

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Babeș-Bolyai Cluj-Napoca
1.2 Facultatea	Facultatea de Matematica și Informatică
1.3 Departamentul	Departamentul de Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Master
1.6 Programul de studiu / Calificarea	Baze de date

### 2. Date despre disciplină

2.1 Denumirea disciplinei	Aritmetica modulară și criptografie						
2.2 Titularul activităților de curs	Prof.Dr. Septimiu Crivei						
2.3 Titularul activităților de seminar	Prof.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 activităților 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 învățământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					28
Pregătire seminariilor/laboratoare, teme, referate, portofolii și eseuri					53
Tutoriat					10
Examinări					14
Alte activități: .....					0
3.7 Total ore studiu individual	133				
3.8 Total ore pe semestru	175				
3.9 Numărul de credite	7				

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	•
4.2 de competențe	•

### 5. Condiții (acolo unde este cazul)

5.1 De desfășurare a cursului	•
5.2 De desfășurare a seminarului/laboratorului	•

### 6. Competențele specifice acumulate

<b>Competențe profesionale</b>	<ul style="list-style-type: none"> <li>• Înțelegerea unor concepte matematice de bază și folosirea lor în activități de rezolvare de probleme</li> <li>• Abilitatea de a înțelege și a aborda probleme de modelare din alte științe</li> </ul>
<b>Competențe transversale</b>	<ul style="list-style-type: none"> <li>• Abilitatea de a lucra independent și/sau în echipă pentru a rezolva probleme în diverse contexte profesionale</li> </ul>

## 7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	<ul style="list-style-type: none"> <li>Prezentarea unor algoritmi matematici folosiți în criptografie</li> </ul>
7.2 Obiectivele specifice	<ul style="list-style-type: none"> <li>Algoritmi numerici și algebrici vor fi studiați și implementați în proiecte</li> </ul>

## 8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Noțiuni de complexitatea algoritmilor, congruente	expunere, algoritmizare	
2. Primalitate și factorizare	expunere, algoritmizare	
3. Resturi patratic	expunere, algoritmizare	
4. Corpuri finite și logaritmi discreți	expunere, algoritmizare	
5. Sisteme clasice de criptare	expunere, algoritmizare	
6. Criptografie cu cheie privată	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. Funcții hash	expunere, algoritmizare	
12. Semnături digitale	expunere, algoritmizare	
13. Protocoale legate de chei	expunere, algoritmizare	
14. Criptografie cuantică	expunere, algoritmizare	

### Bibliografie

- S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
- C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. București, 2005.
- D. Kahn, The Codebreakers, Macmillan, 1967.
- N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
- 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	Observații
1. Noțiuni de complexitatea algoritmilor, congruente	problematizare, exercitiu	Seminarul constă din 2 ore la 2 săptămâni
2. Primalitate	problematizare, exercitiu	
3. Factorizare	problematizare, exercitiu	
4. Resturi patratic	problematizare, exercitiu	
5. Corpuri finite și logaritmi discreți	problematizare, exercitiu	
6. Criptografie cu cheie privată	problematizare, exercitiu	
7. Criptografie cu cheie publică	problematizare, exercitiu	

### Bibliografie

- S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
- N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
- 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 conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

<ul style="list-style-type: none"> <li>Conținutul este orientat către aspecte practice ale criptografiei. Subiectul este prezent în mai multe programe de master în domenii ale informaticii din alte universități.</li> </ul>
--

## 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 performanță			
• Nota 5			

Data completării  
30.04.2014

Titular de curs  
Prof.Dr. Septimiu CRIVEI

Titular de seminar  
Prof.Dr. Septimiu CRIVEI

Data avizării în departament  
30.04.2014

Director de departament  
Prof.Dr. Octavian AGRATINI