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	Calculatoare si tehnologia informatiei
1.5 Ciclul de studii	Licenta
1.6 Programul de studiu / Calificarea	Ingineria informatiei

2. Date despre disciplină

2.1 Denumirea disciplinei				Criptografie si protectia datelor			
2.2 Titularul activităţilor de curs				Prof.Dr. Septimiu Crivei			
2.3 Titularul activităţilor de seminar				Prof.Dr. Septimiu Crivei			
2.4 Anul de studiu	**3**	2.5 Semestrul	**5**	2.6. Tipul de evaluare	**C**	2.7 Regimul disciplinei	**Optional DS**

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 LP
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					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					8
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					14
Tutoriat					14
Examinări					8
Alte activităţi:					0

3.7 Total ore studiu individual	58
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

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	C3.1 Identificarea unor clase de probleme şi metode de rezolvare caracteristice sistemelor informatice C3.2 Utilizarea de cunoştinţe interdisciplinare, a tiparelor de soluţii şi a uneltelor, efectuarea de experimente şi interpretarea rezultatelor lor C3.5 Dezvoltarea şi implementarea de soluţii informatice pentru probleme concrete

Competenţe transversale	CT1 Comportarea onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei CT2 Identificarea, descrierea şi derularea proceselor din managementul proiectelor, cu preluarea diferitelor roluri în echipă şi descrierea clară şi concisă, verbal şi în scris, în limba română şi într-o limbă de circulație internațională, a rezultatelor din domeniul de activitate CT3 Demonstrarea spiritului de inițiativă şi acțiune pentru actualizarea cunoştințelor profesionale, economice şi de cultură organizațională

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	• Prezentarea unor algoritmi matematici folositi in criptografia cu cheie publica
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. Criptografie clasica, exemple	Expunere interactiva, explicatie, demonstratie didactica	
2. Complexitatea algoritmilor, elemente de teoria numerelor	Expunere interactiva, explicatie, demonstratie didactica	
3. Criptografie cu cheie publica. RSA	Expunere interactiva, explicatie, demonstratie didactica	
4. Algoritmi pentru testarea primalitatii	Expunere interactiva, explicatie, demonstratie didactica	
5. Algoritmi de factorizare a intregilor	Expunere interactiva, explicatie, demonstratie didactica	
6. Resturi patratice. Criptosistemul cu cheie publica Rabin	Expunere interactiva, explicatie, demonstratie didactica	
7. Polinoame. Corpuri finite	Expunere interactiva, explicatie, demonstratie didactica	
8. Criptosistemul cu cheie publica ElGamal	Expunere interactiva, explicatie, demonstratie didactica	
9. Algoritmi de calcul al logaritmilor discreti	Expunere interactiva, explicatie, demonstratie didactica	
10. Factorizarea polinoamelor: algoritmul lui Berlekamp	Expunere interactiva, explicatie, demonstratie didactica	
11. Semnaturi digitale	Expunere interactiva, explicatie, demonstratie didactica	
12. Protocoale legate de chei	Expunere interactiva, explicatie, demonstratie didactica	
13. Aspecte practice ale criptosistemelor cu cheie publica	Expunere interactiva, explicatie, demonstratie didactica	
14. Criptografie pe curbe eliptice	Expunere interactiva, explicatie, demonstratie didactica	

Bibliografie

1. M. Cozzens, S.J. Miller, The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society, 2013.
2. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
3. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.

4. 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]
5. C. Paar, J. Pelzl, Understanding Cryptography, Springer, 2009.

8.2 Laborator	Metode de predare	Observaţii
1. Criptografie clasica	Expunere interactiva, algorimtizare	Laboratorul este programat cu 2 ore o data la 2 saptamani
2. Complexitatea algoritmilor	Expunere interactiva, algorimtizare	
3. Aritmetica modulara	Expunere interactiva, algorimtizare	
4. Algoritmi pentru testarea primalitatii	Expunere interactiva, algorimtizare	
5. Algoritmi de factorizare a intregilor	Expunere interactiva, algorimtizare	
6. Criptografie cu cheie publica	Expunere interactiva, algorimtizare	
7. Aspecte practice ale criptosistemelor cu cheie publica	Expunere interactiva, algorimtizare	

Bibliografie

1. M. Cozzens, S.J. Miller, The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society, 2013.
2. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
3. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
4. 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]
5. C. Paar, J. Pelzl, Understanding Cryptography, Springer, 2009.

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 studii in domenii ale informaticii ale universitatilor importante.

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	50
10.5 Seminar	Implementarea de concepte si algoritmi	Examen practic	50
10.6 Standard minim de performanţă			
• Nota 5			

Data completării
30.04.2022

Titular de curs
Prof.Dr. Septimiu CRIVEI

Titular de seminar
Prof.Dr. Septimiu CRIVEI

Data avizării în departament
24.05.2022

Director de departament
Prof.Dr. Laura Diosan