Anexa 2.

FIŞA DISCIPLINEI*

1. Date despre program

Instituția de învățământ superior	Universitatea Lucian Blaga din Sibiu
Facultatea	Facultatea de Științe
Departament	Departamentul de Matematică și Informatică
Domeniul de studiu	Informatică
Ciclul de studii	Master
Specializarea	Sisteme şi tehnologii informatice avansate

2. Date despre disciplină

Denumirea disciplinei	Criptografie			
Codul cursului	Tipul cursului	An de studiu	Semestrul	Număr de credite
38061003015	O	2	3	6
Tipul de evaluare	Categoria formativă a disciplinei *(DA=aprofundare.; DS=sinteză)*			
E	*DS*			
Titular activități curs	Conf. univ. dr. Nicolae CONSTANTINESCU			
Titular activități seminar / laborator/ proiect	Conf. univ. dr. Nicolae CONSTANTINESCU			

3. Timpul total estimat

Extinderea disciplinei în planul de învățământ – număr de ore pe săptămână				
Curs	Seminar	Laborator	Proiect	Total
1	-	2	-	**3**
Extinderea disciplinei în planul de învățământ – Total ore din planul de învățământ				
Curs	Seminar	Laborator	Proiect	Total ($NOAD_{sem}$)
14		28		**42**

Distribuția fondului de timp pentru studiu individual	Nr.ore
Studiul după manual, suport de curs, bibliografie şi notițe	27
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	27
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	27
Tutoriat:	25
Examinări:	2
Total ore alocate studiului individual ($NOSI_{sem}$)	108
Total ore pe semestru ($NOAD_{sem}$ + $NOSI_{sem}$)	**150**

Adresa: Bd-ul. Victoriei, nr.10
Sibiu 550024, România
e-mail: rectorat@ulbsibiu.ro
www.ulbsibiu.ro
tel: +40-(269) 21.60.62
fax: +40-(269) 21.78.87

4. Precondiţii (acolo unde este cazul)

De curriculum (Discipline necesar a fi promovate anterior)	
De competențe	

5. Condiţii (acolo unde este cazul)

De desfășurare a cursului	Sală de curs, dotată cu tablă, calculator, videoproiector şi software
De desfășurare a laboratorului	Sală de laborator dotată cu calculatoare si soft: mediu de programare

6. Competenţe specifice acumulate

Competențe profesionale	• Cunoașterea şi utilizarea adecvată a noțiunilor teoretice fundamentale legate de criptografie • Capacitatea de a explica modul de construcție a algoritmilor criptografici • Capacitatea de a interpreta rezultatele obținute • Capacitatea de a implementa algoritmi criptografici • Capacitatea de a utiliza si modifica conform cerințelor, algoritmi deja implementați • Capacitatea de a proiecta şi realiza aplicații complexe care utilizează algoritmii si tehnicile învățate
Competenţe transversale	• Dezvoltarea atitudinii pozitive fată de muncă şi responsabilitate pentru propria pregătire profesională. • Dezvoltarea spiritului de munca in echipa

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

Obiectivul general al disciplinei	Însușirea algoritmilor criptografici și a modului în care aceștia pot fi folosiți în diverse situații reale.
Obiectivele specifice	Însușirea tehnicilor de criptare, codare, identificare respectiv corecție a erorilor si vulnerabilităților. Protecția împotriva atacurilor informatice.

8. Conţinuturi

Curs		Nr. ore
Curs 1	Definiția Criptografiei și Criptologiei. Criptografie versus Codificare. Scurt istoric al criptografiei.	1
Curs 2	Tipuri de sisteme de criptare. Definirea criptărilor simetrice și asimetrice.	1
Curs 3	Sisteme simetrice de criptare. Cifruri de substituție.	1
Curs 4	Criptare Polialfabetică. Mașini de cifrare.	1

Curs 5	Protocoale Criptografice. Definiție si tipuri.	1
Curs 6	Diffie Hellman. Man in the middle attack.	1
Curs 7	Generatoare pseudoaleatoare	1
Curs 8	Sisteme de cifrare de tip flux	1
Curs 9	Sisteme de cifrare de tip bloc	1
Curs 10	Metode de atac asupra sistemelor de criptare simetrice	1
Curs 11	Sisteme de criptare asimetrice	1
Curs 12	Semnătura Digitală. Funcții Hash. Trusted Part Based Systems	1
Curs 13	Autentificare. Identificare. Impersonare	1
Curs 14	Sisteme electronice de plată. Votul electronic	1
	Total ore curs:	**14**
Seminar/Laborator		Nr. ore
Lab 1	Implementarea algoritmului lui Cezar	2
Lab 2	Implementarea sistemului de criptare Vigenere	2
Lab 3	Implementarea substituirii monoalfabetice	2
Lab 4	Implementarea cifrurilor de permutare	2
Lab 5	Implementarea unui protocol de stabilire a cheii de sesiune agreată de ambele părti	2
Lab 6	Implementarea unui protocol de stabilire a cheii de sesiune impusă de o parte	2
Lab 7	Implementarea unui generator pseudoaleator	2
Lab 8	Implementarea parametrizării sistemelor de tip flux	2
Lab 9	Implementarea parametrizării sistemelor de tip bloc	2
Lab 10	Testarea metodelor de atac asupra sistemelor de criptare simetrice clasice	2
Lab 11	Implementarea parametrizării sistemelor de criptare asimetric	2
Lab 12	API-uri pentru semnături digitale de tip RSA si ECC	2
Lab 13	API-uri si metode de implementare a modulelor de autentificare	2
Lab 14	API-uri pentru sisteme electronice de plata. Evidențierea limitarilor si optimizări parametrizări lor	2
	Total ore seminar/laborator	28

Metode de predare

Expunerea sistematică a cunoştinţelor (deductivă, inductivă şi formalizată, expuneri beamer/prezi); conversaţia frontala; conversaţia euristică, problematizare, studii de caz, modelarea

Bibliografie

Referinţe bibliografice recomandate	1. Nicolae Constantinescu, Criptografie, Editura Academiei Române, 2009. 2. Douglas R. Stinson, "Cryptography - Theory and Practice", Chapman&Hall/CRC 2002.
Referinţe bibliografice suplimentare	1. Hans Delfs, Helmut Knebl, "Introduction to Cryptography - Principles and Applications", Springer 2002. 2. Colin Boyd, Anish Mathuria, "Protocols for Authentication and Key Establishment", Springer 2003. 3. Arto Saloma, "Public Key Cryptography" Second Edition, Springer 1996.

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

Disciplina Criptografie își găsește aplicabilitatea in majoritatea companiilor IT, atât in formarea de baza în ceea ce privește protecția informației cât și în optimizări ale metodelor existente prin implementări particulare. Materia, prin titularul de curs, este în contact direct cu firmele de profil, pentru evidențierea necesitaților acestora si coordonarea unui schimb de informații care să dinamizeze și adapteze programa. Există un contact permanent și cu lumea științifica din domeniu, prin articolele științifice si contractele de cercetare în care este implicat titularul de curs.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Ponderea în nota finală	Obs.**
Curs	Înțelegerea noțiunilor. Nivelul la care cursanții le pot explica si fundamenta afirmațiile Nivelul tehnic al expunerii termenilor Claritatea si percepția ansamblului problematicii din cadrul materiei	Evaluare Continua Proiect Aplicativ / Studiu fundamental sau Combinat Examen practic si teoretic	50%	nCPE nCPE CEF
Laborator	Capacitatea de sinteza a cunoștințelor dobândite Capacitatea de a adapta exemple făcute pentru probleme similare Capacitatea de generalizare Abilitatea de a alege, implementa și compara tehnicile criptografice pentru o problemă dată. Nivelul tehnic al implementării Claritatea si percepția ansamblului proiectului in lucru	Întocmirea și susținerea unui referat Teme pentru dezvoltarea personală Participare activă la laboratoare Realizarea unui proiect final	50%	nCPE CEF
Standard minim de performanta				

- Cunoașterea noțiunilor de baza din domeniul criptografiei: Definiții, Diferențe intre Criptografie si Codificare
- Cunoașterea principalelor sisteme de criptare clasice.
- Cunoașterea metodelor elementare de autentificare.
- Utilizarea unui API de semnătura digitala.
- Toate aceste cerințe se reflecta in modul de notare pentru a obține nota minima 5

(*) **Fişa disciplinei cuprinde componente adaptate persoanelor cu dizabilităţi, în funcţie de tipul şi gradul acestora.**
(**) CPE – condiţionează participarea la examen; nCPE – nu condiţionează participarea la examen; CEF - condiţionează evaluarea finală;

Data completării: 26.09.2019

Data avizării în Departament: 30.09.2019

	Grad didactic, titlul, prenume, numele	Semnătura
Titular disciplină	Conf. univ. dr. Nicolae CONSTANTINESCU	
Director de departament	Prof. Dr. Mugur ACU	