|  |  |
| --- | --- |
| O imagine care conține siglă, simbol, Font, Grafică  Descriere generată automat | MINISTERUL EDUCAŢIEI **UNIVERSITATEA „AUREL VLAICU“ DIN ARAD**310130 Arad, B-dul Revolutiei nr. 77, P.O. BOX 2/158 AR *Tel.: 0040-257- 283010; fax. 0040-257- 280070*  [http://www.uav.ro](http://www.uav-arad.go.ro)*;* e-mail: rectorat@uav.ro |

**Operator de date cu caracter personal nr. 2929**

**SYLLABUS**

1. **Study programme**

|  |  |
| --- | --- |
| 1.1. Higher education institution | **„Aurel Vlaicu” University of Arad** |
| 1.2. Faculty | **of Exact Sciences** |
| 1.3. Department | **Department of Mathematics and Computer Science** |
| 1.4. Field of study | **Mathematics** |
| 1.5. Study level | **2024-2025** |
| 1.6. Ciclul de studii | **Bachelor** |
| 1.7. Study programme / Qualification | **Mathematics-Computer Science** |
| 1.8. Form of education | **Full – Time study** |

1. **Course details**

|  |  |
| --- | --- |
| 2.1. Name of the course | **GlCS6A14 Cryptography and information security** |
| 2.2. Course coordinator | **Bucerzan Dominic, PhD** |
| 2.3. Seminar/laboratory/project coordinator | **Bucerzan Dominic, PhD** |
| 2.4. Study year | **3** |
| 2.5. Semester | **2** |
| 2.6. Evaluation type | **ES** |
| 2.7. Course type | **OP** |

1. **Estimated total time (hours per semester)**

|  |  |
| --- | --- |
| 3.1. Hours per week | **4** |
| 3.2. Lecture hours per week | **2** |
| 3.3. Seminar/laboratory/project hours per week | **2** |
| 3.4. Total hours per curriculum | **56** |
| 3.5. Lecture hours per semester | **28** |
| 3.6. Seminar/laboratory/project hours per semester | **28** |
| Time division [hrs] | |
| 3.4.1. Independent study from textbooks, course support, bibliography and notes | **20** |
| 3.4.2. Additional reading (libraries, specialized electronic platforms and field research) | **20** |
| 3.4.3. Preparing of seminars/laboratories/projects, homework, papers, portfolios and essays | **25** |
| 3.4.4. Tutorial coaching | **0** |
| 3.4.5. Examinations | **4** |
| 3.4.6. Other activities |  |
| 3.7. Total individual study hours | **69** |
| 3.8. Total hours per semester | **125** |
| 3.9. Number of ECTS credits | **5** |

1. **Prerequisites** (if applicable)

|  |  |
| --- | --- |
| 4.1. Curriculum related |  |
| 4.2. Competence related |  |

1. **Conditions** (if applicable)

|  |  |
| --- | --- |
| 5.1. for the lecture | Video projector, Internet connection |
| 5.2. for the seminar |  |
| 5.3. for the laboratory | Video projector, Internet connection, computers |
| 5.4. for the project |  |

1. **Specific educational objectives (competences to be acquired)**

|  |  |
| --- | --- |
| 6.1. Competenţe profesionale | C2. Mathematical processing of data, analysis of phenomena and processes.  C4. Conceiving models for describing phenomena.  C6. Analysing, testing and exploiting information systems. |
| 6.2. Competenţe transversale | CT1. Applying the rules of organized and efficient work, of responsibie attitudes towards teaching-scientific field, to value the own creative potential, while respecting the principles and norms of professional ethics.  CT2. Efficient conduct of team activities.  CT3. Efficient use of information, communication resources and assisted education both in Roumanian and in an internationally widespread language. |

1. **Course outcomes (resulting from the specific educational objectives to be acquired)**

|  |  |
| --- | --- |
| 7.1. General outcomes | The Cryptography and Information Security course lays the foundations for understanding cryptographic solutions applied in the field of information technology in the 21st century |
| 7.2. Specific outcomes | After the course, students must know the main information security methods as well as information encryption methods; the main cryptographic solutions, both symmetric and with public keys, will be studied. |

1. **Outline** (if applicable)

|  |  |  |
| --- | --- | --- |
| 8.1 Lecture Outline | Teaching methods | Remarks |
| 1. Information security in the 21st century Information processes; the impact of the internet in modern society. Methods for ensuring the information security | interactive exposure, problematization, case study |  |
| 2. Cryptography The mathematical foundations of cryptography | interactive exposure, problematization, case study |  |
| 3. Classical cryptography. Modern cryptography. Cryptanalysis | interactive exposure, problematization, case study |  |
| 4. Symmetric cryptographic algorithms | interactive exposure, problematization, case study |  |
| 5. Asymmetric cryptographic algorithms (with public keys) | interactive exposure, problematization, case study |  |
| 6. Digital Signature Algorithms | interactive exposure, problematization, case study |  |
| 7. Legal aspects related to the codification and protection of information | interactive exposure, problematization, case study |  |
| 8.2 Lecture References  1. Bucerzan Dominic, Securitatea informației economice in rețele de calculatoare Teza de doctorat, ASE Bucuresti, 2005  *Securitatea informației economice in rețele de calculatoare*  2. Patriciu Victor-Valeriu, *Criptografia şi securitatea reţelelor de calculatoare*, Ed.Tehnică, 1994  3. Schneier Bruce, *Applied Cryptography*, John Wiley & Sons, Inc. , 1996  4. Tanenbaum S. Andrew, *Computer networks*, Computer Press Agora, 1998  5. http:/www.wikipedia.org  6. http:/www.hackmagedon.com  7. Leliana Valentina Pârvulescu, Igor Vaslav Vitale, *Psihologie aplicată în CyberSecurity*, Brăila :Editura Sfântul Ioan, 2016  8. Hu Xiong, Zhen Qin, Athanasios V. Vasilakos, *Introduction to Certificateless Cryptography*, CRC Press, 2016 | | |

|  |  |  |
| --- | --- | --- |
| 8.3 Seminar Outline | Teaching methods | Remarks |
|  |  |  |
| 8.4 Seminar References | | |
| 8.5 Laboratory Outline | Teaching methods | Remarks |
| 1. Information security in the 21st century Information processes; the impact of the internet in modern society. Methods for ensuring the information security | Case studies will be made |  |
| 2. Cryptography The mathematical foundations of cryptography | Case studies will be made and cryptographic algorithmsimplementation applications will be used |  |
| 3. Classical cryptography. Modern cryptography. Cryptanalysis | Case studies will be made and cryptographic algorithmsimplementation applications will be used |  |
| 4. Symmetric cryptographic algorithms | Case studies will be made and cryptographic algorithmsimplementation applications will be used |  |
| 5. Asymmetric cryptographic algorithms (with public keys) | Case studies will be made and cryptographic algorithmsimplementation applications will be used |  |
| 6. Digital Signature Algorithms | Case studies will be made and cryptographic algorithmsimplementation applications will be used |  |
| 7. Legal aspects related to the codification and protection of information | Case studies will be made and cryptographic algorithmsimplementation applications will be used |  |
| 8.6 Laboratory References  1. Bucerzan Dominic, Securitatea informației economice in rețele de calculatoare Teza de doctorat, ASE Bucuresti, 2005  Securitatea informației economice in rețele de calculatoare  2. Patriciu Victor-Valeriu, Criptografia şi securitatea reţelelor de calculatoare, Ed.Tehnică, 1994  3. Schneier Bruce, Applied Cryptography, John Wiley & Sons, Inc. , 1996  4. Tanenbaum S. Andrew, Reţele de calculatoare, Computer Press Agora, 1998  5. http:/www.wikipedia.org  6. http:/www.hackmagedon.com  7. Leliana Valentina Pârvulescu, Igor Vaslav Vitale, Psihologie aplicată în CyberSecurity, Brăila :Editura Sfântul Ioan, 2016  8. Hu Xiong, Zhen Qin, Athanasios V. Vasilakos, Introduction to Certificateless Cryptography, CRC  Press, 2016 | | |
| 8.7 Project Outline | Teaching methods | Remarks |
| 8.8 Project Outline | | |

1. Correlation of course outline with the expectations of the epistemic community, professional associations and representative employers within the field of the program

The problem of IT security is acute in this period of the development of modern society; IT criminality is a reality of the Internet and electronic commerce. The content of the discipline provides the necessary knowledge so that future specialists can take security measures using cryptographic techniques that are absolutely necessary in any company.

1. **Evaluation / Grading** (if applicable)

|  |  |  |  |
| --- | --- | --- | --- |
| Activity type | Evaluation criteria | Evaluation methods | Percentage of the final grade |
| 10.1. Lecture | Verification of knowledge about the techniques used in cryptography | colloquy | 50% |
| 10.2. Seminar |  |  |  |
| 10.3.Laboratory | Verification of knowledge related to protection methods and cryptographic algorithms | Practical work + project | 50% |
| 10.4. Project |  |  |  |
| 10.5 Minimal performance standard  The student should have general knowledge about cryptography and methods of applying specific algorithms.  The minimum mark for each test must be 5 (five). | | | |

Course coordinator

Bucerzan Dominic PhD

Seminar/laboratory/project coordinator

Bucerzan Dominic PhD

Head of the Department

Lect.univ.dr. Lorena Camelia POPA

Dean

Prof.univ.dr. Sorin-Florin NĂDĂBAN