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	Securitate cibernetica

2. Date despre disciplină

2.1 Denumirea disciplinei	Criptografie						
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	**1**	2.5 Semestrul	**1**	2.6. Tipul de evaluare	**E**	2.7 Regimul disciplinei	**DF**
2.8 Codul disciplinei	**MME3049**						

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

3.1 Număr de ore pe săptămână	4	Din care: 3.2 curs	2	3.3 seminar/laborator	1 seminar+1 proiect
3.4 Total ore din planul de învăţământ	56	Din care: 3.5 curs	28	3.6 seminar/laborator	28
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notițe					28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					28
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					14
Tutoriat					21
Examinări					28
Alte activităţi:					0
3.7 Total ore studiu individual	119				
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. Complexitatea algoritmilor, aritmetica modulara	expunere, algoritmizare	
2. Primalitate si factorizare	expunere, algoritmizare	
3. Corpuri finite și logaritmi discreti	expunere, algoritmizare	
4. Criptografie clasica	expunere, algoritmizare	
5. DES, AES	expunere, algoritmizare	
6. Cifruri fluide	expunere, algoritmizare	
7. Cifruri pe blocuri	expunere, algoritmizare	
8. Criptosistemul RSA	expunere, algoritmizare	
9. Criptosistemul ElGamal	expunere, algoritmizare	
10. Funcții hash	expunere, algoritmizare	
11. Semnături digitale	expunere, algoritmizare	
12. Protocoale legate de chei	expunere, algoritmizare	
13. Aspecte practice	expunere, algoritmizare	
14. Criptografie cuantica	expunere, algoritmizare	

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 Seminar	Metode de predare	Observaţii
1. Complexitatea algoritmilor, aritmetica modulara	problematizare, exercitiu	

2. Primalitate si factorizare	problematizare, exercitiu	
3. Corpuri finite și logaritmi discreti	problematizare, exercitiu	
4. Criptografie clasica	problematizare, exercitiu	
5. DES, AES	problematizare, exercitiu	
6. Cifruri fluide	problematizare, exercitiu	
7. Cifruri pe blocuri	problematizare, exercitiu	
8. Criptosistemul RSA	problematizare, exercitiu	
9. Criptosistemul ElGamal	problematizare, exercitiu	
10. Funcții hash	problematizare, exercitiu	
11. Semnături digitale	problematizare, exercitiu	
12. Protocoale legate de chei	problematizare, exercitiu	
13. Aspecte practice	problematizare, exercitiu	
14. Criptografie cuantica	problematizare, exercitiu	

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 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
26.04.2024

Titular de curs
Prof.Dr. Septimiu CRIVEI

Titular de seminar
Prof.Dr. Septimiu CRIVEI

Data avizării în departament

Director de departament
Prof.Dr. Andrei MARCUS