R40 Anexa 1

FIŞA DISCIPLINEI
(masterat)

1. **Date despre program**

Instituţia de învăţământ superior	**Universitatea „Ştefan cel Mare" Suceava**
Facultatea	**Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor**
Departamentul	**Departamentul de Calculatoare Electronică şi Automatică**
Domeniul de studii	**Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale**
Ciclul de studii	**Masterat**
Programul de studii	**Securitate Cibernetică**

2. **Date despre disciplină**

Denumirea disciplinei	CRIPTOGRAFIA					
Titularul activităţilor de curs	Conf.univ.dr.ing. BALAN Alexandra Ligia					
Titularul activităţilor aplicative	Conf.univ.dr.ing. BALAN Alexandra Ligia					
Anul de studiu	I	Semestrul	1	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DSI – Discipline de sinteză; DAP – Discipline de aprofundare					DSI
	Categoria de opţionalitate a disciplinei: DI - impusă, DO - opţională, DF - facultativă					DI

3. **Timpul total estimat** (ore alocate activităţilor didactice)

I a) Număr de ore, pe săptămână	3	Curs	1	Seminar	1	Laborator	-	Proiect	1
I b) Totalul de ore (pe semestru) din planul de învăţământ	42	Curs	14	Seminar	14	Laborator	-	Proiect	14

II. Distribuţia fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie şi notiţe	18
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	30
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	30
II.d) Tutoriat	2
III. Examinări	3
IV. Alte activităţi (precizaţi):	-

Total ore studiu individual II (a+b+c+d)	80
Total ore pe semestru (Ib+II+III+IV)	125
Numărul de credite	5

4. **Precondiţii** (acolo unde este cazul)

Curriculum	●
Competenţe	●

5. **Condiţii** (acolo unde este cazul)

Desfăşurare a cursului		● PC, videoproiector (prezentări PPT, software specializat)
Desfăşurare aplicaţii	Seminar	● PC, videoproiector (prezentări PPT, software specializat)
	Laborator	●
	Proiect	● PC, videoproiector (prezentări PPT, software specializat)

6. **Competenţe specifice acumulate**

Competenţe profesionale	C1. Operarea cu fundamente tehnice și științifice în tehnologia informației și comunicațiilor, orientate cu precădere către aria Securității Cibernetice C5. Identificarea și combaterea riscurilor și pericolelor privind expunerea sistemelor informatice la atacuri cibernetice C6. Soluționarea incidentelor de securitate folosind instrumente specifice, proiectarea și dezvoltarea de instrumente și aplicații specifice securității cibernetice
Competenţe transversale	●

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

Obiectivul general al disciplinei	● Obiectivul general al acestei discipline este de a prezenta paradigmele și principiile de bază ale criptografiei moderne.
Obiective specifice	● Utilizarea conceptelor fundamentale ale criptografiei ● Descrierea diferențelor dintre criptografia simetrică și cea asimetrică ● Identificarea şi analiza cerințelor de bază pentru criptografie ● Înțelegerea naturii riscurilor și tipurile de amenințări ale sistemelor cibernetice ● Înțelegerea metodelor și strategiilor de protejare a datelor cu privire la software, rețele de calculatoare și comunicații, precum și la alte sisteme informatice și cibernetice. ● Descrierea procesului de implementare a sistemelor criptografice. Definirea conceptului de management al cheilor. Definirea infrastructurii cu cheie publică. Identificarea proceselor pentru administrarea și validarea cheilor ● Conștientizarea vulnerabilităților software, ale rețelelor și sistemelor informatice.

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
● Criptografie și criptoanaliza. Fundamente aritmetice. Introducere în teoria numerelor. Generatoare de numere pseudo-aleatoare.	3	prelegerea, conversația, exemplificarea.	
● Criptografia clasică	1		
● Cifruri bloc : DES și AES.	2		
● Scheme de criptare asimetrică / Criptografia cu cheie publică (PKC)	2		
● Funcții hash criptografice	2		
● Sisteme criptografice asimetrice bazate pe curbe eliptice	2		
● Semnături digitale	2		
Bibliografie			
● Song Y. Yan, Computational Number Theory and Modern Cryptography, ed. John Wiley & Sons Ltd., 2013, ISBN: 978-1-118-18858-3 ● William Stallings, Cryptography and Network Security Principles and Practice, ed. Pearson Education Limited, 2020, ● Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, ed. CRC Press, 2021			

Aplicaţii (**Seminar**)	Nr. ore	Metode de predare	Observaţii
S1. Noțiuni introductive de criptografie și criptoanaliza. Funcții de criptare utilizate în MATLAB. Conversii utilizate în MATLAB pentru criptare. Fundamente aritmetice. Teoria numerelor. Generatoare de numere pseudo-aleatoare.	2	prelegerea, conversația, exemplificarea.	
S2. Criptografia clasică	2		
S3. Cifruri bloc : DES și AES.	2		
S4. Scheme de criptare asimetrică / Criptografia cu cheie publică (PKC)	2		
S5. Funcții hash criptografice	2		
S6. Sisteme criptografice asimetrice bazate pe curbe eliptice	2		
S7. Semnături digitale	2		
Aplicaţii **(Proiect)**	Nr. ore	Metode de predare	Observaţii
Analiza și implementarea unor mecanisme de securitate utilizând diverși algoritmi criptografici:		prelegerea, conversația, exemplificarea.	
1. AES (Advanced Encryption Standard)	2		
2. DES (Data Encryption Standard)	2		
3. RSA (Rivest–Shamir–Adleman Algorithm)	2		
4. DSA (Digital Signature Algorithm)	2		
5. 3-DES	2		

6.	ElGamal	2		
7.	Hash functions	2		

Bibliografie

- M.I. Mihailescu, S. L. Nita, Cryptography and Cryptanalysis in MATLAB, ed. Apress., 2021
- Song Y. Yan, Computational Number Theory and Modern Cryptography, ed. John Wiley & Sons Ltd., 2013, ISBN: 978-1-118-18858-3
- William Stallings, Cryptography and Network Security Principles and Practice, ed. Pearson Education Limited, 2020,
- Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, ed. CRC Press, 2021

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

Conținutul cursului, laboratorului și al proiectului este în concordanță cu cerințele societății actuale și se caracterizează printr-o abordare interdisciplinară adaptată realităților și nevoilor contemporane, care permite acumularea de cunoștințe, dezvoltarea de abilități și reflectă creșterea gradului de responsabilitate și autonomie.

http://staff.cs.upt.ro/~chirila/facultate/planuri/syllabus/master/msisc/1.1_Fisa_disciplinei_SISC_Tehnici_criptografice_moderne_rom.pdf
https://tcsi.ro/fise_discipline/3_Fisa-disciplinei_CC.pdf
https://crypto.stanford.edu/~dabo/cs255/syllabus.html
https://www.cs.columbia.edu/~tal/4261/S22/index.htm

10. **Evaluare**

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- completitudinea şi corectitudinea cunoştinţelor; - coerenţa logică, fluenţa, expresivitatea, forţa de argumentare; - capacitatea de a opera cu cunoştinţele asimilate în activităţi intelectuale	Evaluare prin metode scrise şi orale	**50%**
Seminar	- capacitatea de aplicare în practică, în contexte diferite, a cunoştinţelor învăţate; - capacitatea de analiză, de interpretare personală, originalitatea, creativitatea.	Evaluare prin metode orale şi probe practice.	**25%**
Proiect	- capacitatea de aplicare în practică, în contexte diferite, a cunoştinţelor învăţate; - capacitatea de analiză, de interpretare personală, originalitatea, creativitatea.	Evaluare prin metode orale şi probe practice.	**25%**

Standard minim de performanţă

Cunoaşterea noţiunilor teoretice de bază prezentate la curs şi rezolvarea unor probleme tip.

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie
23.09.2022		

Data avizării în departament	Semnătura directorului de departament
26.09.2022	

Data aprobării în consiliul facultăţii	Semnătura decanului
30.09.2022	