INF-MSc-337: Privacy-Enhancing Technologies					**BOSS-Nr.** 70920
Englischer Modultitel: Privacy-Enhancing Technologies					
Studiengänge: Masterstudiengang Informatik, Masterstudiengang Angewandte Informatik					
Turnus: nach Ankündigung	**Dauer:** 1 Semester	**Studienabschnitt:** 2.–3. Semester		**Credits:** 6	**Aufwand:** 180 (60/120)

1 Modulstruktur

Nr.	Element / Lehrveranstaltung	Typ	Credits	SWS
1	Privacy-Enhancing Technologies	V	3	2
2	Übung und Praktikumsprojekte zu Privacy-Enhancing Technologies	Ü+P	3	2

2 Lehrveranstaltungssprache: englisch

3 Lehrinhalte

Digitale Technologien sind ein wesentlicher Bestandteil unseres täglichen Lebens geworden. Diese Technologien sind zwar oft nützlich, bergen aber auch große Risiken für die Privatsphäre. In diesem Kurs wird gelernt, diese Risiken durch die Entwicklung von datenschutzfreundlichen Systemen zu verringern und den gebotenen Schutz der Privatsphäre zu bewerten. Konkret werden in diesem Modul deshalb die folgenden Themen und Techniken vermittelt:

- Einführung in die Privatsphäre
- Sichere Mehrparteienberechnungen
- (Vollständig) homomorphe Verschlüsselung
- Datenschutzgerechte Authentifizierung
- Anonyme Kommunikation
- Zensurresistenz
- Differential Privacy
- Tracking
- Standortdatenschutz

4 Kompetenzen

Nach erfolgreichem Abschluss des Moduls können die Studierenden

- die grundlegenden Bausteine für den Entwurf datenschutzfreundlicher Systeme erläutern,
- diese Bausteine kombinieren, um einfache Probleme unter Wahrung der Privatsphäre zu lösen, sowie
- die Privatsphäre von einfachen vorgeschlagenen Systemen bewerten.

5 Prüfungen

- Modulprüfung: Klausur (90 - 120 Minuten) oder mündliche Prüfung (30 Minuten), sowie Bewertung der Projekte. BOSS-NR. 70992
- Studienleistung: Keine.

Details werden zu Beginn der Veranstaltungen bekannt gegeben.

6 Prüfungsformen und -leistungen

Modulprüfung

7 Teilnahmevoraussetzungen

- Vorausgesetzte Kenntnisse: Basiswissen der Kryptographie (symmetrische und asymmetrische Verschlüsselung, Hashfunktionen) und Cybersicherheit.

8 Modultyp und Verwendbarkeit des Moduls

- Vertiefungsmodul in den Masterstudiengängen Informatik und Angewandte Informatik
- Forschungsbereich: Software, Sicherheit und Verifikation

9			
	Modulbeauftragte/r Prof. Dr. Christian Rossow, Dr. Wouter Lueks	**Zuständige Fakultät:** Informatik	**Beschluss Fakultätsrat:** voraussichtlich 11.06.2025