LEHRVERANSTALTUNGSBESCHREIBUNG

1. Angaben zum Programm

1.1 Hochschuleinrichtung	Babes-Bolyai Universität
1.2 Fakultät	Mathematik und Informatik
1.3 Department	Informatik
1.4 Fachgebiet	Informatik
1.5 Studienform	Bachelor
1.6 Studiengang / Qualifikation	Informatik

2. Angaben zum Studienfach

2.1 LV-Bezeichnung		Kryptographie					
2.2 Lehrverantwortlicher – Vorlesung				Conf. Dr. Christian Sacarea			
2.3 Lehrverantwortlicher – Seminar				Conf. Dr. Christian Sacarea			
2.4 Studienjahr	2	2.5 Semester	4	2.6. Prüfungsform	Kolloquium	2.7 Art der LV	Wahlpflichtfach

3. Geschätzter Workload in Stunden

3.1 SWS	4	von denen: 3.2 Vorlesung	2	3.3 Seminar/Übung	1
3.4 Gesamte Stundenanzahl im Lehrplan	42	von denen: 3.5 Vorlesung	28	3.6 Seminar/Übung	14
Verteilung der Studienzeit:					Std.
Studium nach Handbücher, Kursbuch, Bibliographie und Mitschriften					**10**
Zusätzliche Vorbereitung in der Bibliothek, auf elektronischen Fachplattformen und durch Feldforschung					**10**
Vorbereitung von Seminaren/Übungen, Präsentationen, Referate, Portfolios und Essays					**20**
Tutorien					**2**
Prüfungen					**2**
Andere Tätigkeiten:					-

3.7 Gesamtstundenanzahl Selbststudium	44
3.8 Gesamtstundenanzahl / Semester	100
3.9 Leistungspunkte	4

4. Voraussetzungen (falls zutreffend)

4.1 curricular	• Algebraische Grundlagen der Informatik
4.2 kompetenzbezogen	•

5. Bedingungen (falls zutreffend)

5.1 zur Durchführung der Vorlesung	•
5.2 zur Durchführung des Seminars / der Übung	• Internetzugang. Computerlabor.

6. Spezifische erworbene Kompetenzen

Berufliche 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

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.

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	Vortrag, Erklärungen, Beispiele, Fallstudien	

Kryptanalyse.		
3. Sicherheit kryptographischer Systeme.	Vortrag, Erklärungen, Beispiele, Fallstudien	
4. Symmetrische Kryptographie. Chiffriermodi.	Vortrag, Erklärungen, Beispiele, Fallstudien	
5. Data Encryption Standard (DES)	Vortrag, Erklärungen, Beispiele, Fallstudien	
6. Advanced Encryption Standard (AES)	Vortrag, Erklärungen, Beispiele, Fallstudien	
7. Public Key Kryptographie.	Vortrag, Erklärungen, Beispiele, Fallstudien	
8. Public Key Kryptographie.	Vortrag, Erklärungen, Beispiele, Fallstudien	
9. Digitale Unterschriften.	Vortrag, Erklärungen, Beispiele, Fallstudien	
10. Hash Funktionen.	Vortrag, Erklärungen, Beispiele, Fallstudien	
11. Kryptographische Hashfunktionen.	Vortrag, Erklärungen, Beispiele, Fallstudien	
12. Verschlüsselungsalgorithmen in GSM Netze.	Vortrag, Erklärungen, Beispiele, Fallstudien	
13. Angriffe in GSM Netze.	Vortrag, Erklärungen, Beispiele, Fallstudien	
14. Praktische Anwendungen der public key Kryptographie.	Vortrag, Erklärungen, Beispiele, Fallstudien	

Literatur

1. Buchmann Johannes, Einführung in die Kryptographie, Springer, 2001.
2. Klein, Andreas, Visuelle Kryptographie, Springer 2007.
3. Schwenk, J., Sicherheit und Kryptographie im Internet, Vieweg, 2005.

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006.

2. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography. CRC Press,

Boca Raton, 1997. (http://www.math.uwaterloo.ca/~ajmeneze)

3. B. Schneier, Applied Cryptography. John Wiley & Sons, 1996.

8.2 Seminar / Übung	Lehr- und Lernmethode	Anmerkungen
1. Klassische Kryptographie I.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
2. Klassische Kryptographie II.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
3. Klassische Kryptographie III.	Debatte, Gespräch,	

	Beispiele, Unterrichtsgespräch Vorführung	
4. DES.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
5. AES.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
6. Public Key Kryptographie.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
7. Praktische Anwendungen der public key Kryptographie.	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
• Note 5 auf einer Skala von 1 bis 10.

Ausgefüllt am:	Vorlesungsverantwortlicher	Seminarverantwortlicher
	Conf.Dr. Christian Sacarea	Conf.Dr. Christian Sacarea
Genehmigt im Department am:		Departmentdirektor
		Prof. Dr. Anca Andreica