

## FIȘA DISCIPLINEI

(licență)

### 1. Date despre program

Instituția de învățământ superior	Universitatea "Ștefan cel Mare" din Suceava
Facultatea	Facultatea de Inginerie Electrică și Știința Calculatoarelor
Departamentul	Calculatoare, Electronică și Automatică
Domeniul de studii	Inginerie electronică, telecomunicații și tehnologii informaționale
Ciclul de studii	Licență
Programul de studii	Rețele și software de telecomunicații

### 2. Date despre disciplină

Denumirea disciplinei	<b>Securitatea comunicațiilor de date</b>				
Titularul activităților de curs	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ				
Titularul activităților aplicative	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ				
Anul de studiu	IV	Semestrul	8	Tipul de evaluare	E
Regimul disciplinei	Categorია formativă a disciplinei DF - fundamentală, DD - în domeniu, DS - de specialitate, DC – complementară				DS
	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	4	Curs	2	Seminar	-	Laborator/lucrări practice	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învățământ	56	Curs	28	Seminar	-	Laborator/lucrări practice	28	Proiect	-

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	7
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	16
II d) Tutoriat	
III Examinări	3
IV Alte activități (precizați):	

Total ore studiu individual II (a+b+c+d)	41
Total ore pe semestru (Ib+II+III+IV)	100
Numărul de credite	4

### 4. Precondiții (acolo unde este cazul)

Curriculum	•
Competențe	•

### 5. Condiții (acolo unde este cazul)

Desfășurare a cursului	• laptop, videoproiector, tablă, suporturi electronice pentru unitatea de curs	
Desfășurare aplicații	Seminar	• -
	Laborator/lucrări practice	• calculatoare, software specializat, laptop, videoproiector, tablă, suport electronic pentru aplicații
	Proiect	• -

### 6. Competențe specifice acumulate

Competențe profesionale	C5. Proiectarea infrastructurii de comunicații, adaptarea arhitecturilor, tehnologiilor și protocoalelor de telecomunicații pentru aplicații suport de rețele locale, metropolitane, de arie mare și integrate
-------------------------	--

	C6. Utilizarea limbajelor și instrumentelor specializate pentru inginerie software, cu orientare către sistemele de telecomunicații integrate
Competențe transversale	

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

Obiectivul general al disciplinei	<ul style="list-style-type: none"> <li>• Însușirea cunoștințelor fundamentale referitoare la algoritmi de criptare cu cheie privată și publică</li> <li>• Înțelegerea principiilor de proiectare și analiză a unor protocoale de comunicație sigure</li> </ul>
-----------------------------------	--

### 8. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
1. Introducere în criptografie 1.1. Istoric 1.2. Terminologie 1.3. Criptografia modernă - cerințe	2	expunerea, prelegerea participativă, conversația, demonstrația, exemplificare, studiu de caz	
2. Algoritmi de criptare clasici 2.1. Cifruri de substituție 2.1.1. Cifruri monoalfabetice: Cezar, afin, Polybios 2.1.2. Cifruri polialfabetice: Playfair, Vigenère 2.1.3. Metode de criptanaliză 2.2. Cifruri cu transpoziție	4		
3. Sisteme mecanice de criptare 3.1. sistemul Skitala 3.2. criptograful lui Alberti 3.3. cilindrul Jefferson	2		
4. Mașini de criptare: mașina Enigma 4.1. Istoric 4.2. Prezentare generală 4.3. Detalii tehnice 4.4. Exemple de criptare / decriptare 4.5. Stabilirea cheilor și a modului de funcționare 4.6. Complexitatea mașinii Enigma 4.7. Slăbiciunile mașinii Enigma. Concluzii	2		
5. Importanța cheilor 5.1. Criptografia cu cheie privată. Descriere. Exemple. 5.2. Criptografia cu cheie publică. Descriere. Exemple.	2		
6. Algoritmi simetrici de criptare 6.1. Cifruri bloc. Rețeaua Feistel 6.2. Algoritmul DES (Data Encryption Standard) 6.2.1. Istoric 6.2.2. Introducere în DES 6.2.3. DES, descriere în detaliu a criptării 6.2.4. DES, descriere în detaliu a decriptării 6.2.5. Controverse 6.2.6. Variante ale DES (Triple DES, DES-X)	2		
7. Algoritmul AES (Advanced Encryption Standard) 7.1. Motivația unui nou standard 7.2. Cerințe inițiale 7.3. Candidații (MARS, RC6, Rijndael, Serpent, Twofish) 7.4. Evaluare finală a candidaților. Considerații 7.5. Preliminarii matematice – câmpuri Galois 7.6. Descrierea algoritmului AES (Rijndael) 7.7. Implementarea algoritmului AES	2		
8. Algoritmul de criptare RSA 8.1. Elemente de Matematică 8.2. Prezentarea algoritmului 8.3. Exemple de criptare / decriptare	2		
9. Algoritmi de criptare ce folosesc funcții de dispersie	2		

9.1. Securitatea algoritmilor de criptare ce se bazează pe funcții de dispersie			
9.2. Algoritmul MD5. Istoric. Descriere in detaliu. Exemple.			
9.3. Algoritmul SHA-1. Descriere in detaliu. Exemple			
10. Semnături digitale	2		
11. Atacuri criptografice	2		
12. Securizarea codului/aplicațiilor	2		
13. Securitatea bazelor de date	2		
<b>Bibliografie</b>			
1. Adrian Atanasiu, <i>Securitatea informației, voll:Criptografie</i> , Editura InfoData, ISBN 978-973-1803-16-6, 2007			
2. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, <i>Criptografie și securitatea informației. Aplicații</i> , Editura Matrixrom, ISBN 9789737556752, 2011			
3. Dumitru Oprea, <i>Protecția și securitatea informațiilor</i> , Editura Polirom, ISBN 978-973-46-0927-7, 2007			
4. Michael Welschenbach, <i>Cryptography in C and C++</i> , Second Edition, Apress, ISBN 1-59059-502-5, 2005			
5. Douglas R. Stinson, Maura B. Paterson, <i>Cryptography: Theory and Practice (4th Edition)</i> , CRC Press, ISBN 978-1-1381-9701-5, 2018			
6. Rolf Oppliger, <i>Cryptography 101: From theory to practice</i> , Artech House, ISBN 13: 978-1-63081-846-3, 2021			
7. Bruce Schneier, <i>Applied Cryptography: Protocols, Algorithms, and Source Code in C</i> , 20 <sup>th</sup> Anniversary Edition, Wiley, ISBN: 978-1-119-09672-6, 2015			
8. Marcelo Sampaio de Alencar, <i>Cryptography and Network Security</i> , River Publishers, ISBN 978-87-7022-406-2 , 2022			
9. Adina Bărlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom			
<b>Bibliografie minimală</b>			
1. Adrian Atanasiu, <i>Securitatea informației, voll:Criptografie</i> , Editura InfoData, ISBN 978-973-1803-16-6, 2007			
2. Adina Bărlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom			

Aplicații (Seminar / <b>laborator</b> / lucrări practice / proiect)	Nr. ore	Metode de predare	Observații
1. Prezentarea normelor de protecția și igiena muncii. Implementarea cifrului lui Cezar	2	expunere, lucrări practice, exercițiu, dezbateri	
2. Implementarea cifrului PlayFair	2		
3. Implementarea cifrului Vigenere	2		
4. Implementarea cifrului cu transpoziție	2		
5. Implementarea algoritmului DES	2		
6. Implementarea algoritmului AES	2		
7. Implementarea criptării RSA	2		
8. Implementarea decriptării RSA	2		
9. Funcții hash	2		
10. Ghid de bune practici pentru securitate cibernetică	2		
11. Controlul accesului	2		
12. Semnături digitale	2		
13. Atacuri criptografice – studii de caz	4		
<b>Bibliografie</b>			
1. Adrian Atanasiu, <i>Securitatea informației, voll:Criptografie</i> , Editura InfoData, ISBN 978-973-1803-16-6, 2007			
2. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, <i>Criptografie și securitatea informației. Aplicații</i> , Editura Matrixrom, ISBN 9789737556752, 2011			
3. Dumitru Oprea, <i>Protecția și securitatea informațiilor</i> , Editura Polirom, ISBN 978-973-46-0927-7, 2007			
4. Michael Welschenbach, <i>Cryptography in C and C++</i> , Second Edition, Apress, ISBN 1-59059-502-5, 2005			
5. Douglas R. Stinson, Maura B. Paterson, <i>Cryptography: Theory and Practice (4th Edition)</i> , CRC Press, ISBN 978-1-1381-9701-5, 2018			
6. Rolf Oppliger, <i>Cryptography 101: From theory to practice</i> , Artech House, ISBN 13: 978-1-63081-846-3, 2021			
7. Bruce Schneier, <i>Applied Cryptography: Protocols, Algorithms, and Source Code in C</i> , 20 <sup>th</sup> Anniversary Edition, Wiley, ISBN: 978-1-119-09672-6, 2015			
8. Marcelo Sampaio de Alencar, <i>Cryptography and Network Security</i> , River Publishers, ISBN 978-87-7022-406-2 , 2022			
9. Adina Bărlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom			

**Bibliografie minimală**

1. Adrian Atanasiu, *Securitatea informației, voll: Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. Adina Bărlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

**9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului**

Conținutul cursului și al laboratorului este în concordanță cu așteptările reprezentanților comunității epistemice și angajatorilor reprezentativi din domeniul calculatoarelor și tehnologiei informației. De asemenea, conținutul cursului și al laboratorului se regăsește în curricula disciplinelor similare de la universități din țară sau străinătate, cum ar fi:

- Universitatea din București/FMI – Securitatea sistemelor informatice  
<https://cursuri.fmi.unibuc.ro/api/uploads/86c717d5-c7a6-4a60-bfad-35da223ac873.pdf>
- Universitatea Politehnică Timișoara/FAC – Securitatea informației  
<https://ac.upt.ro/specializari/informatica/>
- Stanford University - CS255: Introduction to Cryptography  
<http://crypto.stanford.edu/~dabo/cs255>
- University of Illinois - CS/ECE 407: Cryptography  
<https://courses.grainger.illinois.edu/CS407/fa2023/>
- University of California, Berkeley - CS 261 Computer Security  
<https://people.eecs.berkeley.edu/~daw/teaching/cs261-s21/>
- University of Toledo - EECS 4980 - Cryptography course  
<https://www.utoledo.edu/engineering/electrical-engineering-computer-science/current-students/syllabi/eecs-4980-inside-cryptography.html>
- Texas A&M University - CSCI5323:001, Cryptography/Secure Communication  
<https://apps.tamusa.edu/course-information/syllabi/Fall2023/Cryptography-Secure-Comm-CSCI-5323-001.pdf>

**10. Evaluare**

10.1. Standard minim de performanță evaluare la curs

10.2. Standard minim de performanță evaluare la activitatea aplicativă

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	-cunoașterea terminologiei utilizate -însușirea algoritmilor de criptare fundamentali -abilitatea de rezolvare a unor probleme specifice domeniului	evaluare finală: probă scrisă urmată de verificarea orală a gradului de îndeplinire a cerințelor în lucrarea scrisă	50%
Seminar	-		
Laborator	-însușirea algoritmilor specifici domeniului -capacitatea de implementare a algoritmilor specifici domeniului - abilitatea de rezolvare a unor probleme specifice domeniului	probă practică	50%
Proiect			

**Standard minim de performanță**

**Curs:**

- însușirea noțiunilor fundamentale și utilizarea terminologiei
- capacitatea de a descrie din punct de vedere logic, sub forma de prezentare liberă, a cel puțin 3 algoritmi de criptare

**Laborator:**

- capacitatea de a implementa un algoritm clasic de criptare

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicație
18.09.2024		

Data avizării	Semnătura responsabilului de program
20.09.2024	

Data avizării în departament	Semnătura directorului de departament
23.09.2024	

Data aprobării în consiliul facultății	Semnătura decanului
27.09.2024	

