LEHRVERANSTALTUNGSBESCHREIBUNG

Kryptographie

Akademisches Jahr 2025-2026

1. Angaben zum Programm

1.1. Hochschuleinrichtung	**Universitatea Babes-Bolyai**
1.2. Fakultät	**Mathematik und Informatik**
1.3. Department	**Informatik**
1.4. Fachgebiet	**Informatik**
1.5. Studienform	**Bachelor**
1.6. Studiengang / Qualifikation	**Informatik in deutscher Sprache**
1.7. Form des Studiums	**Präsenzstudium**

2. Angaben zum Studienfach

2.1. LV-Bezeichnung	Kryptographie					Code der LV	MLG0059
2.2. Lehrverantwortlicher – Vorlesung	Lekt. dr. Thu Hang Bui						
2.3. Lehrverantwortlicher – Seminar	Lekt. dr. Thu Hang Bui						
2.4. Studienjahr	3	2.5. Semester	1	2.6. Prüfungsform	K	2.7. Art der LV	Wahlpflichtfach

3. Geschätzter Workload in Stunden

3.1. SWS	2+2	von denen: 3.2 Vorlesung	**2**	3.3. Seminar/Übung/Projekt	**2+2**
3.4. Gesamte Stundenanzahl im Lehrplan	24	von denen: 3.5 Vorlesung	**28**	3.6 Seminar/Übung/Projekt	**56**

Verteilung der Studienzeit:	Std
Studium nach Handbücher, Kursbuch, Bibliographie und Mitschriften	20
Zusätzliche Vorbereitung in der Bibliothek, auf elektronischen Fachplattformen und durch Feldforschung	20
Vorbereitung von Seminaren/Übungen, Präsentationen, Referate, Portfolios und Essays	20
Tutoriat	10
Prüfungen	3
Andere Tätigkeiten:	

3.7. Gesamtstundenanzahl Selbststudium	73
3.8. Gesamtstundenanzahl / Semester	125
3.9. Anrechnungspunkte	5

4. Voraussetzungen (falls zutreffend)

4.1. zur Lehrveranstaltung	Algebraische Grundlagen der Informatik
4.2. kompetenzbezogene	

5. Bedingungen (falls zutreffend)

5.1. zur Durchführung der Vorlesung	Vorlesungsraum, Beamer, Laptop
5.2. zur Durchführung des Seminars / der Übung	Computerraum

6.1. Spezifische erworbene Kompetenzen[1]

Berufliche/Wesentliche Kompetenzen	K 4.1 Definieren der Grundkonzepte und Prinzipien der Informatik, sowie der mathematischen Theorien und Modelle K 4.3 Identifizierung der geeigneten Modelle und Methoden für die Lösung realer Probleme K 4.4 Anwendung der Simulierungen für die Untersuchung der Verhaltensweise der angewandten Modelle und Bewertung der Ergebnisse K4.5 Einbauen der formalen Modelle in geeignete Anwendungen der spezifischen Gebiete K6.4 Leistungsmessungen der Antwortzeiten, Ressourcenverbrauch, Festlegen der Zugriffsrechte
Transversale Kompetenzen	TK1 Anwendung der Regeln für gut organisierte und effiziente Arbeit, für verantwortungsvolle Einstellungen gegenüber der Didaktik und der Wissenschaft, für kreative Förderung des eigenen Potentials, mit Rücksicht auf die Prinzipien und Normen der professionellen Ethik TK2 Effizienter Ablauf der Tätigkeiten in einer interdisziplinären Gruppe, das Entwickeln der Kapazitäten für empathische zwischenmenschliche Kommunikation, Verknüpfung und Zusammenarbeit mit unterschiedlichen Gruppen TK3 Anwendung von effizienten Methoden und Techniken für Lernen, Informieren und Recherchieren, für das Entwicklen der Kapazitäten der praktischen Umsetzung der Kenntnisse, der Anpassung an die Bedürfnisse einer dynamischen Gesellschaft, der Kommunikation in rumänischer Sprache und in einer internationalen Verkehrssprache

6.2. Lernergebnisse

Kenntnisse	Der Studierende ist in der Lage, die Entwicklung von Fähigkeiten sicherzustellen, die für die mathematischen und algorithmischen Disziplinen erforderlich sind, um Aufgaben erfolgreich zu bearbeiten. Der Studierende kennt grundlegende Konzepte der Kryptographie und Methoden zu deren Anwendung in wissenschaftlichen Bereichen, die mit Mathematik und Informatik verbunden sind.
Fähigkeiten	Der Absolvent entwickelt mathematisches und algorithmisches Denken, das sich von einem prozeduralen/komputationalen Verständnis der Mathematik zu einem umfassenden Verständnis mit logischem Denken, Generalisierung, Abstraktion und formalem Beweis weiterentwickelt
Verantwortung und Autonomie	Der Studierende ist in der Lage, angewandte mathematische Inhalte selbstständig zu erforschen, indem er auf Ideen und Werkzeuge aus früheren Kursen zurückgreift, um sein Verständnis zu vertiefen. Der Studierende erweitert eigenständig angewandte mathematische Ideen und Argumente aus früheren Kursen auf ein mathematisches oder informatisches Thema, das bisher nicht behandelt wurde.

7. Ziele (entsprechend der erworbenen Kompetenzen)

7.1 Allgemeine Ziele der Lehrveranstaltung	Die grundlegenden kryptographische Algorithmen werden dargestellt
7.2 Spezifische Ziele der Lehrveranstaltung	Algorithmen aus der Zahlentheorie und Algebra werden in konkrete Projekte implementiert.

[1] Man kann Kompetenzen oder Lernergebnisse, oder beides wählen. Wenn nur eine Option ausgewählt wird, wird die Tabelle für die andere Option gelöscht, und die beibehaltene Option erhält die Nummer 6.

8. Inhalt

8.1 Vorlesung	Lehr-und Lernmethode	Anmerkungen
1. Klassische Kryptographie. Beispiele. Chiffriersysteme	Vortrag, Erklärungen, Beispiele, Fallstudien	
2. Prinzipien moderner Kryptographie. Angriffsszenarien. Methoden der Kryptanalyse.	Vortrag, Erklärungen, Beispiele, Fallstudien	
3. Sicherheit kryptographischer Systeme.	Vortrag, Erklärungen, Beispiele, Fallstudien	
4. Symmetrische Kryptographie. Chiffriermodi.	Vortrag, Erklärungen, Beispiele, Fallstudien	
5. Datenverschlüsselungsstandard: (DES) und AES	Vortrag, Erklärungen, Beispiele, Fallstudien	
6. Funktionsweise von Blockchiffren	Vortrag, Erklärungen, Beispiele, Fallstudien	
7. Public-Key-Kryptografie: RSA, Diffie-Hellman	Vortrag, Erklärungen, Beispiele, Fallstudien	
8. Algorithmen für digitale Signaturen: RSA mit Hash-Funktion, ElGamal DS, Schnoor DS, DSA	Vortrag, Erklärungen, Beispiele, Fallstudien	
9. Kryptografische Hash-Funktionen	Vortrag, Erklärungen, Beispiele, Fallstudien	
10. Bitcoins	Vortrag, Erklärungen, Beispiele, Fallstudien	
11. Post-Quanten	Vortrag, Erklärungen, Beispiele, Fallstudien	
12. Verschlüsselungsalgorithmen in Telefonnetzen und Angriffe auf Telefonnetze	Vortrag, Erklärungen, Beispiele, Fallstudien	
13. Kryptografie in der Netzwerksicherheit	Vortrag, Erklärungen, Beispiele, Fallstudien	

Literatur in deutscher Sprache

[1] C. WAGENKNECHT, HIELSCHER M., Formale Sprachen, abstrakte Automaten und Compiler, Vieweg Teubner, 2009.
[2] ASTEROTH, A., BAIER, C., Theoretische Informatik, eine Einführung in Berechnbarkeit, Komplexität und formale Sprachen, Pearson Studium, 2002.
[3] HROMKOVIC, J., Theoretische Informatik, Formale Sprachen, Berechenbarkeit, Komplexitätstheorie, Algorithmik, Kommunikation und Kryptographie, Vieweg Teubner, 2011.

Literatur in englischer Sprache

[1] K.D. COOPER, L. TORCZON - Engineering a Compiler, Elsevier Science & Technology, 2011.
[2] A.V. AHO, D.J. ULLMAN - Principles of compiler design, Addison-Wesley, 1978.

8.3 Labor	Lehr-und Lernmethode	Anmerkungen
Seminar 1: Klassische Kryptografie	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
Seminar 2: Kryptoanalyse für klassische Verschlüsselungsverfahren	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
Seminar 3: Symmetrische öffentliche Schlüssel (DES und AES)	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
Seminar 4: Asymmetrische Schlüssel (RSA) und DSS	Debatte, Gespräch, Beispiele,	

	Unterrichtsgespräch Vorführung	
Seminar 5: MAC und HMAC	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
Seminar 6: Steganografie	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
Seminar 7: Post-Quanten (Quantenschlüsselverteilung QKD)	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
Literatur 1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006. 2. R. **Küsters**, Ralf, Th. **Wilke**, Thomas, Moderne Kryptographie - Eine Einführung, XLeitfäden der Informatik , Springer-Vieweg, 2011		

9. Verbindung der Inhalte mit den Erwartungen der Wissensgemeinschaft, der Berufsverbände und der für den Fachbereich repräsentativen Arbeitgeber

Der Kurs folgt die IEEE und ACM Curricula Empfehlungen für das Informatikstudium Der Kurs existiert in der Mehrzahl der rumänischen und ausländischen Universitäten

10. Prüfungsform

Veranstaltungsart	10.1 Evaluationskriterien	10.2 Evaluationsmethoden	10.3 Anteil an der Gesamtnote
10.4 Vorlesung	Kenntnisse der im Kurs behandelten Themen. Die Lösung der Aufgaben	Klausur	70%
10.5 Seminar / Übung	Die Fähigkeit praktische Probleme direkt am Computer zu lösen. Ausserdem muss jeder Student jede zwei Wochen seine Übungen abgeben.	3 Projekte Leistungen während des Labors	30%
10.6 Minimale Leistungsstandards			
Für das Bestehen der Prüfung muss die Mindestnote 5 erzielt werden.			

11. SDD-Nachhaltigkeits-Logos (Sustainable Development Goals)[2]

Nicht anwendbar.

[2] Bitte belassen Sie nur die Logos, die entsprechend den *Regularien zu Anwendung der Nachhaltigkeits-Logos im akademischen Betrieb* dem jeweiligen Studienfach entsprechen und löschen Sie diejenigen Logos, inklusive das allgemeine *Nachhaltigkeits-Logo* falls dieses nicht zutrifft. Falls keines der Logos für das Studienfach anwendbar ist, löschen Sie alle mit der Angabe „*nicht anwendbar*".

Ausgefüllt am:	Vorlesungsverantwortlicher	Seminarverantwortlicher
30.10.2025	Lekt. dr. Thu Hang Bui	Lekt. dr. Thu Hang Bui

Genehmigt im Department am:	Departmentleiter
...	Conf. dr. Adrian STERCA