FIȘA DISCIPLINEI

1. Date despre program

Facultatea	**Inginerie Electrică şi Ştiinţa Calculatoarelor**
Departamentul	**Calculatoare**
Domeniul de studii	**Calculatoare și tehnologia informației**
Ciclul de studii	**Licență**
Programul de studii	**Calculatoare**

2. Date despre disciplină

Denumirea disciplinei	**CRIPTOGRAFIE ŞI SECURITATE INFORMAȚIONALĂ**					
Anul de studiu	IV	Semestrul	8	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DF - fundamentală, DS - de specializare, DC – complementară					DS
	Categoria de opționalitate a disciplinei: DOB – obligatorie, DOP – opțională, DFA - facultativă					DOP

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

I a) Număr de ore pe săptămână	3,5	Curs	2	Seminar	-	Laborator/lucrări practice	1,5	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	49	Curs	28	Seminar	-	Laborator/lucrări practice	21	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II.a) Studiu individual	48
II.b) Tutoriat (pentru ID)	
III. Examinări	3
IV. Alte activități (precizați):	

Total ore studiu individual (II.a+II.b+III)	51
Total ore pe semestru (I.b+II.a+II.b+III+IV)	100
Numărul de credite	4

4. Competențe specifice acumulate

Competenţe profesionale	CP04 creează softuri CP12 utilizează biblioteci de software CP19 întreține configurarea protocoalelor de internet CP22 modelează și simulează hardware
Competenţe transversale	CT1 munca in echipa CT6 își asumă responsabilitatea

5. Rezultatele învățării

Cunoștințe	Aptitudini	Responsabilitate și autonomie
Studentul/absolventul ● identifică și descrie concepte de criptografie aplicată şi securitate a aplicaţiilor ● analizează funcționarea și performanța algoritmilor moderni de criptare ● identifică principalele tipuri de atacuri criptografice și propune măsuri de protecție împotriva	Studentul/absolventul ● aplică practici de inginerie software şi integrează mecanisme de criptare, autentificare și protecţie la atacuri cibernetice ● utilizează biblioteci criptografice standard pentru dezvoltarea de aplicații sigure	Studentul/absolventul gestionează întregul flux al unui proiect software (de la idee la livrare și mentenanță), colaborează eficient în echipe multidisciplinare, documentează clar procesele și respectă legislația și standardele etice privind protecţia datelor și proprietatea intelectuală.

acestora		

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

Obiectivul general al disciplinei	● Însuşirea conceptelor fundamentale ale criptografiei moderne și familiarizarea cu metodele utilizate pentru securizarea sistemelor informatice

7. Conținutul predării și învățării

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 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 tramspoziție	4		
3. Sisteme mecanice de criptare 3.1. sistemul Skitala 3.2. criptograful lui Alberti 3.3. cilindrul Jefferson 3.4. mașina Enigma	2		
4. Algoritmi de criptare simetrică 4.1. Cifruri bloc. Rețeaua Feistel 4.2. Algoritmul DES (Data Encryption Standard) 4.2.1. Istoric 4.2.2. Descriere algoritm 4.2.3. DES, descriere în detaliu a criptării 4.2.4. DES, descriere în detaliu a decriptării 4.2.5. Controverse 4.2.6. Variante ale DES (Triple DES, DES-X) 4.3. Algoritmul AES (Advanced Encryption Standard) 4.3.1. Motivaţia unui nou standard 4.3.2. Preliminarii matematice – câmpuri Galois 4.3.3. Descrierea algoritmului 4.4. Algoritmul Blowfish	4		
5. Algoritmi de criptare asimetrică 5.1. Algoritmul RSA 5.1.1. Elemente de Matematică 5.1.2. Prezentarea algoritmului 5.1.3. Exemple de criptare / decriptare 5.2. Algoritmul ECC (criptografie pe curbe eliptice)	4		
6. Funcții hash 6.1. Securitatea algoritmilor de criptare ce se bazează pe funcţii hash 6.2. Algoritmul MD5 6.2.1. Istoric. 6.2.2. Descriere 6.3. Algoritmul SHA 6.4. Funcția bcrypt	2		
7. Semnături digitale	2		
8. Securizarea codului/aplicațiilor	2		
9. Securitatea bazelor de date	2		
10. Atacuri criptografice	2		
11. Criptografie cuantică	2		

Bibliografie minimală recomandată

1. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, *Criptografie și securitatea informației. Aplicații*, Editura Matrixrom, ISBN 9789737556752, 2011

2. Dumitru Oprea, *Protecția și securitatea informațiilor,* Editura Polirom, ISBN 978-973-46-0927-7, 2007
3. Douglas R. Stinson, Maura B. Paterson, *Cryptography: Theory and Practice (4th Edition),* CRC Press, ISBN 978-1-1381-9701-5, 2018
4. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 20th Anniversary Edition, Wiley, ISBN: 978-1-1 19-09672-6, 2015
5. Marcelo Sampaio de Alencar, *Cryptography and Network Security*, River Publishers, ISBN 978-87-7022-406-2 , 2022
6. 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 unui cifru polialfabetic	2		
3. Implementarea cifrului cu transpoziție	2		
4. Evaluare	2		
5. Implementarea algoritmului DES	2		
6. Implementarea algoritmului AES	2		
7. Implementarea algoritmului RSA	2		
8. Funcții hash	2		
9. Semnături digitale	2		
10. Evaluare	2		
11. Securitatea bazelor de date	1		

Bibliografie minimală recomandată

1. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, *Criptografie și securitatea informației. Aplicații*, Editura Matrixrom, ISBN 9789737556752, 2011
2. Dumitru Oprea, *Protecția și securitatea informațiilor,* Editura Polirom, ISBN 978-973-46-0927-7, 2007
3. Douglas R. Stinson, Maura B. Paterson, *Cryptography: Theory and Practice (4th Edition),* CRC Press, ISBN 978-1-1381-9701-5, 2018
4. Rolf Oppliger, *Cryptography 101: From theory to practice*, Artech House, ISBN 13: 978-1-63081-846-3, 2021
5. Marcelo Sampaio de Alencar, *Cryptography and Network Security*, River Publishers, ISBN 978-87-7022-406-2 , 2022
6. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

8. Evaluare

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/ Lucrări practice	-însușirea algoritmilor specifici domeniului -capacitatea de implementare a algoritmilor specifici domeniului - abilitatea de rezolvare a unor probleme specifice domeniului	probă practică	50%
Proiect			

Fișa disciplinei include, dacă este cazul, elemente adaptate persoanelor cu dizabilități, în funcție de tipul și gradul acestora.

Data completării	Grad didactic, nume, prenume, semnătura titularului de curs	Grad didactic, nume, prenume, semnătura titularului de aplicație
25.09.2025	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ

Data avizării	Grad didactic, nume, prenume, semnătura responsabilului de program
25.09.2025	Prof. univ. dr. ing. Cristina Elena TURCU

Data avizării în departament	Grad didactic, nume, prenume, semnătura directorului de departament
25.09.2025	Prof. univ. dr. ing. Ovidiu-Andrei SCHIPOR

Data aprobării în consiliul facultății	Grad didactic, nume, prenume, semnătura decanului
26.09.2025	Prof. univ. dr. ing. Laurențiu-Dan MILICI