FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Babes-Bolyai Cluj-Napoca
1.2 Facultatea	Facultatea de Matematica si Informatica
1.3 Departamentul	Departamentul de Informatica
1.4 Domeniul de studii	Informatica
1.5 Ciclul de studii	Master
1.6 Programul de studiu / Calificarea	Sisteme distribuite

2. Date despre disciplină

2.1 Denumirea disciplinei		Aritmetica modulara si criptografie					
2.2 Titularul activităţilor de curs		Conf.Dr. Septimiu Crivei					
2.3 Titularul activităţilor de seminar		Conf.Dr. Septimiu Crivei					
2.4 Anul de studiu	**1**	2.5 Semestrul	**1**	2.6. Tipul de evaluare	**E**	2.7 Regimul disciplinei	**Obligatorie**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14

Distribuţia fondului de timp:	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	28
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	53
Tutoriat	10
Examinări	14
Alte activităţi:	0

3.7 Total ore studiu individual	133
3.8 Total ore pe semestru	175
3.9 Numărul de credite	7

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	
4.2 de competenţe	

5. Condiţii (acolo unde este cazul)

5.1 De desfăşurare a cursului	
5.2 De desfăşurare a seminarului/laboratorului	

6. Competenţele specifice acumulate

Competenţe profesionale	Intelegerea unor concepte matematice de baza si folosirea lor in activitati de rezolvare de probleme Abilitatea de a intelege si a aborda probleme de modelare din alte stiinte
Competenţe transversale	Abilitatea de a lucra independent si/sau in echipa pentru a rezolva probleme in diverse contexte profesionale

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	• Prezentarea unor algoritmi matematici folositi in criptografie
7.2 Obiectivele specifice	• Algoritmi numerici si algebrici vor fi studiati si implementati in proiecte

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Notiuni de complexitatea algoritmilor, congruente	expunere, algoritmizare	
2. Primalitate si factorizare	expunere, algoritmizare	
3. Resturi patratice	expunere, algoritmizare	
4. Corpuri finite si logaritmi discreti	expunere, algoritmizare	
5. Sisteme clasice de criptare	expunere, algoritmizare	
6. Criptografie cu cheie privata	expunere, algoritmizare	
7. Cifruri pe blocuri	expunere, algoritmizare	
8. Cifruri pe siruri	expunere, algoritmizare	
9. Criptosistemul RSA	expunere, algoritmizare	
10. Criptosistemul ElGamal	expunere, algoritmizare	
11. Functii hash	expunere, algoritmizare	
12. Semnaturi digitale	expunere, algoritmizare	
13. Protocoale legate de chei	expunere, algoritmizare	
14. Criptografie cuantica	expunere, algoritmizare	

Bibliografie

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
2. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
3. D. Kahn, The Codebreakers, Macmillan, 1967.
4. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
5. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [http://www.cacr.math.uwaterloo.ca/hac]

8.2 Seminar	Metode de predare	Observaţii
1. Notiuni de complexitatea algoritmilor, congruente	problematizare, exercitiu	Seminarul consta din 2 ore la 2 saptamani
2. Primalitate	problematizare, exercitiu	
3. Factorizare	problematizare, exercitiu	
4. Resturi patratice	problematizare, exercitiu	
5. Corpuri finite si logaritmi discreti	problematizare, exercitiu	
6. Criptografie cu cheie privata	problematizare, exercitiu	
7. Criptografie cu cheie publica	problematizare, exercitiu	

Bibliografie

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
2. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
3. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [http://www.cacr.math.uwaterloo.ca/hac]

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Continutul este orientat catre aspecte practice ale criptografiei. Subiectul este prezent in mai multe programe de master in domenii ale informaticii din alte universitati.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Folosirea unor concepte si metode de baza in exemple	Teme	1/3
10.5 Seminar	Rezolvare de probleme, prezentare de proiecte	Test, examen practic	2/3
10.6 Standard minim de performanţă			
Nota 5			

Data completării
30.04.2013

Titular de curs
Conf.Dr. Septimiu CRIVEI

Titular de seminar
Conf.Dr. Septimiu CRIVEI

Data avizării în departament
30.04.2013

Director de departament
Prof.Dr. Octavian AGRATINI