# FIŞA DISCIPLINEI

**1. Date despre program**

| | |
|---|---|
| 1.1 Instituţia de învăţământ superior | **UNIVERSITATEA DIN ORADEA** |
| 1.2 Facultatea | **Facultatea de Inginerie Electrică şi Tehnologia Informaţiei** |
| 1.3 Departamentul | **Departamentul de Electronică şi Telecomunicaţii** |
| 1.4 Domeniul de studii | **Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale** |
| 1.5 Ciclul de studii | **Licenţă (ciclul I)** |
| 1.6 Programul de studii/Calificarea | **Rețele și Software de Telecomunicații / Inginer** |

**2. Date despre disciplină**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2.1 Denumirea disciplinei | | | | **Algoritmi de Criptare in Rețele de Telecomunicații** | | | |
| 2.2 Titularul activităţilor de curs | | | | **Ș.l. dr. ing. ȚEPELEA LAVINIU** | | | |
| 2.3 Titularul activităţilor de laborator | | | | **Ș.l. dr. ing. ȚEPELEA LAVINIU** | | | |
| 2.4 Anul de studiu | IV | 2.5 Semestrul | VIII | 2.6 Tipul de evaluare | VP | 2.7 Regimul disciplinei | O |

(I) Impusă; (O) Opţională; (F) Facultativă

**3. Timpul total estimat** (ore pe semestru al activităţilor didactice)

| | | | | | |
|---|---|---|---|---|---|
| 3.1 Număr de ore pe săptămână | 3 | din care: 3.2 curs | 2 | 3.3 Seminar/laborator/proiect | -/1/- |
| 3.4 Total ore din planul de învăţământ | 42 | din care: 3.5 curs | 28 | 3.6 laborator | 14 |
| Distribuţia fondului de timp | | | | | 33 |
| Studiul după manual, suport de curs, bibliografie şi notiţe | | | | | 9 |
| Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren | | | | | 9 |
| Pregătire laboratoare, teme, referate, portofolii şi eseuri | | | | | 7 |
| Tutoriat | | | | | - |
| Examinări | | | | | 8 |
| Alte activităţi..... | | | | | - |
| **3.7 Total ore studiu individual** | **33** | | | | |
| **3.9 Total ore pe semestru** | **75** | | | | |
| **3.10 Numărul de credite** | **3** | | | | |

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

| | |
|---|---|
| 4.1 de curriculum | |
| 4.2 de competenţe | |

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

| | |
|---|---|
| 5.1. de desfăşurare a cursului | Sală de curs dotată cu calculator, software adecvat și video proiector, dar și online pe platforma e.uoradea.ro si programul Microsoft Teams, în funcție de situația pandemiei Covid |
| 5.2. de desfăşurare a laboratorului | Sală de laborator dotată cu calculatoare și software dedicat, dar și online pe platforma e.uoradea.ro si programul Microsoft Teams, în funcție de situația pandemiei Covid |

| 6a. Competenţele specifice acumulate | |
|---|---|
| Competenţe profesionale | **C4. Selectarea, instalarea şi exploatarea echipamentelor de comunicaţii, fixe şi mobile, precum şi planificarea, configurarea şi integrarea serviciilor de telecomunicaţii şi elemente de securitatea informaţiei**<br>**C5. Analiza şi adaptarea arhitecturilor, tehnologiilor şi protocoalelor de comunicaţii pentru aplicaţii suport de reţele locale, metropolitane, de arie mare şi integrate:**<br>**C6. Utilizarea unor limbaje şi instrumente specializate pentru inginerie software, cu orientare către sistemele de telecomunicaţii integrate:** |
| Competenţe transversale | |

| 6b. Rezultatele aşteptate ale învăţării | |
|---|---|
| Cunoştiinţe | Studentul/absolventul trebuie să descrie, să analizeze și să aplice principiile fundamentale, metodele și algoritmii de **criptare** (simetrică și asimetrică), de **autentificare** și de asigurare a **integrității datelor** în scopul securizării comunicațiilor în diverse arhitecturi de rețea. |
| Aptitudini | Studentul/absolventul **selectează, configurează și implementează** algoritmi criptografici (e.g., AES, RSA, funcții hash, semnături digitale) pentru a asigura **confidențialitatea, integritatea și autentificarea** datelor transmise în rețele.<br><br>Studentul/absolventul **operează și configurează** instrumente și protocoale criptografice standard (e.g., SSL/TLS, IPsec, SSH, PGP) și utilizează medii de programare (e.g., Python, C++) pentru **simularea și testarea** mecanismelor de securitate.<br><br>Studentul/absolventul **evaluează performanța și rezistența** schemelor criptografice implementate la atacuri comune și **proiectează soluții** de securitate adaptate cerințelor specifice ale arhitecturilor de rețea. |
| Responsabilitate și autonomie | Studentul/absolventul manifestă **responsabilitate** în gestionarea și protecția datelor sensibile, acționând **autonom** pentru a se menține la curent cu cele mai noi **vulnerabilități** și **standarde criptografice** din domeniul securității cibernetice. |

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

| | |
|---|---|
| 7.1 Obiectivul general al disciplinei | Familiarizarea studentilor cu cele mai uzuale metode de criptare utilizate in domeniul calculatoarelor si al telecomunicatiilor. |
| 7.2 Obiectivele specifice | Se abordeaza atat metode de criptare clasice cat si metode de criptare moderne. |

**8. Conţinut**

| 8.1 Curs | Metode de predare | Nr. Ore / Observaţii |
|---|---|---|
| 1. Istoria Criptografiei. Terminologie criptografică. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 2. Cifrul Caesar. Cifruri de substituţie polialfabetică. Cifrul Vigenere. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 3. Algoritmul OTP (One Time Pad). Algoritmul SEAL. | Prelegerea. Explicaţia. Descrierea. | 2 |

| | | |
|---|---|---|
| | Exemplificarea. | |
| 4. Tipuri de algoritmi în criptografia modernă. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 5. Cifrul Data Encryption Standard (DES). | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 6. Cifrul Advanved Encryption Standard (AES). | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 7. Algoritmul Blowfish. Algoritmi simetrici de tip șir. Cifrul RC4. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 8. Algoritmi cu chei publice. Algoritmul Diffie-Hellman. Cifrul RSA. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 9. Semnătura digitală. Aplicarea ei la diferite tipuri de documente. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 10. Steganografia. Aplicarea steganografiei asupra diferitelor tipuri de fişiere. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 11. Utilizarea criptografiei în domeniul e-commerce. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 12. Tehnici RFID. Criptografia în cazul card-urilor. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 13. Criptarea in domeniul Wireless. Criptare WEP, WPA, WPA2. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |
| 14. Securitatea în Reţelele informatice. Atacuri informatice. | Prelegerea. Explicaţia. Descrierea. Exemplificarea. | 2 |

Bibliografie:

1. ***, *Encyclopedia of Cryptography and Security*, Editor-in-chief Henk C.A. van Tilborg, Eindhoven University of Technology The Netherlands, Springer, ISBN-13: (e-book) 978-0387-23483-0, 2005

2. ***, *An Introduction to Cryptography - Second Edition*, Series Editor KENNETH H. ROSEN, Taylor & Francis Group, LLC, ISBN -10: 1-58488-618-8, Boca Raton, 2007

3. Joan Daemen, Vincent Rijmen, *AES - The Advanced Encryption Standard,* Springer, ISBN 3-540-42580-2, Berlin, 1998

4. Bogdan Groza, *Introducere în Sistemele Criptografice cu Cheie Publică,* Universitatea Politehnica Timişoara, Noiembrie, 2007

5. A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1997

6. Douglas Stinson, *Cryptography: Theory and Practice*, CRC Press, **ISBN:** 0849385210, 1995

7. http://en.wikipedia.org

8. Wenbo Mao, *Modern Cryptography: Theory and Practice*, Hewlett-Packard Company, Prentice Hall PTR, ISBN: 0-13-066943-1, July, 2003

| 8.2 Seminar | Metode de predare | Nr. Ore / Observaţii |
|---|---|---|

| | | |
|---|---|---|
| 8.3 Laborator | | |
| 1. Introducere în Algoritmi de criptare. Cifrul Caesar. Realizarea de criptări, decriptări software. | Descrierea. Explicaţia. Exemplificarea. Verificarea. | 2 |
| 2. Cifrul Vigenere. Codul Morse. Realizarea de criptări, decriptări software. | Descrierea. Explicaţia. Exemplificarea. Verificarea. | 2 |
| 3. Maşina de criptare Enigma. Cifrul DES. Realizarea de criptări, decriptări software. | Descrierea. Explicaţia. Exemplificarea. Verificarea. | 2 |
| 4. Cifrul AES. Algoritmul Blowfish. Realizarea de criptări, decriptări software. | Descrierea. Explicaţia. Exemplificarea. Verificarea. | 2 |
| 5. Cifrul RSA. Semnături digitale. Realizarea de criptări, decriptări software. Aplicarea semnăturilor digitale la trimiterea e-mail-urilor si asupra documentelor PDF. | Descrierea. Explicaţia. Exemplificarea. Verificarea. | 2 |
| 6. Aplicaţii steganografice pentru diferite tipuri de fişiere. | Descrierea. Explicaţia. Exemplificarea. Verificarea. | 2 |
| 7. Aplicaţii software de criptare comerciale şi gratuite utilizate frecvent. | Descrierea. Explicaţia. Exemplificarea. Verificarea. | 2 |
| | | |
| 8.4 Proiect | - | - |

Bibliografie:

1. Bogdan Groza, *Introducere în Sistemele Criptografice cu Cheie Publică,* Universitatea Politehnica Timişoara, Noiembrie, 2007
2. A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1997
3. Douglas Stinson, *Cryptography: Theory and Practice,* CRC Press, **ISBN:** 0849385210, 1995
4. http://en.wikipedia.org
5. Wenbo Mao, *Modern Cryptography: Theory and Practice,* Hewlett-Packard Company, Prentice Hall PTR, ISBN: 0-13-066943-1, July, 2003

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

| |
|---|
| |

**10. Evaluare**

| Tip activitate | 10.1 Criterii de evaluare | 10.2 Metode de evaluare | 10.3 Pondere din nota finală |
|---|---|---|---|
| 10.4 Curs | Cunoasterea algoritmilor de criptare principali utilizati in telecomunicatii si utilitatea lor. | Verificare pe parcurs prin doua teste scrise sau două teste grilă în cazul evaluării online | 70% |
| 10.5 Seminar | - | - | - |
| 10.6 Laborator | Acumularea cunostintelor din partea teoretica si utilizarea practica a aplicatiilor. | Un procent de 10% din nota finala de la laborator, se acorda pentru finalizarea cu succes a tematicii de studiu individual.<br>Verificarea acumularii cunostintelor si a abilitatii de utilizare a aplicatiilor practice. | 30% |
| 10.7 Proiect | - | - | - |

10.8 Standard minim de performanţă:

Cunoasterea algoritmilor de criptare moderni DES si AES. Utilizarea semnăturii digitale. Securitatea în Reţelele informatice.

**Cunostinte pentru nota 5:**

Cunoasterea algoritmilor de criptare moderni DES si AES.

| Data completării: | Semnătura titularului de curs: | Semnătura titularului de seminar/laborator: |
|---|---|---|
| 08.09.2025 | Ș.l. dr. ing. Țepelea Laviniu<br>ltepelea@uoradea.ro<br>https://prof.uoradea.ro/ltepelea/ | Ș.l. dr. ing. Țepelea Laviniu<br>ltepelea@uoradea.ro<br>https://prof.uoradea.ro/ltepelea/ |

Data avizării în Departament:
24.09.2025

Director de Departament,
Ș.l. dr. ing. Adrian-Traian Burcă
aburca@uoradea.ro

Data aprobării în Consiliul Facultăţii:
25.09.2025

Decan,
Conf. univ. dr. ing. Eugen Ioan Gergely
egergely@uoradea.ro