

FIȘA DISCIPLINEI

(masterat)

1. Date despre program

Instituția de învățământ superior	Universitatea „Ștefan cel Mare” Suceava
Facultatea	Facultatea de Inginerie Electrică și Știința Calculatoarelor
Departamentul	Departamentul de Calculatoare Electronice și Automatică
Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
Ciclul de studii	Masterat
Programul de studii	Securitate Cibernetică

2. Date despre disciplină

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

3. Timpul total estimat (ore alocate activităților didactice)

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

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

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

4. Precondiții (acolo unde este cazul)

Curriculum	•
Competențe	•

5. Condiții (acolo unde este cazul)

Desfășurare a cursului	• PC, videoproiector (prezentări PPT, software specializat)	
Desfășurare aplicații	Seminar	• PC, videoproiector (prezentări PPT, software specializat)
	Laborator	•
	Proiect	• PC, videoproiector (prezentări PPT, software specializat)

6. Competențe specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> • C1. Operarea cu fundamente tehnice și științifice în tehnologia informației și comunicațiilor, orientate cu precizie • 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
-------------------------	--

Competențe transversale	•
-------------------------	---

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

Obiectivul general al disciplinei	<ul style="list-style-type: none"> • Obiectivul general al acestei discipline este de a prezenta paradigmele și principiile de bază ale criptografiei moderne. •
-----------------------------------	--

8. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
• Criptografie și criptoanaliza. Fundamente aritmetice. Introducere în teoria numerelor. Generatoare de numere pseudo-aleatoare.	3	prelegerea, conversația, demonstrația, 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			
<ul style="list-style-type: none"> • 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 			

Aplicații (Seminar)	Nr. ore	Metode de predare	Observații
• 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, demonstrația, 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		
Aplicații (Proiect)			
Analiza și implementarea unor mecanisme de securitate utilizând diverși algoritmi criptografici:			
• AES (Advanced Encryption Standard)	2	prelegerea, conversația, demonstrația, exemplificarea.	
• DES (Data Encryption Standard)	2		
• RSA (Rivest–Shamir–Adleman Algorithm)	2		
• DSA (Digital Signature Algorithm)	2		
• 3-DES	2		
• ElGamal	2		
• Funcții Hash	2		
Bibliografie			
<ul style="list-style-type: none"> • 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 conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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 și corectitudinea cunoștințelor; - coerența logică, fluența, expresivitatea, forța de argumentare; - capacitatea de a opera cu cunoștințele asimilate în activități intelectuale	Examen oral	50%
Seminar	- capacitatea de aplicare în practică, în contexte diferite, a cunoștințelor învățate; - capacitatea de analiză, de interpretare personală, originalitatea, creativitatea.	Evaluare prin metode orale și probe practice.	20%
Proiect	- capacitatea de aplicare în practică, în contexte diferite, a cunoștințelor învățate; - capacitatea de analiză, de interpretare personală, originalitatea, creativitatea.	Evaluare prin metode orale și probe practice.	30%
Standard minim de performanță			
<ul style="list-style-type: none"> • Cunoașterea noțiunilor teoretice de bază prezentate la curs și rezolvarea unor probleme tip. 			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicație
20.09.2023		

Data avizării	Semnătura responsabilului de program
20.09.2023	

Data avizării în departament	Semnătura directorului de departament
22.09.2023	

Data aprobării în consiliul facultății	Semnătura decanului
27.09.2023	