FIȘA DISCIPLINEI

1. **Date despre program**

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**				
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: DO - obligatorie (impusă), DA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

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	-

Distribuția fondului de timp pe semestru	ore
II.a) Studiu individual	41
II.b) Tutoriat (pentru ID)	
III. Examinări	3
IV. Alte activități (precizați): Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	

Total ore studiu individual (II.a+II.b+III)	44
Total ore pe semestru (I.b+II.a+II.b+III+IV)	100
Numărul de credite	4

4. **Competenţe specifice acumulate**

Competenţe profesionale	CP 9. Stabileste procese de date CP 20. Asigura mentenanta echipamentelor CP 26. Opereaza echipamente de masura de precizie
Competenţe transversale	CT1. Efectueaza calcule CT3. Administreaza identitatea digitala

5. **Rezultatele învățării**

Cunoștințe	Aptitudini	Responsabilitate și autonomie
Studentul/absolventul descrie, identifică, sumarizează concepte și metode elementare de achiziție, analiză și prelucrare a semnalelor, implementate in sisteme cu microprocesoare de uz general sau procesoare de semnal și modul lor de aplicare în probleme concrete	Studentul/absolventul utilizează metode și instrumente specifice pentru caracterizarea semnalelor în domeniul timp și în domeniul frecvență, realizează achiziția, analiza și prelucrarea digitală a semnalelor analogice. Studentul/absolventul proiectează, măsoară, evaluează performanțele, diagnostichează și depanează blocuri funcționale de complexitate mică/medie de analiză și prelucrare digitală a semnalelor, folosind	Studentul/absolventul arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.

Cunoștințe	Aptitudini	Responsabilitate și autonomie
	medii de simulare dedicate (Matlab, Python, etc.). Studentul/absolventul proiectează blocuri funcționale de complexitate mică/medie de analiză și prelucrare digitală a semnalelor și le implementează pe procesoare de semnal, microcontrolere sau procesoare dedicate	

6. **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.

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	2		
4. Maşini de criptare: maşina Enigma 4.1. Istoric 4.2. Prezentare generală 4.3. Detalii tehnice 4.4. Exemple de criptare / decriptare 4.5. Stabilirea cheilor şi a modului de funcţionare 4.6. Complexitatea maşinii Enigma 4.7. Slăbiciunile maşinii Enigma. Concluzii	2		
5. Importanţa 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. Motivaţia unui nou standard 7.2. Cerinţe iniţiale 7.3. Candidaţii (MARS, RC6, Rijndael, Serpent, Twofish) 7.4. Evaluare finală a candidaţilor. Consideraţii 7.5. Preliminarii matematice – câmpuri Galois 7.6. Descrierea algoritmului AES (Rijndael) 7.7. Implementarea algoritmului AES	2		
8. Algoritmul de criptare RSA	2		

8.1. Elemente de Matematică 8.2. Prezentarea algoritmului 8.3. Exemple de criptare / decriptare			
9. Algoritmi de criptare ce folosesc funcţii de dispersie 9.1. Securitatea algoritmilor de criptare ce se bazează pe funcţii de dispersie 9.2. Algoritmul MD5. Istoric. Descriere in detaliu. Exemple. 9.3. Algoritmul SHA-1. Descriere in detaliu. Exemple	2		
10. Semnături digitale	2		
11. Atacuri criptografice	2		
12. Securizarea codului/aplicațiilor	2		
13. Securitatea bazelor de date	2		

Bibliografie minimală recomandată

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. 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 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		

Bibliografie minimală recomandată

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. 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%
Laborator	-însușirea algoritmilor specifici domeniului -capacitatea de implementare a algoritmilor specifici domeniului - abilitatea de rezolvare a unor probleme specifice domeniului	probă practică	50%

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
22.09.2025	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ

Data avizării	Grad didactic, nume, prenume, semnătura responsabilului de program
23.09.2025	Conf. dr. ing. Eugen COCA

Data avizării în departament	Grad didactic, nume, prenume, semnătura directorului de departament
25.09.2025	Conf. dr. ing. Eugen COCA

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