Modulbeschreibung
24-M-ND-CRY Kryptographie

Fakultät für Mathematik

Version vom 23.04.2026

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/533559415

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

24-M-ND-CRY Kryptographie

Fakultät

Fakultät für Mathematik

Modulverantwortliche*r

PD Dr. Barbara Baumeister

Turnus (Beginn)

Dieses Modul ist Teil einer langfristigen Gesamtlehrplanung für das Masterprogramm, die sicherstellt, dass in allen fünf Gebieten jedes Jahr jeweils mindestens Module im Umfang von 20 LP angeboten werden. Im Rahmen dieser Gesamtlehrplanung wird das Modul in unregelmäßigen Abständen angeboten.

Leistungspunkte

10 Leistungspunkte

Kompetenzen

Die Studieren beherrschen weiterführende Inhalte und Methoden der Kryptographie, insbesondere können sie selbstständig sehr komplexere und ein hohes Maß an fachlichen Kompetenzen erfordernde Beweise in diesem Gebiet führen. Die Studierenden sind in der Lage, zentrale Begriffe der Theorie zu definieren und im Kontext anzuwenden. Sie können Methoden aus verschiedenen Bereichen der Kryptographie in verschiedenen Zusammenhängen anwenden.

Die Studierenden werden im Bereich Kryptographie an aktuelle Forschungsfragen herangeführt. Sie können weitere Entwicklungsmöglichkeiten und Forschungsziele erfassen und einschätzen.
Ferner erkennen die Studierende weiter reichende Zusammenhänge zu bereits erarbeiteten mathematischen Sachverhalten. Sie können die bislang erlernten Kenntnisse und Methoden auf tiefer liegende mathematische Problemfelder übertragen und anwenden. Aufgrund einer intensiveren Auseinandersetzung erweitern die Studierende auch ihre mathematische Intuition.
Sie werden im Zusammenspiel mit weiteren vertiefenden Modulen fachlich und methodisch in der Lage sein, im Anschluss eigene Forschungsarbeiten, z. B. eine Masterarbeit im Bereich Kryptographie zu verfassen.
In den Übungen bauen die Studierende ihre Fähigkeit zur fachmathematischen Diskussion aus und bereiten sich so weiter auf die Anforderungen des Mastermoduls, insbesondere auf die fachliche Diskussion im Rahmen des Masterseminarvortrags und die Verteidigung ihrer Masterarbeit, vor.

Lehrinhalte

Die folgenden Lehrinhalte aus dem Bereich Kryptographie sind vorgesehen:

- Eine Auswahl aus den Grundlagen der Kryptographie und historische Beispiele
- Komplexität und Zahlentheorie
- Sicherheit
- Symmetrische Verfahren (AES)
- Asymmetrische Verfahren (RAS, ElGamal, Diffie-Hellman)

- Primzahltests (einige, AKS)
- Faktorisierung ganzer Zahlen
- Der diskrete Logarithmus
- elliptische Kurven
- Signaturen
- Hash-Funktionen
- Kryptographie mit Gittern.

Dieses Modul bereitet inhaltlich eine Masterarbeit vor.

Empfohlene Vorkenntnisse

Kenntnisse der Codierungstheorie (24-M-ND-CTH)

Notwendige Voraussetzungen

–

Erläuterung zu den Modulelementen

Modulstruktur: 1 SL, 1 bPr [1]

Veranstaltungen

Titel	Art	Turnus	Workload [5]	LP [2]
Lecture Cryptography	Vorlesung	Dieses Modul ist Teil einer langfristigen Gesamtlehrplanung für das Masterprogramm, die sicherstellt, dass in allen fünf Gebieten jedes Jahr jeweils mindestens Module im Umfang von 20 LP angeboten werden. Im Rahmen dieser Gesamtlehrplanung wird das Modul in unregelmäßigen Abständen angeboten.	60 h (60 + 0)	2 [Pr]

Tutorials Cryptography	Übung	Dieses Modul ist Teil einer langfristigen Gesamtlehrplanung für das Masterprogramm, die sicherstellt, dass in allen fünf Gebieten jedes Jahr jeweils mindestens Module im Umfang von 20 LP angeboten werden. Im Rahmen dieser Gesamtlehrplanung wird das Modul in unregelmäßigen Abständen angeboten.	90 h (30 + 60)	3 [SL]

Studienleistungen

Zuordnung Prüfende	Workload	LP[2]
Lehrende der Veranstaltung **Tutorials Cryptography (Übung)** *Regelmäßiges Bearbeiten der Übungsaufgaben, jeweils mit erkennbarem Lösungsansatz sowie die Mitarbeit in den Übungsgruppen zu der Vorlesung des Moduls. Zu der Mitarbeit in der Übungsgruppe gehören in der Regel das zweimalige Vorrechnen von Übungsaufgaben nach Aufforderung sowie regelmäßige Beiträge zur fachlichen Diskussion in der Übungsgruppe, etwa in Form von fachlichen Kommentaren und Fragen zu den vorgestellten Lösungsvorschlägen. Die Veranstalterin/der Veranstalter kann einen Teil der Übungsaufgaben durch Präsenzübungen ersetzen.*	siehe oben	siehe oben

Prüfungen

Zuordnung Prüfende	Art	Gewichtung	Workload	LP[2]
Lehrende der Veranstaltung **Lecture Cryptography (Vorlesung)** *(elektronische) Klausur in Präsenz von in der Regel 120 Minuten, mündliche Prüfung in Präsenz oder auf Distanz von in der Regel 40 Minuten. Eine elektronische Klausur auf Distanz ist nicht zulässig.*	e-Klausur o. Klausur o. mündliche e-Prüfung o. mündliche Prüfung	1	150h	5

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