

Verwendbarkeit des Moduls beachten!

BOSS-NR. ?????

<b>Modul INF-BL-323: Grundlagen der Data Privacy (GDP)</b>					
identisch mit					
INF-BSc-323: Grundlagen der Data Privacy (Bachelor Informatik / Angewandte Informatik)					
INF-ML-323: Grundlagen der Data Privacy (Informatik Lehramt Master)					
<b>Studiengänge:</b> Bachelor Lehramt Informatik Gy/Ge					
<b>Turnus</b> jährlich	<b>Dauer</b> 1 Semester	<b>Studienabschnitt</b> ab 5. Semester	<b>Credits</b> 4	<b>Aufwand</b> 120 (45/75)	
<b>1</b>	<b>Modulstruktur</b>				
	<b>Nr.</b>	<b>Element / Lehrveranstaltung</b>	<b>Typ</b>	<b>Credits</b>	<b>SWS</b>
	1	Grundlagen der Data Privacy	V	2	2
	2	Übungen zu Grundlagen der Data Privacy	Ü	2	1
<b>2</b>	<b>Lehrveranstaltungs-sprache:</b> Deutsch				
<b>3</b>	<b>Lehrinhalte</b> Datenverarbeitungssysteme müssen bei der Verarbeitung, Speicherung und Übermittlung personen-gebundener Datenschutz berücksichtigen. In diesem Kurs werden die grundlegenden Algorithmen von privatsphäreschützenden Systemen vermittelt <ol style="list-style-type: none"> <li>1. Einführung in den Datenschutz (Risiken der Re-Identifizierung, Ebenen und Begriff des Datenschutzes, Taxonomie der Datenschutzdefinitionen)</li> <li>2. Datenschutz durch Aggregation (Datenaggregationsmethoden, Datennutzen bei Aggregation, Kennzeichnungsproportionen)</li> <li>3. Datenschutz durch Secret Sharing (Sichere Mehrparteien-Berechnungen)</li> <li>4. Privatsphäre durch Sketches (Streaming Algorithmen, verlustbehaftete Zählung, Reservoir Sampling, Count-Min Sketches, Flajolet-Martin Sketches)</li> <li>5. Vertraulichkeit durch Datenperturbation (Filterung, Vereinfachung, Verallgemeinerung, Hashing)</li> <li>6. Privatsphäre durch differentielle Privatsphäre (Konzept der Differential Privacy, Laplacian Noise, datenschutzgerechte Datenveröffentlichung)</li> <li>7. Grundlagen der Kryptographie (Diskreter Logarithmus, Diskrete Wurzeln, Erweiterter Euklidischer Algorithmus, Chinese Remainder Theorem)</li> <li>8. Privatsphäre durch Kryptographie (Symmetrische vs. asymmetrische Kryptographie, RSA)</li> <li>9. Privatsphäre durch homomorphe Verschlüsselung (Pailliers homomorphes Verschlüsselungsverfahren, Shamir's Secret Sharing, E-Voting-Systeme)</li> <li>10. Datenschutzbestimmungen (GDPR, UNDG)</li> <li>11. Ethik und Big Data (Bewertung von Datenschutz und Ethik, Sensibilisierung für ethische Herausforderungen durch Big Data)</li> </ol> Die Hauptziele des Kurses sind: <ul style="list-style-type: none"> <li>• Lernen der Herausforderungen des Datenschutzes,</li> <li>• Vermittlung von Kenntnissen von privacy-preserving Methoden für die Speicherung/Übertragung/Analyse von Daten und deren Veröffentlichung,</li> <li>• Erlernen von Privacy-by-design Analysemethoden,</li> <li>• Einführung zu gesetzlichen Regelungen in Bezug auf Daten-systeme,</li> </ul> Vorstellung des ethischen Beurteilungsprozesses. <i>Content</i> Data processing systems must take into account the privacy of individuals when processing, storing and transmitting personal data. This course teaches the basic algorithms of privacy-protecting systems.				
<b>4</b>	<b>Kompetenzen</b> Nach Abschluss des Kurses sollen die Teilnehmer*innen in der Lage sein: <ul style="list-style-type: none"> <li>• Die vielfältigen Herausforderungen des Datenschutzes bei der Speicherung, Verarbeitung und</li> </ul>				

	Modellierung von Big Data, Datenströmen oder episodischen Daten zu erklären und zu interpretieren <ul style="list-style-type: none"> <li>• Differential Privacy zu verwenden,</li> <li>• Methoden des Secret Sharing zu verwenden,</li> <li>• Kryptographische Prinzipien darstellen,</li> <li>• eine Ethikbewertung eines Softwaresystems durchführen.</li> </ul>	
5	<b>Prüfungen</b> <i>Modulprüfung:</i> Klausur oder mündliche Prüfung <sup>BOSS-Nr. ?????</sup> <i>Studienleistung:</i> <ul style="list-style-type: none"> <li>• aktive Mitarbeit in der Übung und Erreichen der Mindestpunktzahl bei den Übungsaufgaben<sup>BOSS-Nr. ?????</sup></li> </ul> Die Studienleistung ist Voraussetzung für die Teilnahme an der Modulprüfung	
6	<b>Prüfungsformen und -leistungen</b> <input checked="" type="checkbox"/> Modulprüfung <input type="checkbox"/> Teilleistungen	
7	<b>Teilnahmevoraussetzungen</b> <i>Erfolgreich abgeschlossen:</i> -keine- <i>Wünschenswerte Kenntnisse:</i> Grundlegende Kenntnisse der Mathematik (insbes. Ringe), und Grundlagen der Datenwissenschaft	
8	<b>Modultyp und Verwendbarkeit des Moduls</b> Wahlmodul im Fach Informatik des Lehramtsbachelorstudiengangs für Gymnasien und Gesamtschulen gemäß FSB 2018	
9	<b>Modulbeauftragte/r</b> Prof. Dr. Th. Liebig	<b>Zuständige Fakultät</b> Informatik
		Beschluss Fakultätsrat 18.10.2022