

FIȘA DISCIPLINEI

Anul universitar 2025 - 2026

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Lucian Blaga din Sibiu
1.2. Facultatea	Științe
1.3. Departament	Matematică și Informatică
1.4. Domeniul de studiu	Informatică
1.5. Ciclul de studii ¹	Licenta
1.6. Specializarea	Informatică

2. Date despre disciplină

2.1. Denumirea disciplinei	Criptografie	Cod	FSTI.MAI.INF.L.SO.3.2020.E-5.4
2.2. Titular activități de curs	Conf. univ. dr. Nicolae CONSTANTINESCU		
2.3. Titular activități practice	Lector Univ. Dr. Oana-Adriana Ticleanu		
2.4. An de studiu ²	3	2.5. Semestrul ³	1
2.6. Tipul de evaluare ⁴	E		
2.7. Regimul disciplinei ⁵	O	2.8. Categoria formativă a disciplinei ⁶	S

3. Timpul total estimat

3.1. Extinderea disciplinei în planul de învățământ – număr de ore pe săptămână					
3.1.a.Curs	3.1.b. Seminar	3.1.c. Laborator	3.1.d. Proiect	3.1.e Alte	Total
2	-	2	-	-	4
3.2. Extinderea disciplinei în planul de învățământ – total ore din planul de învățământ					
3.2.a.Curs	3.2.b. Seminar	3.2.c. Laborator	3.2.d. Proiect	3.2.e Alte	Total ⁷
28	-	28	-	-	56
Distribuția fondului de timp pentru studiu individual⁸					Nr. ore
Studiul după manual, suport de curs, bibliografie și notițe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					19
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					20
Tutoriat ⁹					6
Examinări ¹⁰					4
3.3. Total ore alocate studiului individual¹¹ (NOSI_{sem})					69
3.4. Total ore din Planul de învățământ (NOAD_{sem})					56
3.5. Total ore pe semestru¹² (NOAD_{sem} + NOSI_{sem})					125
3.6. Nr ore / ECTS					125
3.7. Număr de credite¹³					5

4. Precondiții (acolo unde este cazul)

4.1. Discipline necesar a fi promovate anterior (de curriculum) ¹⁴	Fundamentele Programării, Algoritmi și Structuri de Date
4.2. Competențe	Cunoasterea modelelor criptografice și modului de aplicare al lor

5. Condiții (acolo unde este cazul)

5.1. De desfășurare a cursului ¹⁵	Sală de curs, dotată cu tablă, calculator, videoproiector și software/Predare Oline
5.2. De desfășurare a activităților practice (lab/sem/pr/alte) ¹⁶	Sală de laborator dotată cu calculatoare desktop/Predare Online

6. Rezultate ale învățării¹⁷

Numărul de credite alocate disciplinei: 5				
Rezultatele învățării				Repartizare credite pe rezultatele învățării
Nr. crt.	Cunoștințe	Aptitudini	Responsabilitate și autonomie	
RÎ 1	Studentul explică noțiunile fundamentale de criptografie, tipurile de sisteme de criptare și proprietățile lor.	Studentul aplică tehnici de criptare și decriptare simetrică și asimetrică pe exemple practice.	Studentul demonstrează responsabilitate în utilizarea algoritmilor și respectă regulile de integritate și confidențialitate.	2
RÎ 2	Studentul descrie principalele algoritmi de criptare și protocoale (DES, AES, RSA, ECC, El Gamal, Diffie-Hellman, Kerberos).	Studentul implementează și testează algoritmi criptografici și compară eficiența și securitatea acestora.	Studentul manifestă autonomie în alegerea algoritmilor și adoptă bune practici în documentarea soluțiilor.	2
RÎ 3	Studentul înțelege aplicarea criptografiei în sisteme electronice (semnături digitale, plăți electronice, vot electronic).	Studentul utilizează protocoale de semnătură, distribuie a cheilor și scheme de securizare a tranzacțiilor.	Studentul își asumă responsabilitatea protejării datelor și adoptă o conduită etică în dezvoltarea aplicațiilor.	1

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

7.1. Obiectivul general	Însușirea algoritmilor criptografici și a modului în care aceștia pot fi folosiți în diverse situații reale
7.2. Obiectivele specifice	Însușirea tehnicilor de criptare, codare, identificare respectiv corecție a erorilor și vulnerabilităților Protecția împotriva atacurilor informatice

8. Conținuturi

8.1. Curs ¹⁸	Metode de predare ¹⁹	Nr. ore
Scurt istoric al criptografiei. Noțiuni de bază. Sisteme simetrice de criptare.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Cifruri de substituție. Sisteme de criptare monoalfabetice	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2



Cifruri de substituție. Sisteme de criptare polialfabetice	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Sisteme de criptare fluide. Sisteme sincronizabile și auto – sincronizabile. Sistemul aditiv fluid de criptare RC4. Securitatea sistemului RC4.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Sistemul de criptare DES. Considerații generale. Descrierea sistemului DES. Controverse legate de DES. Moduri de utilizare ale DES-ului. Sisteme de criptare înrudite cu DES.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Sistemul de criptare AES. Istoric și scurtă prezentare a sistemelor intrate în finală: Mars, RC6, Serpent, Twofish. Detalii ale sistemului de criptare AES.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Criptare cu cheie publică. Considerații generale. Funcții neinvertibile. Trapa secretă. Securitatea sistemelor de criptare cu cheie publică. Comparatie între criptarea simetrică și cea cu cheie publică.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Sistemul de criptare RSA. Implementarea sistemului. Criptarea asimetrică de tip ECC	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Sistemul de criptare El Gamal. Calculul logaritmului discret.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Semnături electronice. Protocoale de semnătură. Semnătura El Gamal. Standarde de semnătură electronică	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Protocoale de distribuire a cheilor. Predistribuirea cheilor. Kerberos. Schimbul de chei Diffie - Hellman	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Sisteme electronice de plată. Proprietăți de bază. Securitatea plăților electronice. Protocoale de semnătură. Scheme de identificare. Problema reprezentării în grupuri.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Sistemul electronic de plată. Modele de implementare	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Protocoale de vot electronic. Caracteristicile unui sistem de vot electronic. Protocoale independente de vot. Protocol cu autoritate centrală.	Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții	2
Total ore curs:		28

8.2. Activități practice (8.2.a. Seminar ²⁰ / 8.2.b. Laborator ²¹ / 8.2.c. Proiect ²² / 8.2.d. Alte act.practice ²³)	Metode de predare	Nr. ore
Implementarea algoritmului lui Cezar	<i>Demonstrație practică, exercițiu</i>	2
Implementarea substituirii monoalfabetice	<i>Demonstrație practică, exercițiu, implementare</i>	2
Implementarea cifrurilor de permutare	<i>Demonstrație practică, exercițiu, implementare</i>	2
Implementarea sistemului de criptare afin	<i>Demonstrație practică, exercițiu, implementare</i>	2
Implementarea sistemului de criptare Polybios	<i>Demonstrație practică, exercițiu, implementare</i>	2
Implementarea sistemului de criptare Playfair	<i>Demonstrație practică, exercițiu, implementare</i>	2
Implementarea sistemului de criptare Vigenere	<i>Demonstrație practică, exercițiu, implementare</i>	2
Implementarea sistemului de criptare Rijndael (AES)	<i>Demonstrație practică, exercițiu, implementare</i>	2
Implementarea sistemului de criptare DES	<i>Demonstrație practică, exercițiu</i>	2
Implementarea sistemelor de criptare cu cheie publică – sistemul RSA	<i>Demonstrație practică, exercițiu</i>	2
Implementarea sistemelor de criptare cu cheie publică – sistemul El Gamal	<i>Demonstrație practică, exercițiu</i>	2
Modele de implementare. Steganografia	<i>Demonstrație practică, exercițiu</i>	2
Modele de implementare. Ascunderea de date	<i>Demonstrație practică, exercițiu</i>	2
Modele de implementare. Tranzacții financiare electronice	<i>Demonstrație practică, exercițiu</i>	2
Total ore seminar/laborator		28

9. Bibliografie

9.1. Referințe bibliografice recomandate	Jan Pelzl, Christof Paar, Understanding Cryptography: A Textbook for Students and Practitioners, Springer 2020
	Douglas Stinson, Maura Paterson, Cryptography: Theory and Practice, CRC Press 2019
	Duncan Buell, Fundamentals of Cryptography, Springer 2021
9.2. Referințe bibliografice suplimentare	Nicolae Constantinescu, Criptografie, Editura Academiei Romane, 2009
	Arto Saloma, "Public Key Cryptography" Second Edition, Springer 1996
	Hans Delfs, Helmut Knebl, "Introduction to Cryptography - Principles and Applications", Springer 2002
	Colin Boyd, Anish Mathuria, "Protocols for Authentication and Key Establishment", Springer 2003

10. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului²⁴

Se realizează prin contacte periodice cu aceștia în vederea analizei problemei. Conținutul disciplinei a fost stabilit ținând cont de interacțiunile constructive ale cadrelor didactice, studenților și a reprezentanților din mediul economic, științific, în cadrul manifestărilor științifice, întâlnirilor de lucru și activităților de practică și dezvoltare de proiecte a studenților.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare		11.3 Pondere din nota finală	Obs. ²⁵
11.4a Examen / Colocviu		Teste pe parcurs ²⁶ :	25%	50% (minim 5)	CPE
		Teme de casă:	20%		

	• Cunoștințe teoretice și practice însușite (cantitatea, corectitudinea, acuratețea)	Alte activități ²⁷ : Evaluare finală:	5% 50% (min. 5)		
11.4b Seminar	• Frecvența/relevanța intervențiilor sau răspunsurilor	Evidența intervențiilor, portofoliu de lucrări (referate, sinteze științifice)	% (minim 5)	N/A	
11.4c Laborator	• Cunoașterea aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea și interpretarea unor rezultate	• Chestionar scris • Răspuns oral • Caiet de laborator, lucrări experimentale, referate, examinare de laborator, etc. • Demonstrație practică	25% (minim 5)	nCPE	
11.4d Proiect	• Calitatea proiectului realizat, corectitudinea documentației proiectului, justificarea soluțiilor alese	• Autoevaluarea, prezentarea și/sau susținerea proiectului • Evaluarea critică a unui proiect	25% (minim 5)	CPE	
11.5 Standard minim de performanță ²⁸ : CP5. Cunoașterea algoritmilor clasici de criptare, notarea la 10 proiecte de laborator.					CEF

Fișa disciplinei cuprinde componente adaptate persoanelor cu CES (persoane cu dizabilități și persoane cu potențial înalt), în funcție de tipul și gradul acestora, la nivelul tuturor elementelor curriculare (competențe, obiective, conținuturi, metode de predare, evaluare alternativă), pentru a asigura șanse echitabile în pregătirea academică a tuturor studenților, acordând atenție sporită nevoilor individuale de învățare.

Data completării: | 1 | 5 | / | 0 | 9 | / | 2 | 0 | 2 | 5 |

Data avizării în Departament: | 3 | 0 | / | 0 | 9 | / | 2 | 0 | 2 | 5 |

	Grad didactic, titlul, prenume, numele	Semnătura
Titular disciplină	Conf. Univ. Dr. Nicolae CONSTANTINESCU	
Responsabil program de studii	Lector Univ. Dr. Daniel Ioan HUNYADI	
Director Departament	Prof. Univ. Dr. Mugur ACU	

¹ Licență / Master

² 1-4 pentru licență, 1-2 pentru master

³ 1-8 pentru licență, 1-3 pentru master

⁴ Examen, colocviu sau VP A/R – din planul de învățământ

⁵ Regim disciplină: O=Disciplină obligatorie; A=Disciplină opțională; U=Facultativă

⁶ Categoria formativă: S=Specialitate; F=Fundamentală; C=Complementară; I=Asistată integral; P=Asistată parțial; N=Neasistată

⁷ Este egal cu 14 săptămâni x numărul de ore de la punctul 3.1 (similar pentru 3.2.a.b.c.d.e.)

⁸ Liniile de mai jos se referă la studiul individual; totalul se completează la punctul 3.37.

⁹ Între 7 și 14 ore

¹⁰ Între 2 și 6 ore

¹¹ Suma valorilor de pe liniile anterioare, care se referă la studiul individual.

¹² Suma (3.5.) dintre numărul de ore de activitate didactică directă (NOAD) și numărul de ore de studiu individual (NOSI) trebuie să fie egală cu numărul de credite alocate disciplinei (punctul 3.7) x nr. ore pe credit (3.6.)

¹³ Numărul de credit se calculează după formula următoare și se rotunjește la valori vecine întregi (fie prin micșorare fie prin majorare)

$$\text{Nr. credite} = \frac{\text{NOCpSpD} \times C_C + \text{NOApSpD} \times C_A}{\text{TOCpSpD} \times C_C + \text{TOApSpD} \times C_A} \times 30 \text{ credite}$$

Unde:

- NOCpSpD = Număr ore curs/săptămână/disciplina pentru care se calculează creditele
- NOApSpD = Număr ore aplicații (sem./lab./pro.)/săptămână/disciplina pentru care se calculează creditele
- TOCpSpD = Număr total ore curs/săptămână din plan
- TOApSpD = Număr total ore aplicații (sem./lab./pro.)/săptămână din plan
- C_C/C_A = Coeficienți curs/aplicații calculate conform tabelului

Coeficienți	Curs	Aplicații (S/L/P)
Licență	2	1
Master	2,5	1,5
Licență lb. străină	2,5	1,25

¹⁴ Se menționează disciplinele obligatorii a fi promovate anterior sau echivalente

¹⁵ Tablă, videoproiector, flipchart, materiale didactice specifice, platforme on-line etc.

¹⁶ Tehnică de calcul, pachete software, standuri experimentale, platforme on-line etc.

¹⁷ Competențele din Grilele aferente descrierii programului de studii, adaptate la specificul disciplinei

¹⁸ Titluri de capitole și paragrafe

¹⁹ Expunere, prelegere, prezentare la tablă a problematicei studiate, utilizare videoproiector, discuții cu studenții (pentru fiecare capitol, dacă este cazul)

²⁰ Discuții, dezbateri, prezentare și/sau analiză de lucrări, rezolvare de exerciții și probleme etc.

²¹ Demonstrație practică, exercițiu, experiment etc.

²² Studiu de caz, demonstrație, exercițiu, analiza erorilor etc.

²³ Alte tipuri de activități practice specifice

²⁴ Legătura cu alte discipline, utilitatea disciplinei pe piața muncii

²⁵ CPE – condiționează participarea la examen; nCPE – nu condiționează participarea la examen; CEF - condiționează evaluarea finală; N/A – nu se aplică

²⁶ Se va preciza numărul de teste și săptămânile în care vor fi susținute.

²⁷ Cercuri științifice, concursuri profesionale etc.

²⁸ Se particularizează la specificul disciplinei standardul minim de performanță din grila de competențe a programului de studii, dacă este cazul.