

## FIȘA DISCIPLINEI

### 1. Date despre program

|                                       |                                       |
|---------------------------------------|---------------------------------------|
| 1.1 Instituția de învățământ superior | Universitatea Tehnică din Cluj-Napoca |
| 1.2 Facultatea                        | Facultatea de Științe                 |
| 1.3 Departamentul                     | Matematică și Informatică             |
| 1.4 Domeniul de studii                | Informatică                           |
| 1.5 Ciclul de studii                  | Licență                               |
| 1.6 Programul de studii / Calificarea | Informatică                           |
| 1.7 Forma de învățământ               | IF – învățământ cu frecvență          |
| 1.8 Codul disciplinei                 | 21.00                                 |

### 2. Date despre disciplină

|                                          |                                                                      |                       |     |
|------------------------------------------|----------------------------------------------------------------------|-----------------------|-----|
| 2.1 Denumirea disciplinei                | Criptografie                                                         |                       |     |
| 2.2 Titularul de curs                    | Conf. univ. dr. Andrei HORVAT-MARC <i>andrei.horvat@mi.utcluj.ro</i> |                       |     |
| 2.3 Titularul activităților de laborator | Conf. univ. dr. Andrei HORVAT-MARC <i>andrei.horvat@mi.utcluj.ro</i> |                       |     |
| 2.4 Anul de studiu                       | I                                                                    | 2.5 Semestrul         | 1   |
|                                          |                                                                      | 2.6 Tipul de evaluare | C   |
| 2.7 Regimul disciplinei                  | Categoriza formativă                                                 |                       | DS  |
|                                          | Opționalitate                                                        |                       | DOB |

### 3. Timpul total estimat

|                                                                                                  |    |           |          |    |             |  |               |    |             |   |
|--------------------------------------------------------------------------------------------------|----|-----------|----------|----|-------------|--|---------------|----|-------------|---|
| 3.1 Număr de ore pe săptămână                                                                    | 2  | din care: | 3.2 Curs | 1  | 3.3 Seminar |  | 3.3 Laborator | 1  | 3.3 Proiect |   |
| 3.4 Număr de ore pe semestru                                                                     | 28 | din care: | 3.5 Curs | 14 | 3.6 Seminar |  | 3.6 Laborator | 14 | 3.6 Proiect |   |
| 3.7 Distribuția fondului de timp (ore pe semestru) pentru:                                       |    |           |          |    |             |  |               |    |             |   |
| (a) Studiul după manual, suport de curs, bibliografie și notițe                                  |    |           |          |    |             |  |               |    |             | 7 |
| (b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren |    |           |          |    |             |  |               |    |             | 4 |
| (c) Pregătire laboratoare, teme, referate, portofolii și eseuri                                  |    |           |          |    |             |  |               |    |             | 7 |
| (d) Tutoriat                                                                                     |    |           |          |    |             |  |               |    |             | 2 |
| (e) Examinări                                                                                    |    |           |          |    |             |  |               |    |             | 2 |
| (f) Alte activități:                                                                             |    |           |          |    |             |  |               |    |             | 0 |
| 3.8 Total ore studiu individual (suma (3.7(a))...3.7(f)))                                        |    |           |          |    | 22          |  |               |    |             |   |
| 3.9 Total ore pe semestru (3.4+3.8)                                                              |    |           |          |    | 50          |  |               |    |             |   |
| 3.10 Numărul de credite                                                                          |    |           |          |    | 2           |  |               |    |             |   |

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

|                   |                                                                                   |
|-------------------|-----------------------------------------------------------------------------------|
| 4.1 de curriculum | Cunoașterea unui limbaj de programare și a noțiunilor de bază ale algebrei        |
| 4.2 de competențe | <ul style="list-style-type: none"> <li>Utilizarea sistemelor de calcul</li> </ul> |

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

|                                     |                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.1. de desfășurare a cursului      | <ul style="list-style-type: none"> <li>Sală de curs dotată corespunzător: tablă, cretă, videoproiector, internet.</li> <li>Studentii trebuie să dețină un cont pe platforma kb.cunbm.utcluj.ro. Pentru a participa la cursurile online (dacă este cazul), studenții trebuie să dispună de sistem de calcul, camera si microfon.</li> </ul> |
| 5.2. de desfășurare a laboratorului | <ul style="list-style-type: none"> <li>Sală de laborator dotată corespunzător: tablă, cretă, calculatoare, rețea, internet, videoproiector.</li> </ul>                                                                                                                                                                                     |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• Studenții vor fi înrolați pe platforma KnowledgeBase, pentru accesarea laboratorului/temelor în format electronic. Rezolvările problemelor propuse ca temă, vor fi încărcate pe platformă.</li> <li>• Termenul predării fiecărei lucrări de laborator este stabilit de titular în momentul enunțării temei. Pentru predarea cu întârziere a lucrărilor de laborator, lucrările vor fi depunctate cu 1 pct./zi de întârziere. Fiecare temă se notează cu punctaje între 1 și 10, nota finală la laborator este media aritmetică a notelor. O lucrare nepredată se notează cu 0. Temele se încarcă pe platforma kb.cunbm.utcluj.ro. Pentru a participa la laboratoarele online (dacă este cazul) studenții trebuie să dispună de sistem de calcul, camera și microfon.</li> </ul> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 6. Competențele specifice acumulate

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Competențe profesionale | <p>Prelucrarea matematica a datelor, analiza și interpretarea unor fenomene și interpretarea rezultatelor prelucrării datelor prin sisteme de criptare</p> <p>Analiza comparativă a rezultatelor obținute prin utilizarea diverselor sisteme de criptare</p> <p>Elaborarea și analiza unor algoritmi pentru rezolvarea problemelor</p> <p>Identificarea noțiunilor de baza folosite în construcția și specificarea algoritmilor de criptare a informației și a altor protocoale criptografice</p> <p>Explicarea etapelor care intervin în algoritmii criptografici</p> |
| Competențe transversale | <p>Aplicarea regulilor de muncă organizată și eficientă, a unor atitudini responsabile față de domeniul didactic-științific, pentru valorificarea creativă a propriului potențial, cu respectarea principiilor și a normelor de etică profesională</p> <p>Utilizarea unor metode și tehnici eficiente de învățare, informare, cercetare și dezvoltare a capacităților de valorificare a cunoștințelor, de adaptare la cerințele unei societăți dinamice și de comunicare în limba română și într-o limbă de circulație internațională</p>                              |

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

|                                       |                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.1 Obiectivul general al disciplinei | <p>Insușirea de către studenți a noțiunilor, conceptelor și exemplelor fundamentale din criptografie și securitatea datelor</p> <p>Familiarizarea studenților cu tehnici de bază din criptografie și criptanaliză. Construcția și analiza unor algoritmi criptografici de bază</p>                            |
| 7.2 Obiectivele specifice             | <ul style="list-style-type: none"> <li>• Să explice funcționarea principalilor algoritmi criptografici.</li> <li>• Să utilizeze noțiuni și rezultate de bază din aritmetică.</li> <li>• Să calculeze cheile, mesajele în clar și mesajele criptate în cadrul principalelor criptosisteme studiate.</li> </ul> |

## 8. Conținuturi

| 8.1 Curs                                                                                                                                                                                                            | Nr. ore | Metode de predare                                                                   | Observații |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------------------------------------------------------------------------------|------------|
| Noțiuni introductive. Securitatea informației și criptografia. Concepte și noțiuni de bază.                                                                                                                         | 2 ore   | Prelegerea participativă, problematizarea, expunerea, demonstrația, exemplificarea. |            |
| Sisteme simetrice de criptare. Cifruri de substituție: monoalfabetice (Cezar, afin, Polybos), polialfabetice (Vigenere, Playfair, Homofonic). Criptanaliza sistemelor de criptare monoalfabetice și polialfabetice. | 2 ore   |                                                                                     |            |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                |                          |                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------------|-------------------|
| Sisteme fluide de criptare. Sisteme sincronizabile și auto-sincronizabile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2 ore          |                          |                   |
| Sistemul de criptare DES. Modalități de atac.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2 ore          |                          |                   |
| Sistemul de criptare AES. Modalități de atac.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2 ore          |                          |                   |
| Criptare cu cheie publică.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2 ore          |                          |                   |
| Sistemul de criptare RSA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2 ore          |                          |                   |
| <b>Bibliografie</b><br>1. Menezes, A., Oorschot, P., Vanstone, S., Handbook of Applied Cryptography, CRC Press, Florida, 1998<br>2. Christof Paar, Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010<br>3. D. Stinton, Cryptography, Theory et Praticte, Second Edition, Chapman & Hall/CRC, 2002<br>4. Yan, Song Y., Number theory for computing, ed. a II-a, Springer Verlag, 2002<br>5. <a href="https://www.researchgate.net/profile/Adrian_AtanasIU/publication/308791446_Securitatea_Informatiei_vol_1_Criptografie/links/57f1f67608ae280dd0b2804e/Securitatea-Informatiei-vol-1-Criptografie.pdf">https://www.researchgate.net/profile/Adrian_AtanasIU/publication/308791446_Securitatea_Informatiei_vol_1_Criptografie/links/57f1f67608ae280dd0b2804e/Securitatea-Informatiei-vol-1-Criptografie.pdf</a>             |                |                          |                   |
| <b>8.2 Laborator</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>Nr. ore</b> | <b>Metode de predare</b> | <b>Observații</b> |
| Cifrurile Richelieu, Cezar, afin, Polybos, afin, Hill.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2 ore          |                          |                   |
| Cifrurile Vigenere, Playfair, Homofonic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2 ore          |                          |                   |
| Sistemele cu cheie fluidă                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2 ore          |                          |                   |
| Sisteme de criptare înrudite de DES: 3DES, DES-X, IDEA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2 ore          |                          |                   |
| Sisteme AES: RC6, Serpent, Twofish                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2 ore          |                          |                   |
| Comparație între criptare simetrică și criptare cu cheie publică.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2 ore          |                          |                   |
| Algoritmul Euclid extins. Teorema chineză a resturilor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2 ore          |                          |                   |
| <b>Bibliografie</b><br>1. Menezes, A., Oorschot, P., Vanstone, S., Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, 1998<br>2. Christof Paar, Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010<br>3. D. Stinton, Cryptography, Theory et Praticte, Second Edition, Chapman & Hall/CRC, 2002<br>4. Yan, Song Y., Number theory for computing, ed. a II-a, Springer Verlag, 2002<br>5. <a href="https://www.researchgate.net/profile/Adrian_AtanasIU/publication/308791446_Securitatea_Informatiei_vol_1_Criptografie/links/57f1f67608ae280dd0b2804e/Securitatea-Informatiei-vol-1-Criptografie.pdf">https://www.researchgate.net/profile/Adrian_AtanasIU/publication/308791446_Securitatea_Informatiei_vol_1_Criptografie/links/57f1f67608ae280dd0b2804e/Securitatea-Informatiei-vol-1-Criptografie.pdf</a> |                |                          |                   |

## 9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului

Tematica acestui curs este în concordanță cu ceea ce este prevăzut în programul de studii la nivel licență al celor mai importante universități din țară și străinătate.

## 10. Evaluare

| Tip activitate | 10.1 Criterii de evaluare                                                                                                       | 10.2 Metode de evaluare                                                                                              | 10.3 Pondere din nota finală |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------|
| 10.4 Curs      | Cunoașterea principalelor aspecte teoretice prezentate la curs.                                                                 | Evaluare prin probă scrisă sau test online (în funcție de situația epidemiologică în vigoare în perioada examinării) | 60 %                         |
| 10.5 Laborator | Capacitatea de a explica și opera cu noțiunile prezentate la curs, cunoașterea și utilizarea sistemelor de criptare prezentate. | Verificare pe parcursul semestrului                                                                                  | 40 %                         |

|                                                                                                                                                                                                                               |  |  |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
|                                                                                                                                                                                                                               |  |  |  |
| 10.6 Standard minim de performanță<br>Cunoașterea noțiunilor de bază legate de criptografie și a sistemelor de bază. Obținerea notei cel puțin 5 la examenul scris și obținerea mediei cel puțin 5 la lucrările de laborator. |  |  |  |

| Data completării: | Titulari  | Titlu Prenume NUME                 | Semnătura |
|-------------------|-----------|------------------------------------|-----------|
| 10.09.2026        | Curs      | Conf. univ. dr. Andrei HORVAT-MARC |           |
|                   | Laborator | Conf. univ. dr. Andrei HORVAT-MARC |           |
|                   |           |                                    |           |

|                                                                         |                                                 |
|-------------------------------------------------------------------------|-------------------------------------------------|
| Data avizării în Consiliul Departamentului de Matematică și Informatică | Director Departament Matematică și Informatică, |
| 14.09.2026                                                              | Conf. univ. dr. Cosmin Sabo                     |
| Data aprobării în Consiliul Facultății de Științe                       | Decan,                                          |
| 17.09.2026                                                              | Conf. univ. dr. Monica Marian                   |