# FIŞA DISCIPLINEI

*Anul universitar 2023 - 2024*

## 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] | 2 | 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 individual[8]** | **Nr. ore** |
|---|---|---|
| | Studiul după manual, suport de curs, bibliografie și notițe | 14 |
| | Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren | 8 |

[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.*

| | | |
|---|---|---|
| | Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri | 16 |
| | Tutoriat[9] | 4 |
| | Examinări[10] | 2 |
| | **3.3. Total ore alocate studiului individual[11] *(NOSI$_{sem}$)*** | **44** |
| | **3.4. Total ore din Planul de învățământ (*NOAD$_{sem}$*)** | **56** |
| | **3.5. Total ore pe semestru[12] (*NOAD$_{sem}$ + NOSI$_{sem}$*)** | **100** |
| | **3.6. Nr ore / ECTS** | **100** |
| | **3.7. Număr de credite[13]** | **4** |

[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 alocat 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*

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
- TOCpSdP = Număr total ore curs/săptămână din plan
- TOApSdP = 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

**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 si 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 şi 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. Competențe specifice acumulate[17]**

| | | | |
|---|---|---|---|
| | | Număr de credite alocat disciplinei[18] | 4 |
| **6.1. Competențe profesionale** | CP1 | Cunoașterea și utilizarea adecvată a noțiunilor teoretice fundamentale legate de criptografie | 1 |
| | CP2 | Capacitatea de a explica modul de construcție a algoritmilor criptografici | 0,5 |
| | CP3 | Capacitatea de a interpreta rezultatele obținute | 0,5 |
| | CP4 | Capacitatea de a implementa algoritmi criptografici | 0,5 |
| | CP5 | Capacitatea de a utiliza și modifica, conform cerințelor, algoritmii deja implementați | 0,5 |
| | CP6 | Capacitatea de a proiecta și realiza aplicații complexe care utilizează algoritmii și tehnicile învățate | 0,5 |
| **6.2. Competențe transversale** | CT1 | Dezvoltarea atitudinii pozitive față de muncă și responsabilitate pentru propria pregătire profesională | 0,25 |
| | CT2 | Dezvoltarea spiritului de muncă în echipă | 0,25 |

Repartizare credite pe competențe[19]

**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<br>Protecția împotriva atacurilor informatice |

**8. Conținuturi**

| **8.1. Curs[20]** | **Metode de predare[21]** | **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 |

[14] *Se menționează disciplinele obligatoriu 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] *Din planul de învățământ*

[19] *Creditele alocate disciplinei se distribuie pe competențe profesionale și transversale în funcție de specificul disciplinei*

[20] *Titluri de capitole și paragrafe*

[21] *Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții (pentru fiecare capitol, dacă este cazul)*

| | | |
|---|---|---|
| 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. Sisteneme 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 publica. Considerații generale. Funcții neinversabile. Trapa secretă. Securitatea sistemelor de criptare cu cheie publică. Comparație 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 asimetrica 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[22]/ 8.2.b. Laborator[23]/ 8.2.c. Proiect[24] / 8.2.d. Alte act.practice[25]) | **Metode de predare** | **Nr. ore** |
|---|---|---|
| Implementarea algoritmului lui Cezar | *Demonstrație practică, exercițiu* | 2 |
| Implementarea substituirii monoalfabetice | *Demonstrație practică, exercițiu, implementare* | 2 |
| Implementarea cifrurilor de permutare | *Demonstrație practică, exercițiu, implementare* | 2 |
| Implementarea sistemului de criptare afin | *Demonstrație practică, exercițiu, implementare* | 2 |
| Implementarea sistemului de criptare Polybios | *Demonstrație practică, exercițiu, implementare* | 2 |
| Implementarea sistemului de criptare Playfair | *Demonstrație practică, exercițiu, implementare* | 2 |
| Implementarea sistemului de criptare Vigenere | *Demonstrație practică, exercițiu, implementare* | 2 |
| Implementarea sistemului de criptare Rijndael (AES) | *Demonstrație practică, exercițiu, implementare* | 2 |
| Implementarea sistemului de criptare DES | *Demonstrație practică, exercițiu* | 2 |
| Implementarea sistemelor de criptare cu cheie publică – sistemul RSA | *Demonstrație practică, exercițiu* | 2 |
| Implementarea sistemelor de criptare cu cheie publică – sistemul El Gamal | *Demonstrație practică, exercițiu* | 2 |
| Modele de implementare. Steganografia | *Demonstrație practică, exercițiu* | 2 |
| Modele de implementare. Ascunderea de date | *Demonstrație practică, exercițiu* | 2 |
| Modele de implementare. Tranzacții financiare electronice | *Demonstrație practică, exercițiu* | 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 2010 |
| | 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 programului[26]**

Se realizează prin contacte periodice cu aceștia în vederea analizei problemei.

[22] *Discuții, dezbateri, prezentare și/sau analiză de lucrări, rezolvare de exerciții și probleme etc.*

[23] *Demonstrație practică, exercițiu, experiment etc.*

[24] *Studiu de caz, demonstrație, exercițiu, analiza erorilor etc.*

[25] *Alte tipuri de activități practice specifice*

[26] *Legătura cu alte discipline, utilitatea disciplinei pe piața muncii*

Conținutul disciplinei a fost stabilit ţinând cont de interacţiunile constructive ale cadrelor didactice, studenţilor şi a reprezentanţilor din mediul economic, ştiinţific, în cadrul manifestărilor ştiinţifice, întâlnirilor de lucru şi activităţilor de practică şi dezvoltare de proiecte a studenţilor.

**11. Evaluare**

| Tip activitate | 11.1 Criterii de evaluare | 11.2 Metode de evaluare | | 11.3 Pondere din nota finală | Obs.[27] |
|---|---|---|---|---|---|
| 11.4a Examen / Colocviu | ● Cunoștințe teoretice și practice însușite (cantitatea, corectitudinea, acuratețea) | Teste pe parcurs[28]: | 25% | 50% (minim 5) | CPE |
| | | Teme de casă: | 20% | | |
| | | Alte activități[29]: | 5% | | |
| | | Evaluare finală: | 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<br>● Răspuns oral<br>● Caiet de laborator, lucrări experimentale, referate, examinare de laborator, etc.<br>● Demonstrație practică | | 25% (minim 5) | nCPE |
| 11.4d Proiect | ● Calitatea proiectului realizat, corectitudinea documentației proiectului, justificarea soluțiilor alese | ● Autoevaluarea, prezentarea și/sau susținerea proiectului<br>● Evaluarea critică a unui proiect | | 25% (minim 5) | CPE |
| 11.5 Standard minim de performanță[30]: CP5 | | | | | 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: |_2_|_5_| / |_0_|_9_| / |_2_|_0_|_2_|_3_|

Data avizării în Departament: |_2_|_8_| / |_0_|_9_| / |_2_|_0_|_2_|_3_|

| | **Grad didactic, titlul, prenume, numele** | **Semnătura** |
|---|---|---|
| **Titular disciplină** | Conf. Univ. Dr. Nicolae CONSTANTINESCU | |
| **Responsabil program de studii** | Prof. Univ. Dr. Dana SIMIAN | |

[27] *CPE – condiționează participarea la examen; nCPE – nu condiționează participarea la examen; CEF - condiționează evaluarea finală; N/A – nu se aplică*

[28] *Se va preciza numărul de teste și săptămânile în care vor fi susținute.*

[29] *Cercuri științifice, concursuri profesionale etc.*

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

| | | |
|---|---|---|
| **Director Departament** | Prof. Univ. Dr. Mugur ACU | |

Str. Ion Rațiu Nr. 5-7
550012, Sibiu, România
stiinte**.ulbsibiu.ro**

Tel.: +40 269216642
Fax: +40 269 216617
E-mail: dep.matinf@ulbsibiu.ro