Modulbeschreibung

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

4 Workload

				Workload insgesamt	
	Lehrformen/ Form	**SWS je Lehrform**	**Std. pro Semester je Lehrform/ angegebener Form** 1 SWS darf als 15 Zeitstunde angesetzt werden, d. h. 1 SWS = 1 UStd. x 15 Semesterwochen	**Arbeitsaufwand in Std. (Workload)** Summe Kontaktzeit + Summe Selbststudium in Std.	**Leistungspunkte (Credits)** i. d. R. 30 Std. = 1 LP; nur ganze Zahlen zulässig!
Kontaktzeit (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 4	Summe Kontaktzeit in Std. 60	**150**	**5**
Selbststudium (z. B. Tutorium, Vor-/ Nachbereitung, Prüfungsvorbereitung, Ausarbeitung von Hausarbeiten, Recherche)	Vor-/Nachbereitung und Prüfungsvorbereitung		90		
	Summen		Summe Selbststudium in Std. 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 effizient und sicher implementieren. Sie kennen die wichtigsten Algorithmen für verschiedene Verfahren in der Kryptographie.
Sie können kryptographische Implementierungen auf Ihre Sicherheit und Effizienz hin theoretisch und praktisch evaluieren.

Entwickelte Sozialkompetenz:
Die Studierenden können Pro- und Contra-Abwägungen durchführen und in der Gruppe vorstellen und diskutieren. Sie können Ihre eigenen Arbeiten in der Gruppe präsentieren und praktisch in einer Live-Umgebung demonstrieren.

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 Algorithmen für die benötigten Anforderungen auszusuchen und kritisch auf Ihre Eignung zu evaluieren.

5.2 Lerninhalte

Inhaltlich werden die folgenden Themen besprochen:

- Messen einer Implementierung eines kryptographischen Verfahrens (Bspw. Geschwindigkeit, Größe, Sicherheit)
- Algorithmische „Tricks“: Wie beeinflusst die Wahl der Algorithmus-Parameter die Geschwindigkeit der Ausführung (Bsp. RSA-Exponent, ECC-Kurvenparameter)
- Trade-off zwischen Geschwindigkeit und Speicherbedarf (Bspw. Lookup-Tabellen)
- Einfluss der Algorithmen auf die Sicherheit des Systems (Bspw. „Seitenkanalangriffe“)
- Geschicktes Ausnutzen der Hardwareeigenschaften (Bspw. Division durch Bitshift, „Bit-Slicing“)

→ 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 Implementierung kryptographischer Verfahren ist entscheidend für die Gesamtperformance und Sicherheit aller digitalen Systeme.
In diesem Modul lernen Sie verschiedene Möglichkeiten kryptographische Algorithmen zu implementieren und insbesondere hinsichtlich Geschwindigkeit, Größe und Sicherheit einzuschätzen.

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 Prüfung

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

Mündliche 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)

12

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

Literaturempfehlung:

Menzes, van Oorshot, Vanstone: Handbook of Applied Cryptography, 2001 (online verfügbar: https://cacr.uwaterloo.ca/hac/)

Hankerson, Vanstone, Menezes: Guide to Elliptic Curve Cryptography, 2004