FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea „Lucian Blaga” din Sibiu
1.2 Facultatea / Departamentul	Științe / Departamentul de Matematică și Informatică
1.3 Catedra	Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Masterat
1.6 Programul de studii/Calificarea	Sisteme și Tehnologii Informatice Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei				Criptografie			
2.2 Titularul activităţilor de curs				Lector univ. dr. Daniel Hunyadi			
2.3 Titularul activităţilor de seminar				Lector univ. dr. Daniel Hunyadi			
2.4 Anul de studiu	2	2.5 Semestrul	3	2.6 Tipul de evaluare	Ex	2.7 Regimul disciplinei	O

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	2
3.4 Total ore din planul de învăţământ	56	din care: 3.2 curs	28	3.3 seminar/laborator	28
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					20
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					70
Tutoriat					28
Examinări					2
Alte activităţi					

3.7 Total ore studiu individual	140
3.9 Total ore pe semestru	196
3.10 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 desfăşura seminarului/laboratorului	●

6. Competenţele specifice accumulate

Competențe profesionale	• Cunoaşterea şi utilizarea adecvată a noţiunilor teoretice fundamentale legate de criptografie • Capacitatea de a explica modul de constructie a algoritmilor croptografici • Capacitatea de a interpreta rezultatele obtinute • Capacitatea de a implemnta algoritmi criptografici • Capacitatea de a utiliza si modifica conform cerinteleor algoritmii deja implementati • Capacitatea de a proiecta şi realiza aplicaţii complexe care utilizeaza algoritmii si tehnicile invatate
Competențe transversale	• Dezvoltarea atitudinii pozitive faţă de muncă şi responsabilitate pentru propria pregătire profesională. • Dezvoltarea spiritului de munca in echipa.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Insusirea tehnicilor de criptare, codare, identificare respectiv corectie a erorilor si vulnerabilitatilor. Protectia impotriva atacurilor informatice.
7.2 Obiectivele specifice	Insusirea tehnicilor de criptare, codare, identificare respectiv corectie a erorilor si vulnerabilitatilor. Protectia impotriva atacurilor informatice.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
Scurt istoric al criptografiei. Concepte de baza.	Expunerea, explicatia, exemplificarea si conversatia frontala	
Tehnologii criptografice	Expunerea, explicatia, exemplificarea si conversatia frontala	
Ascunderea informatiilor	Expunerea, explicatia, exemplificarea si conversatia frontala	
Sisteme criptate prin chei secrete (simetrice).	Expunerea, explicatia, exemplificarea si conversatia frontala	
Sisteme de criptare prin chei publice (asimetrice). Sisteme de certificare a cheilor publice.	Expunerea, explicatia, exemplificarea si conversatia frontala	
Semnatura digitala.	Expunerea, explicatia, exemplificarea si conversatia frontala	
Infrastructura cheilor publice.	Expunerea, explicatia, exemplificarea si conversatia	

	frontala	
Atacuri informatice	Expunerea, explicatia, exemplificarea si conversatia frontala	
Validarea tranzacţiilor. Securitatea si securizarea tranzacţiilor.	Expunerea, explicatia, exemplificarea si conversatia frontala	

Bibliografie

1. B. Schneier - Applied Cryptography – Protocols, Algorithms and Source Code in C. Second Edition- John Willey & Sons, 1996
2. J. Menezes, Paul von Oorschot, S. A. Vanstone, Handbook of Applied Cryptography – CRC Press, 1997
3. V. Patriciu, M.Pietrosanu, I. Bica, N. Voicu, C. Vaduva, - Securitatea în comerţul electronic-Ed. All, 2001

8.2 Seminar/laborator	Metode de predare	Observaţii
Algoritmul criptografic, textul cifrat, cheia, codurile, criptanaliza, criptarea.	Explicatia, exemplificarea, invatarea prin descoperire	
Cifrul lui Cezar, Criptografia prin chei simetrice, cifrul lui Vernam, grila lui Cardan.	Explicatia, exemplificarea, invatarea prin descoperire	
Ascunderea informatiei (Steganografia, Filigranarea, Securitatea tiparirii hartiilor de valoare).	Explicatia, exemplificarea, invatarea prin descoperire	
Sisteme criptate prin chei secrete (simetrice: DES, AES, IDEA).	Explicatia, exemplificarea, invatarea prin descoperire	
Sisteme de criptare prin chei publice (asimetrice: Shimbul de chei Diffie-Hellman, RSA). Sisteme de certificare a cheilor publice.	Explicatia, exemplificarea, invatarea prin descoperire	
Semnatura digitala.	Explicatia, exemplificarea, invatarea prin descoperire	
Infrastructura cheilor publice (PKI).	Explicatia, exemplificarea, invatarea prin descoperire	
Atacuri criptografice (forta bruta, text clar (cunoscut, ales, selectat, ...), atac zi de nastere, intalnire la mijloc, om la mijloc, ...)	Explicatia, exemplificarea, invatarea prin descoperire	
Validarea tranzacţiilor. Securitatea si securizarea tranzacţiilor. Erorile sistemelor, calculatoare moleculare.	Explicatia, exemplificarea, invatarea prin descoperire	

Bibliografie

1. M. Howard, D. LeBlanc, Writing Secure Code, Practical strategies and techniques for secure application coding in a networked world, Second Edition, Microsoft, 2002
2. D. Oprea, Protectia si securitatea informatiilor, Ed. Polirom, Iasi, 2003

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

● Algoritmii criptografici predați sunt folosiți în firmele de soft existente pe piața locală, națională și mondială

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs			
10.5 Seminar/laborator	Prezentare proiect	Evaluare pe parcurs	50%
10.6 Standard minim de performanţă			
● Pentru promovarea examenului, trebuie obținută minim nota 5 la proiect și la examenul de evaluare finală			

Data completării,	Semnătura titularului de curs,	Semnătura titularului de seminar,
22.09.2016	.....	.....

Data avizării în catedră

28.09.2016

Semnătura directorului de departament

Prof.univ.dr. Mugur Acu