

FIȘA DISCIPLINEI

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea „Tibiscus” din Timișoara
1.2. Facultatea	Calculatoare și Informatică Aplicată
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Licență
1.6. Programul de studii/Calificarea	Informatică

2. Date despre disciplină

2.1. Denumirea/codul disciplinei	ALGORITMI DE SECURITATE INFORMATICĂ (ASI) - LIN221						
2.2. Titularul activității de curs	Conf.univ.dr. Victoria IORDAN						
2.3. Titularul activității de laborator	Lect.univ.dr. Kristijan CINCAR						
2.4. Anul de studiu	2	2.5. Semestrul	2	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	Conținut ¹ =DF Obligativitate ² =DO

3. Timpul total estimat

3.1. Numărul de ore pe săptămână	4	din care 3.2. curs	2	3.3. laborator+proiect	1+1
3.4. Total ore din planul de învățământ	56	din care 3.5. curs	28	3.6. laborator+proiect	14+14
Distribuția fondului de timp					Ore
Studiul după manual, suport de curs, bibliografie și notițe					24
Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate					20
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					25
Tutoriat					4
Examinări					4
Alte activități					-
3.7. Total ore studiu individual					69
3.8. Total ore pe semestru					125
3.9. Numărul de credite					5

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Programare 1, Programare orientată pe obiect, Structuri de date și algoritmi, Noțiuni fundamentale de arhitectura calculatoarelor
4.2. de competențe	Bune cunoștințe de programare într-un limbaj de nivel înalt Abilitatea de a lucra cu structuri de date (liste, arbori, grafuri, tabele hash) Capacitatea de analiză și rezolvare a problemelor tehnice

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Sală de curs dotată corespunzător: tablă albă, SmartBoard, videoproiector, calculator. Suport electronic al cursului disponibil pe platforma Google Classroom
5.2. de desfășurare a seminarului/laboratorului	Sală de laborator, dotată corespunzător: tablă, laptop/proiector, calculatoare, rețea, legătură internet, software adecvat. Platformă de predare a temelor (Google Classroom)

6. Obiectivele disciplinei - rezultate așteptate ale învățării la formarea cărora contribuie parcurgerea și promovarea disciplinei

Cunoștințe	La finalizarea disciplinei, studentul va cunoaște și va înțelege: Noțiunile fundamentale privind tehnici și proceduri de securitate informatică.
------------	--

	• Rolul algoritmilor de criptare/decriptare în securitatea rețelelor și transmiterea datelor. • Proceduri de autentificare și control al accesului. • Măsurile de protecție împotriva atacurilor cibernetice și gestionarea riscurilor în infrastructura IT.
Abilități	La finalizarea disciplinei, studentul va fi capabil să: • Implementeze algoritmi de criptare simetrici și asimetrici utilizând un limbaj de programare adecvat. • Utilizeze biblioteci specializate pentru implementarea unor algoritmi standard. • Analizeze și interpreteze rezultatele obținute în urma aplicării algoritmilor. • Compare diferite metode de procesare și să justifice alegerea unei soluții. • Dezvolte aplicații simple care includ funcționalități de securitate a informațiilor.
Responsabilitate și autonomie	La finalizarea disciplinei, studentul va demonstra: • Capacitatea de a lucra autonom în rezolvarea problemelor de securitate a informațiilor. • Capacitatea de a respecta cerințele tehnice și termenele de predare. • Spirit critic în evaluarea performanței algoritmilor implementați. • Capacitatea de a colabora eficient în echipă pentru dezvoltarea unui proiect aplicativ.

7. Conținuturi

7.1. Curs	Metode de predare	Observații
C1 Probleme ale protecției și securității datelor -Noțiuni generale -Vulnerabilitatea informației și calculatoarelor -Modele de securitate a informației	Expunerea interactivă, problematizarea, conversația euristică, documentarea pe web, exemplificarea	Materialele prezentate la curs vor fi postate pe Google Classroom
C2 Evoluția sistemelor criptografice -Structura unui sistem criptografic -Evoluția istorică a criptografiei -Clasificarea metodelor de criptare. Criptografie clasică și tendințe actuale în criptografie și analiza criptografică		
C3-C5 Criptarea convențională clasică. Modelul criptării convenționale Metode criptografice clasice -Metoda substituției -Metoda transpoziției Algoritmi de criptare clasici (Codul lui Caesar, Tabele Viginere, Tabela Porta, Codificări matrice, Codificări Bifid, Codul Playfair, Codul Hill)		
C6-C8 Metode criptografice clasice -Metode computaționale: sisteme simetrice, sisteme cu chei publice Algoritmi moderni de criptare Principiile codurilor bloc. Structura codului Feistel Algoritmii: DES, Triplu DES, IDEA, RC5, AES	Expunerea interactivă, problematizarea, conversația euristică, documentarea pe web, exemplificarea	Materialele prezentate la curs vor fi postate pe Google Classroom
C9 Criptarea cu chei publice. Algoritmul RSA. Algoritmul Diffie-Hellman		Materialele prezentate la curs vor fi postate pe Google Classroom
C10 Funcții hash, semnături digitale.		
C11 Tehnici de atac și apărare în era internetului.		
C12-C14 Arhitecturi de securitate la calculatoare și sisteme distribuite -Protecția informațiilor -Protocoale de identificare și autentificare -Protocoale pentru transferul de date -Integrarea securității în arhitectura rețelelor de calculatoare		Materialele prezentate la curs vor fi postate pe Google Classroom
Bibliografie [1] I. Angheloiu, E. Gyorfi, V. V. Patriciu, Securitatea și protecția informației în sistemele electronice de calcul, Editura Militară, București, 1986 [2] T. Băjenescu, M. Borda, Securitatea în informatică și telecomunicații, Editura Dacia, Cluj Napoca, 2001 [3] Nicolae Constantinescu. Criptografie. Ed. Acdemiei Române, 2009 [4] V. V. Patriciu, Criptografia și securitatea rețelelor de calculatoare cu aplicații în C și Pascal, Editura Tehnică, București, 1994		

[5] V. V. Patriciu, M. Pietroșanu-Ene, I. Bica, C. Cristea, Securitatea informatică în Unix și Internet, Editura Tehnică, București, 1998 [6] Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography (2nd edition), (http://www.cs.umd.edu/~jkatz/imc.html). [7] Harold F. Tipton, Micki Krause – Information Security Management Handbook, Auerbach Publications, CRC Press LLC, 2000		
7.2. Laborator/proiect	Metode de predare/învățare	Observații
1. Implementarea algoritmilor de criptare/decriptare de tip Caesar	Exercițiul, discuțiile și dezbaterile, modelarea, proiectul, lucrul în grup organizat	Laboratoarele și temele vor fi postate pe Google Classroom
2. Implementarea algoritmilor de criptare/decriptare Polybius		
3. Implementarea algoritmilor de criptare/decriptare de tip Playfair		
4. Implementarea algoritmilor de criptare/decriptare bazati pe Tabela Porta (sau Bifid) si Codul Hill		
5. Coduri de tip Vigenere		
6. Implementarea algoritmului DES - Data Encryption Standard		
7. Implementarea algoritmului AES - Advanced Encryption Standard	Exercițiul, discuțiile și dezbaterile, modelarea, proiectul, lucrul în grup organizat	Laboratoarele și temele vor fi postate pe Google Classroom
8. Implementarea algoritmului Secure Hash Algorithm 1 (SHA-1)		
9. Cifruri cu chei publice (1)		
10. Cifruri cu chei publice (2)		
11. Mecanism de semnătură electronică		
12. Realizare proiect.		
13. Prezentare proiect.		
14. Prezentare proiect.		
Bibliografie		
[1] M. Joldoș, Securitatea sistemelor și a aplicațiilor, Universitatea Tehnică din Cluj-Napoca, 2015, disponibil pe: http://users.utcluj.ro/~jim/SSA/Resources/Laboratory/ [2] V. V. Patriciu, Criptografia și securitatea rețelelor de calculatoare cu aplicații în C și Pascal, Editura Tehnică, București, 1994 [3] V. V. Patriciu, M. Pietroșanu-Ene, I. Bica, C. Cristea, Securitatea informatică în Unix și Internet, Editura Tehnică, București, 1998 [4] Jonathan Knudsen - Java Cryptography, Editura O'Reilly, 1998 [5] Victoria Iordan – Algoritmi de securitate informatică - Suport de curs – Editura Mirton 2025		

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

Conținuturile disciplinei sunt corelate cu standardele academice și profesionale actuale din domeniul securității informatice, fiind aliniate la recomandările comunității științifice internaționale, ale organismelor profesionale și ale angajatorilor din sectorul IT. Prin activitățile practice (implementarea algoritmilor criptografici, analiza atacurilor, studii de caz privind vulnerabilități), studenții dezvoltă capacitatea de a integra mecanisme de securitate în aplicații software, abilități de exploatare a rețelilor de calculatoare pentru potențiali utilizatori. Piața muncii locală, națională sau europeană este în permanentă căutare de absolvenți cu bune cunoștințe în proiectarea unor rețele sigure. Conținuturile disciplinei sunt actualizate periodic pe baza evoluției amenințărilor cibernetice și a tehnologiilor emergente (cloud, IoT, AI).
--

9. Evaluare

Tip de activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
9.1. Curs	Cunoașterea, înțelegerea și utilizarea corectă a noțiunilor teoretice în rezolvarea aplicațiilor practice; capacitatea de analiză și argumentare.	Examen scris (test grilă + aplicații)	40%
9.2. Laborator/proiect	Capacitatea de implementare într-un limbaj de programare (C, Python) a algoritmilor de criptare/ decriptare prezentați la curs.	Teme de laborator	20%
	Realizarea unui proiect individual (implementare de algoritmi de criptare/decriptare într-o aplicație complexă)	Prezentare orală	40%

9.3. Standard minim de performanță
• Cunoașterea elementelor fundamentale de teorie despre securitate informatică • Cunoașterea și implementarea corectă a minim 4 algoritmi de criptare și decriptare a informației (3 algoritmi cu cheie simetrică și 1 algoritm cu cheie publică). • Realizarea unui referat din tematica cursului prezentat la curs. Pentru promovare este necesară obținerea notei minime 5 atât la evaluarea teoretică, cât și la componenta practică.

Notă:

1) Regimul disciplinei (conținut) - pentru nivelul de licență se alege una din variantele: DF (disciplină fundamentală) / DS (disciplină de specialitate) / DC (disciplină complementară).

2) Regimul disciplinei (obligativitate) - se alege una din variantele: DO=discipline obligatorii (impuse) / DOP=discipline opționale/ DFc (disciplină facultativă).

Data completării

Titular de curs

Titular de laborator

17.02.2026

Conf.univ.dr. Victoria IORDAN

Lect.univ.dr. Kristijan CINCAR

Data avizării în departament

Director de departament

20.02.2026

Conf. univ. dr. Victoria IORDAN