Modulbezeichnung:	**Einführung in die Kryptografie (Krypto)** (Introduction To Cryptography)	**5 ECTS**
Modulverantwortliche/r:	Marc Spisländer	
Lehrende:	Marc Spisländer, Xiaochen Wu	

Startsemester: WS 2021/2022	Dauer: 1 Semester	Turnus: jährlich (WS)
Präsenzzeit: 30 Std.	Eigenstudium: 120 Std.	Sprache: Deutsch

Lehrveranstaltungen:

Einführung in die Kryptografie (WS 2021/2022, Seminar, 2 SWS, Anwesenheitspflicht, Marc Spisländer et al.)

Inhalt:

In diesem Seminar werden symmetrische und asymmetrische Verfahren zur Identifikation, Verschlüsselung und Signierung behandelt. Dazu werden sowohl die mathematischen Grundlagen vermittelt als auch die entsprechenden Algorithmen vorgestellt.

Lernziele und Kompetenzen:

Die Studierenden

- erläutern wesentliche Konzepte der modernen Kryptografie;
- klassifizieren Kryptoverfahren und charakterisieren deren Stärken und Schwächen;
- tragen vor Publikum über wissenschaftliche Ergebnisse vor;
- recherchieren selbständig Fachliteratur;
- fassen wissenschaftliche Erkenntnisse in Schriftform zusammen;
- nutzen Verbesserungshinweise des Betreuers zur Analyse eigener Stärken und Schwächen und leiten daraus Konsequenzen für ihr künftiges Lern-Handeln ab;
- können komplexe fachbezogene Inhalte klar und zielgruppengerecht präsentieren und argumentativ vertreten.

Verwendbarkeit des Moduls / Einpassung in den Musterstudienplan:

Das Modul ist im Kontext der folgenden Studienfächer/Vertiefungsrichtungen verwendbar:

[1] **Computational Engineering (Rechnergestütztes Ingenieurwesen) (Bachelor of Science)**
(Po-Vers. 2010 | TechFak | Computational Engineering (Rechnergestütztes Ingenieurwesen) (Bachelor of Science) | Gesamtkonto | Seminar Informatik für CE | Seminar Einführung in die Kryptografie)

[2] **Computational Engineering (Rechnergestütztes Ingenieurwesen) (Master of Science)**
(Po-Vers. 2008 | TechFak | Computational Engineering (Rechnergestütztes Ingenieurwesen) (Master of Science) | Gesamtkonto | Wahlpflichtbereich Informatik | Seminar im Masterstudium | Seminar Einführung in die Kryptografie)

[3] **Computational Engineering (Rechnergestütztes Ingenieurwesen) (Master of Science)**
(Po-Vers. 2008 | TechFak | Computational Engineering (Rechnergestütztes Ingenieurwesen) (Master of Science) | Gesamtkonto | Wahlpflichtbereich Angewandte Mathematik | Seminar im Masterstudium | Seminar Einführung in die Kryptografie)

[4] **Computational Engineering (Rechnergestütztes Ingenieurwesen) (Master of Science)**
(Po-Vers. 2008 | TechFak | Computational Engineering (Rechnergestütztes Ingenieurwesen) (Master of Science) | Gesamtkonto | Wahlpflichtbereich Technisches Anwendungsfach | Seminar im Masterstudium | Seminar Einführung in die Kryptografie)

[5] **Informatik (Bachelor of Arts (2 Fächer))**
(Po-Vers. | TechFak | Informatik (Bachelor of Arts (2 Fächer)) | Hauptseminar | Seminar Einführung in die Kryptografie)

[6] **Informatik (Bachelor of Arts (2 Fächer))**
(Po-Vers. 2013 | TechFak | Informatik (Bachelor of Arts (2 Fächer)) | Hauptseminar | Seminar Einführung in die Kryptografie)

[7] **Informatik (Bachelor of Science)**
(Po-Vers. | TechFak | Informatik (Bachelor of Science) | Gesamtkonto | Hauptseminar | Seminar Einführung in die Kryptografie)

[8] **Informatik (Bachelor of Science)**

(Po-Vers. | TechFak | Informatik (Bachelor of Science) | Hauptseminar | Seminar Einführung in die Kryptografie)

[9] **Informatik (Bachelor of Science)**
(Po-Vers. 2009w | TechFak | Informatik (Bachelor of Science) | Gesamtkonto | Hauptseminare, Praktika, Bachelorarbeit | Hauptseminar | Seminar Einführung in die Kryptografie)

[10] **Informatik (Master of Science)**
(Po-Vers. 2010 | TechFak | Informatik (Master of Science) | Gesamtkonto | Hauptseminar, Projekt, Masterarbeit | Hauptseminar | Seminar Einführung in die Kryptografie)

[11] **International Information Systems (IIS) (Master of Science)**
(Po-Vers. 2014w | ReWiFak | International Information Systems (IIS) (Master of Science) | Informatics | Informatics Electives | Software Engineering II | Seminar Einführung in die Kryptografie)

[12] **International Information Systems (IIS) (Master of Science)**
(Po-Vers. 2017w | ReWiFak | International Information Systems (IIS) (Master of Science) | Gesamtkonto | Informatics | Informatics Electives | Software Engineering II | Seminar Einführung in die Kryptografie)

Studien-/Prüfungsleistungen:

Seminar Einführung in die Kryptografie (Prüfungsnummer: 153330)
Prüfungsleistung, Seminarleistung
Anteil an der Berechnung der Modulnote: 100%
weitere Erläuterungen:
Die Bewertung der Prüfungsleistung setzt sich zusammen aus Seminarvortrag (Dauer 45 Min., Gewichtung 1/2), Ausarbeitung (Umfang 10 - 12 Seiten, Gewichtung 1/4) und mündlicher Prüfung (Dauer 15 Min., Gewichtung 1/4). Jede dieser Einzelleistungen muss mit mindestens 4,0 bestanden werden.

Erstablegung: WS 2021/2022, 1. Wdh.: SS 2022
1. Prüfer: Francesca Saglietti
