**Modulbeschreibung**

| | | | |
|---|---|---|---|
| 1 | **1.1 Modulbezeichnung (dt. / engl.)**<br>Grundlagen der Kryptographie | **1.2 Kurzbezeichnung (optional)** | **1.3 Modul-Code** (aus HIS-POS) |
| 2 | **2.1 Modulturnus:**<br>**Angebot in ☐ jedem SoSe, ☒ jedem WiSe, anderer Turnus, nämlich:** | **2.2 Moduldauer:**<br>**☒ 1 Semester ☐ 2 Semester** | |
| 3 | **3.1 Angebot für folgenden Studiengang/folgende Studiengänge** | **3.2 Pflicht, Wahlpflicht, Wahl** | **3.3 Empfohlenes Fachsemester** |
| | Bachelor Informatik (auch dual) | Wahlpflicht | 5 |
| | Bachelor Elektrotechnik (auch dual) | Wahl | 5 |

**4 Workload**

| | | | | Workload insgesamt | |
|---|---|---|---|---|---|
| | **Lehrformen/ Form** | **SWS je Lehrform** | **Std. pro Semester je Lehrform/ angegebener Form**<br>1 SWS darf als 15 Zeitstunde angesetzt werden, d. h. 1 SWS = 1 UStd. x 15 Semesterwochen | **Arbeitsaufwand in Std. (Workload)**<br>Summe Kontaktzeit + Summe Selbststudium in Std. | **Leistungspunkte (Credits)**<br>i. d. R. 30 Std. = 1 LP; nur ganze Zahlen zulässig! |
| **Kontaktzeit**<br>(z. B. Vorlesung, Übung, Praktikum, seminaristischer Unterricht, Projekt-/ Gruppenarbeit, Fallstudie, Planspiel, kreditiertes Tutorium) (weitere Zeilen möglich) | Vorlesung | 2 | 30 | | |
| | Praktikum | 2 | 30 | | |
| | | | | | |
| | | | | | |
| | **Summen** | Summe Kontaktzeit in SWS<br>4 | Summe Kontaktzeit in Std.<br>60 | **150** | **5** |
| **Selbststudium**<br>(z. B. Tutorium, Vor-/ Nachbereitung, Prüfungsvorbereitung, Ausarbeitung von Hausarbeiten, Recherche) | Vor-/Nachbereitung und Prüfungsvorbereitung | | 90 | | |
| | | | | | |
| | | | | | |
| | **Summen** | | Summe Selbststudium in Std.<br>90 | | |

**5 5.1 Lernziele** (Was sollen Studierende nach Abschluss des Moduls können? Bietet das Modul neben fachlichen Lernzielen Gelegenheiten, außerfachliche Kompetenzen zu entwickeln? Wofür sind die beschriebenen Ziele relevant (z. B. Voraussetzung für weitere Studienelemente oder für bestimmte berufliche Tätigkeiten)?)

Entwickelte Fachkompetenz:
Die Studierenden können kryptographische Verfahren für verschiedene Anwendungen spezifizieren und die Sicherheit dieser Verfahren beurteilen.

Die Studierenden erlernen die Unterschiede und Besonderheiten der kryptographischen Verfahren und Algorithmen.

Die Studierenden lernen weiterhin die wichtigsten Aspekte der zu Grunde liegenden Mathematik der kryptographischen Algorithmen sowie die interne Funktionsweise der Algorithmen.

In dem Praktikum erlernen die Studierenden den Umgang mit den gängigen kryptographischen Softwaretools (z.B. Cryptool, Cyberchef) und Krypto-Bibliotheken (z.B. OpenSSL) um die Verfahren auch in der Praxis nutzen zu können.

Entwickelte Sozialkompetenz:
Die Studierenden können sich in die Angreiferrolle reinversetzen um zu entscheiden welche kryptographischen Verfahren für verschiedene Anwendungen benötigt werden. In den Praktika können sich die Studierenden gegenseitig unterstützen und bei Problemen untereinander Hilfestellungen geben.

Entwickelte Selbstkompetenz:
Die Studierenden beteiligen sich an Diskussionen in der Vorlesung und lernen in den Praktika selbstverantwortlich Aufgaben zu bearbeiten.

Entwickelte Methodenkompetenz:
Die Studierenden sind in der Lage selbstständig die passenden kryptographischen Verfahren sowie die zu benutzenden Tools auszusuchen und kritisch auf Ihre Eignung zu evaluieren.

**5.2 Lerninhalte**

Inhaltlich werden die folgenden Themen besprochen:

- Geschichte der Kryptographie: Warum wurde die Kryptographie überhaupt entwickelt und wie war die weitere Entwicklung bis heute
- Symmetrische Verschlüsselung (z.B. AES, Streamcipher, Modi)
- Asymmetrische Verschlüsslung (z.B. RSA, Elliptische-Kurven-Kryptographie)
- Schlüsselaustausch zwischen zwei Parteien
- Hashalgorithmen

→ zu den Details: siehe Vorlesungsverzeichnis, Lehrveranstaltungsplan etc.

5 **5.3 Modulkurzinformation** (Dieser Absatz [max. 250 Zeichen] wird auf der FH-Webseite veröffentlicht, um Studieninteressierte bei der Wahl ihres Studiengangs zu unterstützen. Fokussieren Sie sich auf wesentliche Inhalte und Ziele, gern verbunden mit Aussagen zur Bedeutung des Moduls für das weitere Studium oder berufliche Tätigkeiten. Bitte formulieren Sie ganze Sätze, sprechen Sie die Adressaten direkt an und vermeiden Sie Fachtermini.)

Die Kryptographie ist der Grundbaustein für sichere digitale Systeme, online im Netz als auch offline.
In diesem Modul lernen Sie die verschiedenen kryptographischen Verfahren und Ihre Anwendungsgebiete kennen. Sie erlernen dazu die wichtigsten mathematischen internen Prinzipien, die für die kryptographischen Algorithmen benötigt werden.

6 **6.1 Teilnahmevoraussetzungen** (*Formal:* Prüfung in Modul XY muss bestanden sein o. ä.; *Inhaltlich:* Modul XY sollte absolviert sein, folgende Kenntnisse sollten vorhanden sein, …)

**6.2 Voraussetzungen für die Vergabe von Leistungspunkten** (z. B. Bestehen der Prüfung, erfolgreicher Abschluss einer Studienleistung, regelmäßige und aktive Teilnahme)

Bestehen der Klausur

**6.3 Prüfungsformen und -umfang** (z. B. Klausur, mündliche Prüfung, Hausarbeit, Präsentation, Portfolio, Dauer der Prüfung in Min.)

In der Regel 120 min, in Ausnahmefällen mdl. Prüfung (30 min)

**6.4 Voraussetzungen für die Zulassung zur Prüfung**

Erfolgreiche Teilnahme am Praktikum

**6.5 Gewichtung der Note bei Ermittlung der Endnote**

s. Prüfungsordnung/ -en für oben (Zeile 3) genannte Studiengänge*

*Die Prüfungsordnungen der Studiengänge finden Sie in den Amtlichen Bekanntmachungen der FH Münster unter dem folgenden Link https://www.fh-muenster.de/hochschule/aktuelles/amtliche_bekanntmachungen/index.php?p=2,7.

7 **7.1 Veranstaltungssprache/n**

☒**Deutsch** ☐ **Englisch** ☐ **Weitere, nämlich:**

**7.2 Modulverantwortliche/r**

Prof. Dr. Christoph Saatjohann

**7.3 Hauptamtlich Lehrende (optional)**

**7.4 Maximale Teilnehmerzahl (optional)**

**7.5 Ergänzende Informationen (optional)** (z. B. Literaturempfehlungen, weitere beteiligte Personen etc.)

Literaturempfehlung:
Understanding Cryptography - From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms, 2. Auflage, 2024
(Online für FH Münster-Angehörige verfügbar: https://link-springer-com.ezproxy.fh-muenster.de/book/10.1007/978-3-662-69007-9)