FIŞA DISCIPLINEI
(licenţă)

1. **Date despre program**

Instituţia de învăţământ superior	Universitatea "Ştefan cel Mare" din Suceava
Facultatea	Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor
Departamentul	Calculatoare, Electronică şi Automatică
Domeniul de studii	Inginerie electronică, telecomunicaţii şi tehnologii informaţionale
Ciclul de studii	Licenţă
Programul de studii	Rețele și software de telecomunicații

2. **Date despre disciplină**

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

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	7
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	16
II d) Tutoriat	
III Examinări	3
IV Alte activităţi (precizaţi):	

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

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

Curriculum	•
Competenţe	•

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

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

6. **Competenţe specifice acumulate**

Competenţe profesionale	C5. Proiectarea infrastructurii de comunicaţii, adaptarea arhitecturilor, tehnologiilor şi protocoalelor de telecomunicaţii pentru aplicaţii suport de reţele locale, metropolitane, de arie mare şi integrate

	C6. Utilizarea limbajelor şi instrumentelor specializate pentru inginerie software, cu orientare către sistemele de telecomunicaţii integrate
Competenţe transversale	

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

Obiectivul general al disciplinei	• Însuşirea cunoştinţelor fundamentale referitoare la algoritmi de criptare cu cheie privată şi publică
	• Înțelegerea principiilor de proiectare și analiză a unor protocoale de comunicație sigure

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Introducere în criptografie 1.1. Istoric 1.2. Terminologie 1.3. Criptografia modernă - cerinţe	2	expunerea, prelegerea participativă, conversaţia, demonstraţia, exemplificare, studiu de caz	
2. Algoritmi de criptare clasici – cifruri de substituție 2.1. Cifruri monoalfabetice: Cezar, afin, Polybios 2.2. Cifruri polialfabetice: Playfair, Vigenère 2.3. Metode de criptanaliză	4		
3. Algoritmi de criptare clasici – cifruri cu tramspoziție	2		
4. Sisteme mecanice de criptare 4.1. sistemul Skitala 4.2. criptograful lui Alberti 4.3. cilindrul Jefferson	2		
5. Mașini de criptare: maşina Enigma 5.1. Istoric 5.2. Prezentare generală 5.3. Detalii tehnice 5.4. Exemple de criptare / decriptare 5.5. Stabilirea cheilor şi a modului de funcţionare 5.6. Complexitatea maşinii Enigma 5.7. Slăbiciunile maşinii Enigma. Concluzii	2		
6. Importanţa cheilor 6.1. Criptografia cu cheie privată. Descriere. Exemple. 6.2. Criptografia cu cheie publică. Descriere. Exemple.	2		
7. Algoritmi simetrici de criptare 7.1. Cifruri bloc. Rețeaua Feistel 7.2. Algoritmul DES (Data Encryption Standard) 7.2.1. Istoric 7.2.2. Introducere în DES 7.2.3. DES, descriere în detaliu a criptării 7.2.4. DES, descriere în detaliu a decriptării 7.2.5. Controverse 7.2.6. Variante ale DES (Triple DES, DES-X)	4		
8. Algoritmul AES (Advanced Encryption Standard) 8.1. Motivaţia unui nou standard 8.2. Cerinţe iniţiale 8.3. Candidaţii (MARS, RC6, Rijndael, Serpent, Twofish) 8.4. Evaluare finală a candidaţilor. Consideraţii 8.5. Preliminarii matematice – câmpuri Galois 8.6. Descrierea algoritmului AES (Rijndael) 8.7. Implementarea algoritmului AES	2		
9. Algoritmul de criptare RSA 9.1. Elemente de Matematică 9.2. Prezentarea algoritmului 9.3. Exemple de criptare / decriptare	2		
10. Algoritmi de criptare ce folosesc funcţii de dispersie 10.1. Securitatea algoritmilor de criptare ce se bazează	2		

pe funcții de dispersie 10.2. Algoritmul MD5. Istoric. Descriere in detaliu. Exemple. 10.3. Algoritmul SHA-1. Descriere in detaliu. Exemple			
11. Semnături digitale	2		
12. Atacuri criptografice	2		

Bibliografie

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, *Criptografie și securitatea informației. Aplicații*, Editura Matrixrom, ISBN 9789737556752, 2011
3. Dumitru Oprea, *Protecția și securitatea informațiilor,* Editura Polirom, ISBN 978-973-46-0927-7, 2007
4. Michael Welschenbach, *Cryptography in C and C++*, Second Edition, Apress, ISBN 1-59059-502-5**,** 2005
5. Douglas R. Stinson, Maura B. Paterson, *Cryptography: Theory and Practice (4th Edition)*, CRC Press, ISBN 978-1-1381-9701-5, 2018
6. Rolf Oppliger, *Cryptography 101: From theory to practice*, Artech House, ISBN 13: 978-1-63081-846-3, 2021
7. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 20th Anniversary Edition, Wiley, ISBN: 978-1-1 19-09672-6, 2015
8. Marcelo Sampaio de Alencar, *Cryptography and Network Security*, River Publishers, ISBN 978-87-7022-406-2 , 2022
9. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

Bibliografie minimală

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

Aplicaţii (Seminar / **laborator** / lucrări practice / proiect)	Nr. ore	Metode de predare	Observaţii
1. Prezentarea normelor de protecţia şi igiena muncii. Implementarea cifrului lui Cezar	2	expunere, lucrări practice, exerciţiu, dezbatere	
2. Implementarea cifrului PlayFair	2		
3. Implementarea cifrului Vigenere	2		
4. Implementarea cifrului cu transpoziție	2		
5. Implementarea criptării /decriptării Enigma	2		
6. Implementarea DES – diversificarea cheii	2		
7. Implementarea criptării/decriptării DES	2		
8. Implementarea algoritmului AES	2		
9. Implementarea criptării RSA	2		
10. Implementarea decriptării RSA	2		
11. Funcții hash	2		
12. Semnături digitale	2		
13. Atacuri criptografice – studii de caz	4		

Bibliografie

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, *Criptografie și securitatea informației. Aplicații*, Editura Matrixrom, ISBN 9789737556752, 2011
3. Dumitru Oprea, *Protecția și securitatea informațiilor,* Editura Polirom, ISBN 978-973-46-0927-7, 2007
4. Michael Welschenbach, *Cryptography in C and C++*, Second Edition, Apress, ISBN 1-59059-502-5**,** 2005
5. Douglas R. Stinson, Maura B. Paterson, *Cryptography: Theory and Practice (4th Edition)*, CRC Press, ISBN 978-1-1381-9701-5, 2018
6. Rolf Oppliger, *Cryptography 101: From theory to practice*, Artech House, ISBN 13: 978-1-63081-846-3, 2021
7. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 20th Anniversary Edition, Wiley, ISBN: 978-1-1 19-09672-6, 2015
8. Marcelo Sampaio de Alencar, *Cryptography and Network Security*, River Publishers, ISBN 978-87-7022-406-2 , 2022
9. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

Bibliografie minimală

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

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

Cursuri asemanatoare din comunitatea academica si industrie:
CS255: Introduction to Cryptography
http://crypto.stanford.edu/~dabo/cs255/
Applied Cryptography
https://www.udacity.com/course/cs387
Cryptography and Cryptanalysis
http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-875-cryptography-and-cryptanalysis-spring-2005/
Cryptographer and Entrepreneur
http://saweis.net/crypto.html
Applied Cryptography
http://courses.engr.illinois.edu/cs598man/fa2009/
CSE 107 Introduction to Modern Cryptography
http://cseweb.ucsd.edu/users/mihir/cse107/
CSE 207 Modern Cryptography
http://cseweb.ucsd.edu/~mihir/cse207/
An introduction to cryptography
https://www.ice.cam.ac.uk/component/courses/?view=course&cid=3779
650.445: PRACTICAL CRYPTOGRAPHIC SYSTEMS
http://spar.isi.jhu.edu/~mgreen/650.445/650.445__Main.html
CS 276 Cryptography
http://www.cs.berkeley.edu/~daw/teaching/cs276-s06/

10. **Evaluare**
10.1. Standard minim de performanţă evaluare la curs
10.2. Standard minim de performanţă 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 performanţă			
Curs: - însușirea noțiunilor fundamentale și utilizarea terminologiei - capacitatea de a descrie din punct de vedere logic, sub forma de prezentare libera, 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 aplicaţie
19.09.2023		

Data avizării	Semnătura responsabilului de program
20.09.2023	

Data avizării în departament	Semnătura directorului de departament
22.09.2023	

Data aprobării în consiliul facultăţii	Semnătura decanului
22.09.2023	