariante).*	Portfolio mit Abschlussprüfung	unbenotet	30h	1
Modulverantwortliche*r prüft oder bestimmt Prüfer*in *Portfolio aus Übungsaufgaben, die veranstaltungsbezogen gestellt werden (Bestehensgrenze 50% der erzielbaren Punkte) und Abschlussklausur (mit einem zeitlichen Rahmen von ca. 90 Minuten) oder mündlicher Abschlussprüfung (mit einem zeitlichen Rahmen von ca. 30 Minuten).* *Die Kontrolle der Aufgaben umfasst auch direkte Fragen zu den Lösungsansätzen, die von den Studierenden in den Übungen beantwortet werden müssen. Die Veranstalterin/der Veranstalter kann ein individuelles Erläutern und Vorführen von Aufgaben verlangen sowie einen Teil der Aufgaben durch Präsenzübungen ersetzen.* *Die Aufgaben im Rahmen des Portfolios werden in der Regel wöchentlich ausgegeben.*	Portfolio mit Abschlussprüfung	1	30h	1

Weitere Hinweise

Bei diesem Modul handelt es sich um ein auslaufendes Angebot. Dieses Modul richtet sich nur noch an Studierende, die nach einer der nachfolgend angegebenen FsB Versionen studieren. Ein entsprechendes Angebot, um dieses Modul abzuschließen, wird bis maximal Sommersemester 2028 vorgehalten. Genaue Regelungen zum Geltungsbereich s. jeweils aktuellste FsB-Fassung.
Bisheriger Angebotsturnus war jedes Sommersemester.

Legende

1 Die Modulstruktur beschreibt die zur Erbringung des Moduls notwendigen Prüfungen und Studienleistungen.

2 LP ist die Abkürzung für Leistungspunkte.

3 Die Zahlen in dieser Spalte sind die Fachsemester, in denen der Beginn des Moduls empfohlen wird. Je nach individueller Studienplanung sind gänzlich andere Studienverläufe möglich und sinnvoll.

4 Erläuterungen zur Bindung: "Pflicht" bedeutet: Dieses Modul muss im Laufe des Studiums verpflichtend absolviert werden; "Wahlpflicht" bedeutet: Dieses Modul gehört einer Anzahl von Modulen an, aus denen unter bestimmten Bedingungen ausgewählt werden kann. Genaueres regeln die "Fächerspezifischen Bestimmungen" (siehe Navigation).

5 Workload (Kontaktzeit + Selbststudium)

SoSe Sommersemester

WiSe Wintersemester

SL Studienleistung

Pr Prüfung

bPr Anzahl benotete Modul(teil)prüfungen

uPr Anzahl unbenotete Modul(teil)prüfungen