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		Public key Kryptographie					
2.2 Lehrverantwortlicher – Vorlesung				Lect. Dr. Christian Sacarea			
2.3 Lehrverantwortlicher – Seminar				Lect. 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	2
3.4 Gesamte Stundenanzahl im Lehrplan	56	von denen: 3.5 Vorlesung	28	3.6 Seminar/Übung	28
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	•
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	• Verstehen der Grundbegriffe der Kryptographie, sowie die Fähigkeit diese praktisch Anzuwenden. • Fähigkeiten verschiedene Probleme aus andere Bereiche zu verstehen und zu modellieren.
Transversale Kompetenzen	• Aneignen verschiederener Fähigkeiten aus der Datensicherheit und Kryptographie. • Selbständige Arbeit • Kreativität.

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.	Vortrag, Erklärungen, Beispiele, Fallstudien	
2. Public key Kryptographie.	Vortrag, Erklärungen, Beispiele, Fallstudien	
3. Komplexität der Algorithmen.	Vortrag, Erklärungen, Beispiele, Fallstudien	
4. Modulare Kongruenzen.	Vortrag, Erklärungen, Beispiele, Fallstudien	
5. Primzahlen. Residuen.	Vortrag, Erklärungen, Beispiele, Fallstudien	
6. Primzahltest Algorithmen.	Vortrag, Erklärungen, Beispiele, Fallstudien	
7. Primzahlzerlegung Algorithmen I.	Vortrag, Erklärungen,	

	Beispiele, Fallstudien	
8. Primzahlzerlegung Algorithmen II.	Vortrag, Erklärungen, Beispiele, Fallstudien	
9. Das Rabin Kryptosystem.	Vortrag, Erklärungen, Beispiele, Fallstudien	
10. Das ElGamal Kryptosystem. Endliche Körper.	Vortrag, Erklärungen, Beispiele, Fallstudien	
11. Polynomzerlegung. Algorithmus von Berlekamp.	Vortrag, Erklärungen, Beispiele, Fallstudien	
12. Diskrete Logarythmen.	Vortrag, Erklärungen, Beispiele, Fallstudien	
13. Praktische Anwendungen der public key Kryptographie I.	Vortrag, Erklärungen, Beispiele, Fallstudien	
14. Praktische Anwendungen der public key Kryptographie II.	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. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.

3. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

4. 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)

5. 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. Komplexität der Algorithmen.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch	

	Vorführung	
5. Modulare Arithmetik I.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
6. Modulare Arithmetik II.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
7. Primzahltest Algorithmen I.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
8. Primzahltest Algorithmen II.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
9. Primzahlzerlegung Algorithmen I.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
10. Primzahlzerlegung Algorithmen II.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
11. Public key Kryptographie I.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
12. Public key Kryptographie II.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
13. Praktische Anwendungen der public key Kryptographie I.	Debatte, Gespräch, Beispiele, Unterrichtsgespräch Vorführung	
14. Praktische Anwendungen der public key Kryptographie II.	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. 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.

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	2 Tests Klausur Klausur	10% 20% 25%
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	45%
10.6 Minimale Leistungsstandards			
• Note 5 auf einer Skala von 1 bis 10.			

Ausgefüllt am:	Vorlesungsverantwortlicher	Seminarverantwortlicher
13.04.2015	Lect.Dr. Christian Sacarea	Lect.Dr. Christian Sacarea

Genehmigt im Department am:	Departmentdirektor
13.04.2015	Prof. Dr. Bazil Parv