**fişa disciplinei**

**1. Date despre program**

|  |  |
| --- | --- |
| 1.1 Instituţia de învăţământ superior | **Universitatea Babeş-Bolyai Cluj-Napoca** |
| 1.2 Facultatea | **Matematică şi Informatică** |
| 1.3 Departamentul | **Informatică** |
| 1.4 Domeniul de studii | **Informatică** |
| 1.5 Ciclul de studii | **licenţă** |
| 1.6 Programul de studiu / Calificarea | **Informatică (în limba germană)** |

**2. Date despre disciplină**

|  |  |
| --- | --- |
| 2.1 Denumirea disciplinei | **Criptografie** |
| 2.2 Titularul activităţilor de curs | Lekt. dr. Thu Hang Bui |
| 2.3 Titularul activităţilor de seminar | Lekt. dr. Thu Hang Bui |
| 2.4 Anul de studiu | **2** | 2.5 Semestrul | **4** | 2.6. Tipul de evaluare | **C** | 2.7 Regimul disciplinei | **optional** |
| 2.8. Codul disciplinei | **MLG0059** |

**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 | **1+2pr** |
| 3.4 Total ore din planul de învăţământ | **60** | Din care: 3.5 curs | **24** | 3.6 seminar/laborator | **36** |
| Distribuţia fondului de timp: | ore |
| Studiul după manual, suport de curs, bibliografie şi notiţe | **20** |
| Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren | **30** |
| Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri | **20** |
| Tutoriat | **1** |
| Examinări  | **4** |
| Alte activităţi: .................. |  |
| 3.7 Total ore studiu individual | **65** |
| 3.8 Total ore pe semestru | **125** |
| 3.9 Numărul de credite | **5** |

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

|  |  |
| --- | --- |
| 4.1 de curriculum | * Fundamentele algebrice ale informaticii
 |
| 4.2 de competenţe |  |

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

|  |  |
| --- | --- |
| 5.1 De desfăşurare a cursului | * Videoproiector
 |
| 5.2 De desfăşurare a seminarului/laboratorului | * Calculatoare
 |

**6. Competenţele specifice acumulate**

|  |  |  |  |
| --- | --- | --- | --- |
| **Competenţe profesionale** |

|  |
| --- |
| C 4.1 Definirea conceptelor şi principiilor de bază ale informaticii, precum şi a teoriilor şi modelelor matematice C 4.3 Identificarea modelelor si metodelor adecvate pentru rezolvarea unor probleme reale C 4.4 Utilizarea simulării pentru studiul comportamentului modelelor realizate si evaluarea performantelor C 4.5 Încorporarea de modele formale în aplicaţii specifice din diverse domenii  |

|  |
| --- |
|  C6.4 Efectuarea de măsurători de performanţă pentru timpi de răspuns, consum de resurse; stabilirea drepturilor de acces.  |

 |
| **Competenţe transversale** | **CT1** Aplicarea regulilor de muncă organizată şi eficientă, a unor atitudini responsabile faţă de domeniul didactic-ştiinţific, pentru valorificarea creativă a propriului potenţial, cu respectarea principiilor şi a normelor de etică profesională **CT2** Desfăşurarea eficientă a activităţilor organizate într-un grup inter-disciplinar și dezvoltarea capacităţilor empatice de comunicare inter-personală, de relaţionare şi colaborare cu grupuri diverse **CT3** Utilizarea unor metode şi tehnici eficiente de învăţare, informare, cercetare şi dezvoltare a capacităţilor de valorificare a cunoştinţelor, de adaptare la cerinţele unei societăţi dinamice și de comunicare în limba română și într-o limbă de circulație internațională  |

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

|  |  |
| --- | --- |
| 7.1 Obiectivul general al disciplinei | * Prezentarea principalilor algoritmi criptografici
 |
| 7.2 Obiectivele specifice | * Se studiaza algoritmi de teoria numerelor si algebra, fiind apoi implementati in proiecte concrete.
 |

**8. Conţinuturi**

|  |  |  |
| --- | --- | --- |
| 8.1 Curs | Metode de predare | Observaţii |
| 1. Criptografie clasica. Exemple. Sisteme de criptare. | expunerea, conversaţia, discutarea unor studii de caz |  |
| 2. Principiile criptografiei moderne. Scenarii de atac. Metode de criptanaliza. | expunerea, conversaţia, discutarea unor studii de caz |  |
| 3. Securitatea sistemelor criptografice. | expunerea, conversaţia, discutarea unor studii de caz |  |
| 4. Criptografia simetrica. Moduri de criptare. | expunerea, conversaţia, discutarea unor studii de caz |  |
| 5. Data Encryption Standard (DES) | expunerea, conversaţia, discutarea unor studii de caz |  |
| 6. Advanced Encryption Standard (AES) | expunerea, conversaţia, discutarea unor studii de caz |  |
| 7. Criptografie cu cheie publica | expunerea, conversaţia, discutarea unor studii de caz |  |
| 8. Criptografie cu cheie publica | expunerea, conversaţia, discutarea unor studii de caz |  |
| 9. Semnaturi digitale | expunerea, conversaţia, discutarea unor studii de caz |  |
| 10. Functii de hash | expunerea, conversaţia, discutarea unor studii de caz |  |
| 11. Functii de hash. | expunerea, conversaţia, discutarea unor studii de caz |  |
| 12. Algoritmi de criptare in retele GSM. | expunerea, conversaţia, discutarea unor studii de caz |  |
| 13. Criptanaliza sistemelor GSM. | expunerea, conversaţia, discutarea unor studii de caz |  |
| 14. Aspecte practice ale criptografiei cu cheie publica. | expunerea, conversaţia, discutarea unor studii de caz |  |
| In limba germana: 1. Buchmann Johannes, Einführung in die Kryptographie, Springer, 2001.
2. Klein, Andreas, Visuelle Kryptographie, Springer 2007.
3. Schwenk, J., Sicherheit und Kryptographie im Internet, Vieweg, 2005.

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006.2. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography. CRC Press,Boca Raton, 1997. (<http://www.math.uwaterloo.ca/~ajmeneze>)3. B. Schneier, Applied Cryptography. John Wiley & Sons, 1996. |
| 8.2 Seminar / laborator | Metode de predare | Observaţii |
| L1. Criptografie clasica I. | problematizarea, exemplificarea |  |
| L2. Criptografie clasica II.  | problematizarea, exemplificarea |  |
| L3. Criptografie clasica III. | problematizarea, exemplificarea |  |
| L4. DES. | problematizarea, exemplificarea |  |
| L5. AES. | problematizarea, exemplificarea |  |
| L6. Criptografie cu cheie publica | problematizarea, exemplificarea |  |
| L7. Aspecte practice ale criptosistemelor cu cheie publica. | problematizarea, exemplificarea |  |
| Bibliografie 1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006.2. R. **Küsters,** Ralf, Th. **Wilke**, Thomas, Moderne Kryptographie - Eine Einführung, [Leitfäden der Informatik](http://www.springer.com/series/12636) , Springer-Vieweg, 2011 |

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

|  |
| --- |
| * Cursul respectă recomandările curiculare IEEE / ACM pentru programele de studii de informatică;
* Cursuri cu conţinut similar sunt predare la majoritatea universităţilor din România care au programe de studii similare;
* Companiile de dezvoltare de software consideră foarte important conţinutul cursului pentru formarea viitorilor dezvoltatori de software
 |

**10. Evaluare**

|  |  |  |  |
| --- | --- | --- | --- |
| Tip activitate | 10.1 Criterii de evaluare | 10.2 metode de evaluare | 10.3 Pondere din nota finală |
| 10.4 Curs | Conceptele predate la curs şi metodologiile de modelare | Examen final | 70% |
|  |  |  |
| 10.5 Seminar/laborator | Modalitatea de aplicare a metodologiilor de modelare pentru rezolvarea unor probleme concrete | 3 miniproiecte de modelareprezenţa/activitatea de la seminar | 30% |
|  |  |  |
| 10.6 Standard minim de performanţă |
| * minim nota 5 la fiecare dintre examene (parţial şi final)
* minim nota 5 la evaluarea miniproiectelor
 |

Data completării Titular de curs Titular de seminar

10.04.2024 Lekt. dr. Thu Hang Bui Lekt. dr. Thu Hang Bui

Data avizării în departament Semnătura directorului de departament Conf. dr. Adrian Sterca