SYLLABUS

1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master
1.6 Program of study / Qualification	Cybersecurity Engineering / Master
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	***Applied Cryptography***			Subject code	**14.00**
2.2 Course responsible / lecturer	Prof. dr. eng. Alin SUCIU - asuciu@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Prof. dr. eng. Alin SUCIU - asuciu@cs.utcluj.ro				
2.4 Year of study	II	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DA
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DI

3. Estimated total time

3.1 Number of hours per week	4	of which:	Course	2	Seminars	2	Laboratory	0	Project	0
3.2 Number of hours per semester	56	of which:	Course	28	Seminars	28	Laboratory	0	Project	0
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										24
(b) Supplementary study in the library, online and in the field										10
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										32
(d) Tutoring										0
(e) Exams and tests										2
(f) Other activities:										0

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	68
3.5 Total hours per semester (3.2+3.4)	124
3.6 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1 Curriculum	N/A
4.2 Competence	C Programming

5. Requirements (where appropriate)

5.1. For the course	blackboard, beamer, computers
5.2. For the applications	blackboard, beamer, computers

6. Specific competence

6.1 Professional competences	The graduate is capable to: • perform risk analysis • educate on data confidentiality • provide ICT consulting advice • perform data analysis • ensure information privacy • monitor developments in field of expertise • keep up with the latest information systems solutions
6.2 Cross competences	The graduate is capable to: • develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open minded

7. Expected Learning Outcomes

Knowledge	The student has knowledge of: • ICT encryption • cyber security • information confidentiality
Skills	The student is able to: • analyse ICT systems • interpret technical texts • use software libraries • address problems critically • protect personal data and privacy • manage digital identity • manage keys for data protection • use an application-specific interface
Responsibilities and autonomy	The student has the ability to work independently in order to: • develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded

8. Discipline objectives (as results from the *key competences gained*)

8.1 General objective	Becoming familiar with the fundamentals of cryptography, with the use and application of the most popular and most representative cryptographic primitives, and their applications in the current systems. Acquiring the capability to apply and use the various methods and techniques of cryptography and assessing their value in the field of information security.
8.2 Specific objectives	1. Understanding the existing cryptographic primitives and methods 2. Understanding and being able to assess the security of cryptographic primitives 3. Becoming able to integrate cryptographic primitives in one's own security applications 4. Becoming able to analyse and determine the needs of a software project from a cryptographic perspective.

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
Introduction, short history and fundamentals of cryptography	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	
Fundamental ciphers: transposition, monoalphabetic substitution	2		
Fundamental ciphers: polyalphabetic substitution	2		
Fundamental ciphers: polygramic substitution, Playfair cipher and Hill cipher	2		
One Time Pad, Random number generators (TRNG, PRNG)	2		
Stream Ciphers	2		
Block ciphers – DES cipher	2		
Block ciphers – AES cipher	2		
Block ciphers – modes of operation (ECB, CBC, OFB, CFB, etc.)	2		
Public key cryptography – principles, mathematical foundations	2		
Public key cryptography – RSA cipher	2		
Digital Signatures, Cryptographic hash functions	2		
Message Authentication Codes (MAC)	2		
Key management, Digital Certificates	2		

Bibliography:

- Understanding Cryptography: A Textbook for Students and Practitioners, (Paar, Pelzl -2010, Springer-Verlag New York Inc .)
- Cryptography Engineering: Design Principles and Practical Applications (Ferguson, Niels - 2010- Willey)
- Cryptography and Network Security. Principles and Practice (Stallings, William - 2013 - Prentice Hall)
- Cryptography: A Very Short Introduction (Piper, Fred - 2002 - Oxford University Press)

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
		Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	

Bibliography

- Understanding Cryptography: A Textbook for Students and Practitioners, (Paar, Pelzl -2010, Springer-Verlag New York Inc .)
- Cryptography Engineering: Design Principles and Practical Applications (Ferguson, Niels - 2010- Willey)
- Cryptography and Network Security. Principles and Practice (Stallings, William - 2013 - Prentice Hall)
- Cryptography: A Very Short Introduction (Piper, Fred - 2002 - Oxford University Press)

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

Cryptography courses are a must in the majority of master programs that are focusing on information and computer security; here are some examples:

- CSci 6331 Cryptography – The George Washington University – Washington DC, USA – Master of Science in Cybersecurity
- Cryptography (252-0407-00) – ETH Zurich – Switzerland – Information Security Master
- Computational Cryptography – Technical Military Academy – Bucharest – Master of IT Security

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade

Course	Ability to define concepts and methods specific to applied cryptography field. Capability to give correct and functional solutions to problems specific to applied cryptography. Attendance frequency, interest, and interactivity during lecture classes.	Written exam, testing both the theoretical understanding of the topics and practical problem solving. (*Summative assessment*) In exceptional cases, the exam could be given/taken online remotely, using the MS Teams platform.	70%
Seminar	Capability and ability to give correct and functional solutions to problems specific to applied cryptography. Attendance frequency, interest, and interactivity during seminar classes.	Submit correct solutions and/or explanations to weekly problems discussed during the corresponding seminar, using the MS Teams platform. (*Continuous assessment*)	30%
Laboratory	-	-	-
Project	-	-	-
Minimum standard of performance: **Lectures**. Students must attend a minimum of 50% of lecture classes, to be allowed to take the final examination. Students must be able to define and describe fundamental concepts and algorithms specific to applied cryptography. The final exam grade must be >= 5 to pass the exam. **Seminars**. Students must submit a minimum of 50% of proposed seminar problems. Students must be able to explain and apply fundamental cryptographic algorithms. The seminar grade must be >= 5 to participate in the final exam.			

Date of filling in: 01.09.2025	**Responsible**	**Title First name Last name**	**Signature**
	Course	Prof. dr. eng. Alin SUCIU	
	Applications	Prof. dr. eng. Alin SUCIU	

Date of approval in the department 17.09.2025	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council 19.09.2025	Dean, Prof.dr.eng. Vlad Mureșan