



COURSE SYLLABUS APPLIED CRYPTOGRAPHY

1. Program identification details

1.1 Higher education institution	"OVIDIUS" UNIVERSITY OF CONSTANȚA
1.2 Faculty	Faculty Mathematics and Computer Science
1.3 Department	Mathematics and Computer Science
1.4 Field of study	Computer Science
1.5 Degree	Master
1.6 Programme of study	Cyber Security and Machine Learning
1.7 Academic year	2025-2026

2. Course identification details

2.1 Course title	APPLIED CRYPTOGRAPHY						
2.2 Course code	FMI.CSML.II.1.01						
2.3 Lecture instructor	Prof. Răcuciu Ciprian, Ph.D.						
2.4 Seminar instructor	Prof. Răcuciu Ciprian, Ph.D.						
2.5 Year	2	2.6 Semester	1	2.7. Evaluation type	E	2.8 Course type */**	SC/MC

* FC – fundamental course, SC – specialty course, CC – complementary course

**MC – mandatory course; OC – optional course; EC – elective course

3. Estimated workload (hours per semester)

3.1 Number of teaching hours/week	4	of which: 3.2 lecture	2	3.3 applications***	2
3.4 Number of teaching hours/semester	56	of which: 3.5 lecture	28	3.6 applications	28
3.7 Individual study workload					144
Workload distribution					[hours]
Reading (books, coursebooks, course reader, lecture notes, course bibliography)					45
Additional library / specialised platform research and fieldwork					40
Seminar / lab / project preparation, home assignments, research papers, portfolios and essays					45
Presentation or test preparation					10
Final examination preparation					10
Other activities: tutorials					4
3.8 Total hours/semester	56 + 144				
3.9 Number of credits	8				

*** S - seminar; L - lab; P - project

4. Prerequisites (where applicable)

4.1 curriculum-related	Undergraduate studies
4.2 skills-related	Computer Programming

5. Necessary requirements for optimum teaching and learning (where applicable)



OUC-PO-10 Annex 3a

5.1. for running the lecture	Classroom available
5.2. for running the seminar/ lab / project*	Laboratory room available with computers

**Type of application to be chosen according to the nature of the course*

6. Course objectives

6.1 The general objective of the course	Identificarea problemelor cheie legate de gestionarea securității informațiilor și conștientizarea faptului că criptografia este doar o parte a securității informațiilor.
6.2 Specific objectives	Dezvoltarea instrumentelor necesare pentru implementarea unui proces specific de gestionare a cheilor criptografice .

7. Learning outcomes

Knowledge	Dobândirea cunoștințelor de bază legate de modelarea, proiectarea și utilizarea tehnicilor criptografice.
Skills	Identificarea conceptelor și modelelor de bază pentru diferite tipuri de sisteme criptografice în raport cu cerințele de securitate. Identificarea, explicarea și utilizarea tehnicilor criptografice avansate.
Responsibility and autonomy	Executarea de sarcini profesionale complexe, în condiții de autonomie și independență profesională, implicând detectarea și rezolvarea problemelor legate de utilizarea tehnicilor criptografice avansate. Utilizarea eficientă a surselor de informații și a resurselor de comunicare, precum și dezvoltarea muncii în echipă, în cazul proiectării, administrării și utilizării diferitelor tipuri de criptosisteme în raport cu cerințele de securitate.

8. Contents

8.1 Lecture	Teaching methods	No. of hours
1. Securitatea informațiilor - principii de bază, riscuri, servicii, istoric. Bazele sistemelor criptografice, ipotezele de securitate pentru acestea și spargerea sistemelor criptografice.	Dialog Problematizare	4
2. Tehnici criptografice simetrice - clasificare, cifruri secvențiale, cifruri bloc, cifruri DES, 3DES, AES; alte tehnici de criptare simetrică și viitorul acestora; aplicații.	Metode active și interactive Interacțiune, problematizare, argumentare	4
3. Tehnici criptografice asimetrice – clasificare, caracteristici și analiză comparativă: metoda RSA, metoda ElGamal, criptografie bazată pe curbe eliptice (ECC); alte tehnici de criptare asimetrică și viitorul acestora; aplicații.	Sintetizarea/esențializarea informațiilor	4



OUC-PO-10 Annex 3a

4. Integritatea datelor și autentificarea entităților 4.1. Integritatea datelor – clasificarea caracteristicilor și analiza comparativă: funcții hash, coduri de autentificare a mesajelor (MAC); aplicații. 4.2. Autentificarea entităților; Scheme de semnătură digitală: caracteristici, RSA, ElGamal, curbe eliptice; aplicații.	Învățare independentă și în echipă	4
5. Protocoale criptografice: AKE (protocoale de autentificare și stabilire a cheilor), gestionarea cheilor simetrice și asimetrice (generare, stabilire, stocare, utilizare), modele bazate pe autorități de certificare.		4
6. Aplicații criptografice - securitatea rețelelor Internet, LAN și WLAN, a rețelelor de telecomunicații mobile, a plăților electronice, a monedelor digitale, a dispozitivelor personale.		4

Bibliography

- [1]. J. P. Aumasson, Serious cryptography: a practical introduction to modern encryption. No Starch Press, 2017.
- [2]. Patriciu, V.V., Pietroșanu, M., Bica, I. and Priescu, J., 2006. Semnături electronice și securitate informatică. Editura All, București.
- [3]. E. Petac, Course Support
- [4]. E. Petac, D. Petac, Principles and Techniques for Information Security in Computer Networks/ Metode si tehnici de protectie a informatiei in retelele de calculatoare, Ed. MatrixRom, Bucuresti, 1998.
- [5]. S. Rubinstei-Salzedo, Cryptography. Cham, Switzerland: Springer, 2018.
- [6]. J. Katz, L. Yehuda, Introduction to modern cryptography. Chapman and Hall/CRC, 2014.

8.2 Applications (seminar/lab/project)*

** Type of application to be chosen according to the nature of the course*

	Teaching methods	No. of hours
1. Fundamentele sistemelor criptografice, ipotezele de securitate pentru acestea și evaluarea sistemelor criptografice. Aplicații.	Dialog	4
2. Tehnici criptografice simetrice - cifruri secvențiale, cifruri bloc, cifruri DES, 3DES, AES; alte tehnici de criptare simetrică. Aplicații.	Problematizare	4
3. Tehnici criptografice asimetrice – clasificare, caracteristici și analiză comparativă: metoda RSA, metoda ElGamal, criptografie bazată pe curbe eliptice (ECC); alte tehnici de criptare asimetrică. Aplicații.	Metode active și interactive	4
4. Integritatea datelor: funcții hash, coduri de autentificare a mesajelor (MAC). Autentificarea entităților; Scheme de semnătură digitală. Aplicații.	Interacțiune, problematizare, argumentare	4
5. Protocoale criptografice: AKE (protocoale de autentificare și stabilire a cheilor), gestionarea cheilor simetrice și asimetrice (generare, stabilire, stocare, utilizare), modele bazate pe autorități de certificare.	Sintetizarea/esențializarea informațiilor	4
	Învățare independentă și în echipă	4



6. Aplicații criptografice - securitatea rețelelor Internet, LAN și WLAN, a rețelelor de telecomunicații mobile, a plăților electronice, a monedelor digitale, a dispozitivelor personale.		8
--	--	---

Bibliography:

- [1]. J. P. Aumasson, Serious cryptography: a practical introduction to modern encryption. No Starch Press, 2017.
- [2]. Patriciu, V.V., Pietroșanu, M., Bica, I. and Priescu, J., 2006. Electronic signatures and computer security/Semnături electronice și securitate informatică. Editura All, București.
- [3]. E. Petac, Course Support.
- [4]. E. Petac, D. Petac, Principles and Techniques for Information Security in Computer Networks/ Metode si tehnici de protectie a informatiei in retelele de calculatoare, Ed. MatrixRom, Bucuresti, 1998.
- [5]. S. Rubinstein-Salzedo, Cryptography. Cham, Switzerland: Springer, 2018.
- [6]. J. Katz, L. Yehuda, Introduction to modern cryptography. Chapman and Hall/CRC, 2014.
- [7]. Java Tutorial, <https://docs.oracle.com/javase/tutorial/>
- [8]. Python tutorial, <https://docs.python.org/3.7/tutorial/>

9. Evaluation

Type of activity	9.1 Evaluation criteria	9.2 Evaluation methods	9.3 Percentage of final grade
9.4 Lecture	Participarea activă la activitățile didactice	Examen scris Curs și laborator	30%
		Proiect	50%
9.5 Applications* <i>*Type of application to be chosen according to the nature of the course</i>	Disponibilitatea și capacitatea de a lucra individual și în echipă	Prezentarea unei lucrări de cercetare (aplicarea unei metode analitice avansate - studiu de caz)	20%

9.6 Minimum standard of achievement / Pass requirements

Realizarea și prezentarea unui proiect pe o temă specializată în domeniul tehnicilor criptografice avansate, în contextul programei cursului.

Date of
completion,
18.09.2025

Lecture instructor,
Prof. Răcuciu Ciprian, Ph.D

Application instructor,
Prof. Răcuciu Ciprian, Ph.D

Date of approval at Department level,
24.09.2025

Head of Department,
Assoc. Prof. Pelican Elena, PhD

Dean,
Assoc. Prof. Nicola Aurelian, PhD