



DISCIPLINE ACADEMIC SHEET
ACADEMIC YEAR 2025 – 2026

1. PROGRAMME DATA

1.1. Higher Education Institution	UNIVERSITY OF CRAIOVA
1.2. Faculty	Automation, Computers and Electronics
1.3. Department	Computers and Information Technology
1.4. Field of Study	Computers and Information Technology
1.5. Study level	L(License / Undergraduate)
1.6. Organizational form	IF
1.7. Study Program (name/code) /Qualification	Computers / L2060101010

2. DISCIPLINE DATA

2.1 Discipline Name				Data Security			
2.2 Course Activities Holder				Prof. univ. dr. ing. Marius MARIAN			
2.3. Practical Activities Holder				Asist. univ. drd. ing. Claudiu TRĂISTARU			
2.4. Study Year	4	2.5. Semester	1	2.6. Evaluation type	E	2.7. Discipline regime	DOB

3. ESTIMATED TOTAL TIME (hours per semester of teaching activities)

3.1. Number of hours per week	4	in which: 3.2 course	2	3.3. sem./lab./pr.	2
3.4. Total hours of curriculum	56	in which: 3.5 course	28	3.6. sem./lab./pr.	28
3.7. Time distribution - hours/week					hours
Study after manual, course support, bibliography and notes					10
Additional documentation in library, on specialized electronic platforms and field					6
Training seminars / labs, homework, portfolios and essays					10
Tutorial					-
Examinations					14
Other activities.....					4
Total hours per individual activities					44
3.8. Total hours per semester					100
3.9. Number of credits					4

4. PRECONDITIONS (where appropriate)

4.1. of curriculum	The student must possess fundamental and specialized knowledge acquired in the following disciplines: Linear Algebra and Geometry, Special Mathematics, Numerical Methods, Computer Programming, Programming Techniques, Fundamentals of Computer Logic Design, Data Structures and Algorithms, Operating Systems, Data Communications, Computer Structure and Organization, Databases, Object-Oriented Programming, Computer Architecture, Microprocessor
--------------------	--

	Systems Design, Computer Networks, Development of Distributed Network Applications, Verification and Testing of Computing Systems, Software Engineering.
4.2. of competence	The student benefits if they already possess the competences in the list below (but studying the discipline without these competences is not penalizing):

5. CONDITIONS (where appropriate)

5.1. of the course	The course is taught using the computer, the Internet and the video projector. The board is used for more detailed explanations of the concepts illustrated in the course support slides and to answer the questions asked by the students in the room. Students are advised to practice note-taking (in writing, in math-style notebooks). Course support in electronic format and access to up-to-date documentation are provided. The teaching process has the following structure: • 70% theoretical presentation, based on the course support (slides); • 30% interactive activity (practical demonstrations and dialogue with the students). Knowledge transmission and assimilation strategies used: exposition, questioning, deduction, testing, continuous and summative evaluation. NOTE: the course may combine several teaching methods: classic, online (depending on the decision of the University Senate and the Faculty Council), with video projector.
5.2. of seminar/ laboratory/project	Examples are presented and various exercises and problems are solved based on the theoretical notions presented in the course, in the classic way and using specific programming and simulation environments. In the seminar and laboratory, the board is used to exemplify the algorithms and the various programming techniques studied, plus a computer network. These are used together with integrated programming environments to exemplify the concepts presented in the course, as well as to solve the types of problems proposed to students in the laboratory. Students will be exposed to and encouraged to experiment with several commonly used cryptographic techniques and libraries. Students will be involved in practical exercises manipulating the taught cryptographic algorithms and security mechanisms. Notes and course notebooks are mandatory at the course, seminar and laboratory, with the students' approach and practical problem-solving strategy being monitored.

6. COURSE OBJECTIVES – expected learning outcomes that are supported by completing and passing the course

Knowledge	The student/graduate identifies and explains the basic concepts, theories and methods of the data security field.
-----------	---

Skills (Abilities)	The student/graduate selects and applies evaluation criteria, principles and methods for the identification, modeling, simulation and experimentation of phenomena and processes in the data security field.
Responsibility and autonomy	The student/graduate selects and analyzes the bibliographic sources specific to the field. The student/graduate demonstrates learning autonomy on topics specific to the field.

7. CONTENT

7.1. Course	The method of implementation	Teaching methods	Allocated time (hours)
1. Course 1. Introduction to information security • basic notions; classic crypto-systems; threats, attacks and critical information; functional security requirements; information security strategies.		The course is taught using the video projector. The practical exemplification of the presented concepts and problem solving is done directly in the visual presentation/programming environment etc. The course is structured in the ratio below: 1. 80% theoretical presentation, based on the course support (slides); 2. 20% interactive activity (dialogue with the students). The necessary materials will be made available to students in electronic and printed format. The knowledge transmission and assimilation strategies used are: Exposition; Questioning; Deduction; Testing; Final evaluation.	2
2. Course 2. Cryptographic tools • symmetric encryption; public-key encryption; digital signature and key management; pseudo-random number generation.			2
3. Course 3. User authentication mechanisms • authentication principles; password-based authentication; token-based authentication; biometric authentication.			2
4. Course 4. Access control mechanisms • access control principles; subjects, objects and access rights; discretionary control; role-based control.			2
5. Course 5. Database security • access control to a database; inference; statistical databases; database encryption			2
6. Course 6. Intrusion			2

detection • identifying intruders; intrusion detection in individual computing systems; intrusion detection in distributed computing systems; intrusion detection in computer networks; adaptive intrusion detection in distributed systems; honeypot or honeynet lure mechanisms			
7. Course 7. Malicious software • types of malicious software; computer viruses; countermeasures against computer viruses; computer worms; bots; rootkits			2
8. Course 8. Denial of service • denial of service (DoS) attacks; flooding attacks; distributed denial of service attacks; reflector and amplifier attacks; possible countermeasures to DoS attacks			2
9. Course 9. Firewall and intrusion prevention systems • the need for firewalls; types of firewalls; network architectures and firewall placement; intrusion prevention systems			2
10. Course 10. Multi-level security; trust models • the Bell-LaPadula model; other formal models of system security; the concept of a trusted system; applying multi-level security; the common criteria for IT security evaluation			2
11. Course 11. Buffer overflow • stack overflow attacks; protection countermeasures; other overflow attacks; writing security-safe code			2
12. Course 12. Physical and infrastructure security matters • threats against the physical security of systems; prevention and			2

countermeasures to physical attacks on systems; system recovery after a physical attack; threat identification; planning and implementing countermeasures; integrating physical system security with logical security			
13. Course 13. IT security management and risk identification • IT security management; the organizational context and security policies; identifying risks to system security; risk analysis			2
14. Course 14. Legal and ethical aspects • digital forensics; intellectual property; confidentiality and privacy; ethical matters			2
Bibliography:			
1. W. Stallings, L. Brown, "Computer Security: Principles and Practice", Prentice-Hall, 2008, ISBN-13: 9780136004240 2. W. Stallings, "Network Security Essentials: Applications and Standards", Prentice-Hall, 2007, ISBN-13: 9780132380331 3. B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", Wiley, 1996, ISBN- 13: 978-0471117094			

7.2. Seminar/laboratory/project	The method of implementation	Teaching methods	Allocated time (hours)
Lab 1: introduction to using the OpenSSL cryptographic library		Examples are presented and various exercises and problems are solved based on the theoretical notions presented in the course. The student is encouraged to take on responsibilities in analyzing the problem and finding its algorithmic/software solution.	2
Lab 2: using symmetric cryptography (DES, 3DES, AES)			2
Lab 3: using asymmetric cryptography (RSA)			2
Lab 4: using the digital signature			2
Lab 5: familiarization with digest algorithms and digital signature algorithms (MD5, SHA1, DSA, DH)			2
Lab 6: implementing and using an application based on access control lists (ACL)			2
Lab 7: implementing a			2

client-server architecture secured on the communication side			
Lab 8: installing, configuring and getting familiar with the SNORT utility (intrusion detection system)			2
Lab 9: exemplification of computer viruses and the use of anti-virus software			2
Lab 10: installing, configuring and getting familiar with a firewall utility			2
Lab 11: installing, configuring and getting familiar with an IDS/IPS utility			2
Lab 12: applications vulnerable to buffer overflow attacks			2
Lab 13: familiarization with a public key infrastructure (digital certificates, certification authorities, registration authorities)			2
Lab 14: familiarization with the services of a public key infrastructure (PKI)			2
Bibliography:			
1. W. Stallings, L. Brown, "Computer Security: Principles and Practice", Prentice-Hall, 2008, ISBN-13: 9780136004240 2. W. Stallings, "Network Security Essentials: Applications and Standards", Prentice-Hall, 2007, ISBN-13: 9780132380331 3. B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", Wiley, 1996, ISBN- 13: 978-0471117094			

8. Correlating the content of the discipline with the expectations of representatives from the epistemic community, professional associations and representative employers in the field related to the program

The course content was discussed with the representatives of: ▪ C-S România SA ▪ Forvia-Hella Craiova ▪ Netrom Software Craiova

9. EVALUATION

Activity Type	9.1. Evaluation criteria	9.2. Evaluation methods	9.3. Final mark weight
9.4. Course			

9.5. Seminar/laboratory/project			
9.6. Minimum standard of performance			

Date of Completion	Signature of the Course Activities Holder,	Signature of the Practical Activities Holder,
23.08.2025	Prof. univ. dr. ing. Marius MARIAN	Asist. univ. drd. ing. Claudiu TRĂISTARU

Date of Approval in the Department	Signature of the Department Director,
25.08.2025	Ș.l.dr.ing. Nicolae ENESCU

Date of Approval in the Faculty	Signature of the Dean,
	Prof.dr.ing. Dorin ȘENDRESCU