

## FIȘA DISCIPLINEI

### *Criptografie și securitate informațională*

#### 1. Date despre program

|     |                                   |  |
|-----|-----------------------------------|--|
| 1.1 | Instituția de învățământ superior | Universitatea din Pitești                        |
| 1.2 | Facultatea                        | Electronica, Comunicatii si Calculatoare         |
| 1.3 | Departamentul                     | Electronica, Calculatoare si Inginerie Electrica |
| 1.4 | Domeniul de studii                | Calculatoare și tehnologia informației           |
| 1.5 | Ciclul de studii                  | Licență  |
| 1.6 | Programul de studii / Calificarea | Calculatoare/Inginer                             |

#### 2. Date despre disciplină

|                           |                                      |    |     |           |   |  |                   |   |     |                     |     |  |
|---------------------------|--------------------------------------|----|-----|-----------|---|--|-------------------|---|-----|---------------------|-----|--|
| 2. Date despre disciplina |                                      |    |     |           |   |  |                   |   |     |                     |     |  |
| 2.1                       | Denumirea disciplinei                |    |     |           |   | <b>Criptografie și securitate informațională</b> |                   |   |     |                     |     |  |
| 2.2                       | Titularul activităților de curs      |    |     |           |   | Conf. dr. ing. Petre ANGHELESCU                  |                   |   |     |                     |     |  |
| 2.3                       | Titularul activităților de laborator |    |     |           |   | Conf. dr. ing. Petre ANGHELESCU                  |                   |   |     |                     |     |  |
| 2.4                       | Anul de studii                       | IV | 2.5 | Semestrul | I | 2.6  | Tipul de evaluare | E | 2.7 | Regimul disciplinei | S/O |  |

#### 3. Timpul total estimat

|  |                              |    |     |               |    |     |           |     |
|--|------------------------------|----|-----|---------------|----|-----|-----------|-----|
| 3.1  | Număr de ore pe săptămână    | 3  | 3.2 | din care curs | 2  | 3.3 | laborator | 1   |
| 3.4  | Total ore din planul de inv. | 42 | 3.5 | din care curs | 28 | 3.6 | laborator | 14  |
| Distribuția fondului de timp   |                              |    |     |               |    |     |           | ore |
| Studiul după manual, suport de curs, bibliografie și notițe                                    |                              |    |     |               |    |     |           | 26  |
| Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren |                              |    |     |               |    |     |           | 10  |
| Pregătire seminarii/laboratoare, teme, referate, portofolii, eseuri                            |                              |    |     |               |    |     |           | 10  |
| Tutoriat   |                              |    |     |               |    |     |           | 2   |
| Examinări  |                              |    |     |               |    |     |           | 6   |
| Alte activități .....  |                              |    |     |               |    |     |           | -   |
| 3.7  | Total ore studiu individual  | 54 |     |               |    |     |           |     |
| 3.8  | Total ore pe semestru        | 96 |     |               |    |     |           |     |
| 3.9  | Număr de credite             | 4  |     |               |    |     |           |     |

#### 4. Precondiții (acolo unde este cazul)

|     |               |   |
|-----|---------------|---|
| 4.1 | De curriculum | Parcursirea disciplinelor de matematică (in special matematici speciale și algebra, capitolele referitoare la teoria numerelor), Bazele inteligenței artificiale. |
| 4.2 | De competențe | <b>C1</b> Operarea cu fundamente stiintifice, ingineresti si ale informaticii   |

#### 5. Condiții (acolo unde este cazul)

|     |                                |  |
|-----|--------------------------------|--|
| 5.1 | De desfășurare a cursului      | Sală cu o capacitate de minim 100 locuri dotată cu două table, videoproiector și ecran de proiecție.                               |
| 5.2 | De desfășurare a laboratorului | Laboratorul disciplinei (sala T 215), Calculatoare (minim 15), Internet, Mediul de programare Visual Studio .NET (Visual C++, C#). |

#### 6. Competențe specifice acumulate

|                         |  |
|-------------------------|--|
| Competențe profesionale | <b>C5 Proiectarea, gestionarea ciclului de viata, integrarea si integritatea sistemelor hardware, software (4 puncte credit)</b><br>C5.1 Precizarea criteriilor relevante privind ciclul de viata, calitatea, securitatea si interactiunea sistemului de calcul cu mediul si cu operatorul uman (0,5 puncte credit)<br>C5.2 Utilizarea unor cunostinte interdisciplinare pentru adaptarea sistemului informatic în raport cu cerintele domeniului de aplicatii (1 punct credit)<br>C5.3 Utilizarea unor principii si metode de baza pentru asigurarea securitatii, sigurantei si usurintei în exploatare a sistemelor de calcul (0,5 puncte credit)<br>C5.4 Utilizarea adecvata a standardelor de calitate, siguranta si securitate în prelucrarea informatiilor (1 punct credit)<br>C5.5 Realizarea unui proiect incluzând identificarea si analiza problemei, proiectarea, dezvoltarea si demonstrând o înțelegere a nevoii de calitate (1 punct credit) |
| Competențe transversale |  |

#### 7. Obiectivele disciplinei

|                                       |   |
|---------------------------------------|---|
| 7.1 Obiectivul general al disciplinei | Insusirea cunostintelor referitoare la probleme din teoria numerelor care stau la baza sistemelor criptografice, algoritmi de criptare si decriptare conventionali, algoritmi de criptare si decriptare cu cheie publica, generatoare de secvente pseudo-aleatoare, algoritmi de criptare/decriptare bazați pe teoria automatelor celulare (sisteme dinamice) |
|---------------------------------------|---|

|                           |   |
|---------------------------|---|
|                           | haotice). In cadrul cursului sunt prezentate tehnici de criptare/decriptare și elemente de criptanaliză.  |
| 7.2 Obiectivele specifice | <p><i>Obiective cognitive</i><br/> Insușirea cunoștințelor de bază privind domeniul securității prin criptografie (criptosistem simetric și asimetric, generatoare LFSR, criptografie cu sisteme dinamice, criptanaliza).</p> <p><i>Obiective procedurale</i><br/> Insușirea tehnicilor de baza pentru proiectarea și implementarea sistemelor criptografice ce folosesc algoritmi simetrici, respectiv asimetrici, inclusiv elemente de criptanaliza.</p> <p><i>Obiective atitudinale</i><br/> Dobândirea deprinderilor privind ordinea și lucrul în echipă în vederea realizării rapide de aplicații criptografice utilizând limbajul C#.</p> |

## 8. Conținuturi

| 8.1. Curs |   | Metode de predare                                    | Observații<br>Resurse folosite           |
|-----------|---|--|--|
| 1.        | <b>Noțiuni de bază ale criptografiei (1)</b><br>1. <i>Terminologie și concepte folosite în criptografie:</i> Criptologie, Criptografie, Criptanaliza, Criptosistem, Cifruri bloc, Cifruri stream, Criptare hardware, Criptare software.<br>2. <i>Servicii de securitate:</i> confidențialitate, autenticitate, integritate, nerepudiare, controlul accesului, disponibilitate.<br>-Timp alocat <b>2 ore</b> | Prelegere<br>Dezbateri<br>Descriere și exemplificare | Tabla,<br>Calculator,<br>Videoproiector. |
| 2.        | <b>Noțiuni de bază ale criptografiei (2)</b><br>1. <i>Atacuri asupra securității sistemelor criptografice:</i> atacuri pasive și atacuri active – mod de operare, caracteristici.<br>2. <i>Taxonomia sistemelor criptografice:</i> Criptosisteme simetrice (cu cheie secretă), Criptosisteme asimetrice (cu cheie publică).<br>-Timp alocat <b>2 ore</b>  | Prelegere<br>Dezbateri<br>Descriere și exemplificare | Tabla,<br>Calculator,<br>Videoproiector. |
| 3.        | <b>Criptografie clasică (cu cheie secretă, simetrică) (1)</b><br>1. Clasificarea metodelor de criptare simetrice (substituție, transpoziție, combinate).<br>2. Cifruri de substituție monoalfabetică (cifrul Caesar, cifrul Polybius).<br>3. Criptanaliza cifrurilor de substituție monoalfabetică.<br>-Timp alocat <b>2 ore</b>  | Prelegere<br>Dezbateri<br>Studiu de caz              | Tabla,<br>Calculator,<br>Videoproiector. |
| 4.        | <b>Criptografie clasică (cu cheie secretă, simetrică) (2)</b><br>1. Cifruri de substituție omofonica.<br>2. Criptanaliza cifrurilor de substituție omofonica.<br>-Timp alocat <b>2 ore</b>  | Prelegere<br>Dezbateri<br>Studiu de caz              | Tabla,<br>Calculator,<br>Videoproiector. |
| 5.        | <b>Criptografie clasică (cu cheie secretă, simetrică) (3)</b><br>1. Cifruri de substituție poligramică.<br>2. Criptanaliza cifrurilor de substituție poligramică.<br>-Timp alocat <b>2 ore</b>  | Prelegere<br>Dezbateri<br>Studiu de caz              | Tabla,<br>Calculator,<br>Videoproiector. |
| 6.        | <b>Criptografie clasică (cu cheie secretă, simetrică) (4)</b><br>3. Cifruri de substituție polialfabetică.<br>4. Criptanaliza cifrurilor de substituție polialfabetică.<br>-Timp alocat <b>2 ore</b>  | Prelegere<br>Dezbateri<br>Studiu de caz              | Tabla,<br>Calculator,<br>Videoproiector. |
| 7.        | <b>Criptografie clasică (cu cheie secretă, simetrică) (5)</b><br>1. Cifruri de permutare/transpoziție.<br>2. Criptanaliza cifrurilor de permutare/transpoziție.<br>-Timp alocat <b>2 ore</b>  | Prelegere<br>Dezbateri<br>Studiu de caz              | Tabla,<br>Calculator,<br>Videoproiector. |
| 8.        | <b>Sistemul de criptare DES (Data Encryption Standard)</b><br>1. Considerații generale.<br>2. Descrierea sistemului criptografic.<br>3. Modalități de atac asupra DES.<br>-Timp alocat <b>2 ore</b>   | Prelegere<br>Dezbateri<br>Studiu de caz              | Tabla,<br>Calculator,<br>Videoproiector. |
| 9.        | <b>Sistemul de criptare AES (Advanced Encryption Standard)</b><br>1. Considerații generale.<br>2. Descrierea sistemului criptografic.<br>3. Modalități de atac asupra AES.<br>-Timp alocat <b>2 ore</b>   | Prelegere<br>Dezbateri<br>Studiu de caz              | Tabla,<br>Calculator,<br>Videoproiector. |
| 10.       | <b>Criptografie asimetrică (cu cheie publică)</b><br>1. Considerații generale.<br>2. Funcții neinvertibile.<br>3. Securitatea sistemelor de criptare cu cheie publică.<br>4. Comparație între criptarea simetrică și cea asimetrică.  | Prelegere<br>Dezbateri<br>Descriere și exemplificare | Tabla,<br>Calculator,<br>Videoproiector. |

|   |   |   |  |
|---|---|---|--|
|   | -Timp alocat <b>2 ore</b>   |   |  |
| 11.   | <b>Sistemul de criptare RSA (Rivest-Shamir Adleman)</b> <ol style="list-style-type: none"> <li>1. Considerații generale.</li> <li>2. Descrierea sistemului criptografic RSA.</li> <li>3. Exemplu.</li> <li>4. Generalizarea sistemului de criptare RSA.</li> </ol>  | Prelegere<br>Dezbateri<br>Studiu de caz                     | Tabla,<br>Calculator,<br>Videoproiector.   |
|   | -Timp alocat <b>2 ore</b>   |   |  |
| 12.   | <b>Generatoare de secvențe pseudoaleatoare.</b> <ol style="list-style-type: none"> <li>1. Generatoare bazate pe LFSR.</li> <li>2. Generatoare bazate pe sisteme dinamice (haotice).</li> <li>3. Generatoare bazate pe sisteme bioinspirate (automate celulare).</li> <li>4. Metode de testare a calității secvențelor pseudoaleatoare generate. Standardul NIST.</li> </ol> | Prelegere<br>Dezbateri<br>Studiu de caz                     | Tabla,<br>Calculator,<br>Videoproiector.   |
|   | -Timp alocat <b>2 ore</b>   |   |  |
| 13.   | <b>Sisteme criptografice simetrice bazate pe automate celulare (sisteme dinamice haotice) (1)</b> <ol style="list-style-type: none"> <li>1. Considerații generale.</li> <li>2. Sisteme criptografice ce funcționează pe baza teoriei automatelor celulare.</li> </ol>   | Prelegere<br>Dezbateri<br>Studiu de caz                     | Tabla,<br>Calculator,<br>Videoproiector.   |
|   | -Timp alocat <b>2 ore</b>   |   |  |
| 14.   | <b>Sisteme criptografice simetrice bazate pe automate celulare (sisteme dinamice haotice) (2)</b> <ol style="list-style-type: none"> <li>1. Exemple.</li> <li>2. Analiza performanțelor algoritmilor dezvoltati.</li> </ol>   | Prelegere<br>Dezbateri<br>Studiu de caz                     | Tabla,<br>Calculator,<br>Videoproiector.   |
|   | -Timp alocat <b>2 ore</b>   |   |  |
| <b>Bibliografie</b> <ol style="list-style-type: none"> <li>1. Petre Angheliescu, "AUTOMATE CELULARE – fundamente și abordări practice cu aplicații în criptare", Editura Matrix ROM, ISBN 978-973-755-821-3, București, 2012 (disponibila la biblioteca si in laborator).</li> <li>2. Rodriguez-Henriquez, F., Saqib, N. A., Diaz-Perez, A., Koc, C. K., "Cryptographic algorithms on reconfigurable hardware", Springer Science + Business Media, LLC, ISBN 0-387-33883-7, 2006.</li> <li>3. Koc, C. K., "Cryptographic engineering", Springer Science + Business Media, LLC, ISBN: 978-0-387-71816-3, 2009.</li> <li>4. Menezes, A., Oorschot, P., Vanstone, S., "Handbook of applied cryptography", CRC Press, ISBN: 0-8493-8523-7, 1996.</li> <li>5. C. Shannon. Communication Theory of Secrecy Systems. Bell Sys. Tech. J. 28, pp. 656–715, 1949. (netlab.cs.ucla.edu/wiki/files/shannon1949.pdf).</li> <li>6. Petre Angheliescu, Teza de doctorat: „Proiectarea si analiza automatelor celulare pentru prelucrarea informatiei”, Conducător de doctorat – prof. univ. dr. ing. Emil Sofron, Pitesti, Decembrie 2007 (disponibila in laborator).</li> <li>7. Petre Angheliescu, Matthew Szudzik "Exploring Hybrid Cellular Automata (HCA) for Cryptographic Applications", A New Kind of Science Summer School, Boston, SUA, 26.06.2011 – 17.07.2011, <a href="http://www.wolframscience.com/summerschool/2011/participants/angheliescu.html">http://www.wolframscience.com/summerschool/2011/participants/angheliescu.html</a>.</li> <li>8. Stephen Wolfram, "A new kind of science", Wolfram Media Inc., ISBN: 1-57955-008-8, 2002 (disponibila in laborator).</li> <li>9. Petre Angheliescu, <i>Criptografie si securitate informationala</i> – Note de curs, format letric si electronic, 2016</li> </ol> |   |   |  |
| <b>8.2. Aplicații – Laborator</b>   |   | <b>Metode de predare</b>                                    | <b>Observații<br/>Resurse folosite</b>   |
| 1.  | Implementarea software și analiza cifrurilor de criptare simetrice (cu cheie secretă) monoalfabetice și polialfabetice (cifrul Caesar, cifrul Polybius, cifrul Vigenere, cifrul Playfair).  | Studiul de caz<br>Exercițiul<br>Lucrul în grup<br>Dezbateri | Calculator,<br>Visual Studio .NET (C#, Visual C++) instalat pe fiecare stație de lucru |
|   | -Timp alocat <b>4 ore</b>   |   |  |
| 2.  | Implementarea software și analiza sistemelor de criptare simetrice DES și AES.  | Studiul de caz<br>Exercițiul<br>Lucrul în grup<br>Dezbateri |  |
|   | -Timp alocat <b>4 ore</b>   |   |  |
| 3.  | Proiectarea și implementarea generatoarelor de secvențe pseudoaleatoare (LFSR, automate celulare) utilizate la construirea algoritmilor criptografici. Utilizarea testelor statistice NIST pentru analiza calității secvențelor generate.   | Studiul de caz<br>Exercițiul<br>Lucrul în grup<br>Dezbateri |  |
|   | -Timp alocat <b>4 ore</b>   |   |  |
| 4.  | Proba practica. Verificarea deprinderilor și abilităților practice dobândite de fiecare student.  | Exercițiul  |  |
|   | -Timp alocat <b>2 ore</b>   |   |  |
| <b>Bibliografie</b> <ol style="list-style-type: none"> <li>1. Petre Angheliescu, "AUTOMATE CELULARE – fundamente și abordări practice cu aplicații în criptare", Editura Matrix ROM, ISBN 978-973-755-821-3, București, 2012 (disponibila la biblioteca si in laborator).</li> <li>2. Rodriguez-Henriquez, F., Saqib, N. A., Diaz-Perez, A., Koc, C. K., "Cryptographic algorithms on reconfigurable hardware", Springer Science + Business Media, LLC, ISBN 0-387-33883-7, 2006.</li> <li>3. Koc, C. K., "Cryptographic engineering", Springer Science + Business Media, LLC, ISBN: 978-0-387-71816-3, 2009.</li> <li>4. Menezes, A., Oorschot, P., Vanstone, S., "Handbook of applied cryptography", CRC Press, ISBN: 0-8493-8523-7, 1996.</li> <li>5. Stephen Wolfram, "A new kind of science", Wolfram Media Inc., ISBN: 1-57955-008-8, 2002 (disponibila in laborator).</li> <li>6. Petre Angheliescu, <i>Criptografie si securitate informationala</i> – Note de laborator, format electronic, 2016</li> </ol>  |   |   |  |

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

Atat pentru elaborarea tematicii, cât și pentru alegerea metodelor de predare/învățare, titularul disciplinei a analizat pe de o parte oferta academică a unor instituții naționale și internaționale de prestigiu de învățământ superior (UT Cluj, UP București, MIT, NPTEL), iar pe de altă parte a avut întâlniri de lucru cu specialiști din producție și angajatori, inclusiv participarea la conferințe și workshop-uri din domeniu. În acest fel, disciplina respecta nivelul impus de rigorile academice și ofera în același timp abilitățile necesare pentru dezvoltarea de aplicații criptografice în vederea securizării informațiilor stocate sau transmise în rețelele de comunicații.

#### 10. Evaluare

| Tip activitate                     | 10.1 Criterii de evaluare  | 10.2 Metode de evaluare             | 10.3 Pondere din nota finală |
|------------------------------------|--|-------------------------------------|------------------------------|
| 10.4 Curs                          | Tema de casa   | Referat și susținere tema           | 20%                          |
|                                    | Evaluare pe parcurs  | Test scris la jumătatea semestrului | 20%                          |
|                                    | Evaluare finală  | Probă scrisă                        | 50%                          |
| 10.5 Laborator                     | Verificarea deprinderilor și abilităților practice dobândite de fiecare student.   | Probă practică                      | 10%                          |
| 10.6 Standard minim de performanță | <p>* Se are în vedere rezolvarea cerințelor de la lucrările de laborator și nota minimă 5 la proba practică.</p> <p>* Set de cunoștințe minimale pentru promovarea examenului final:<br/> (sa cunoască terminologia și taxonomia sistemelor criptografice, să descrie tipurile de atacuri criptografice, să descrie serviciile de securitate, să descrie un sistem de criptare simetric, să descrie un sistem de criptare asimetric, să prezinte un generator de numere pseudoaleatoare, să stăpânească metodele de proiectare, realizare și evaluare a unui algoritm criptografic).</p> |                                     |                              |

Data completării  
22.09.2017

Titular de curs  
Conf. dr. ing. Petre ANGHELESCU

Titular de laborator  
Conf. dr. ing. Petre ANGHELESCU

Data avizării în departament  
25.09.2017

Director de departament  
Prof. univ. dr. ing. Gheorghe SERBAN