



COURSE SYLLABUS CRYPTOGRAPHY ADVANCED TECHNIQUES

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	Cryptography Advanced Techniques						
2.2 Course code	CSML.1.2.15						
2.3 Lecture instructor	Prof. Răcuciu Ciprian, Ph.D.						
2.4 Seminar instructor	Prof. Răcuciu Ciprian, Ph.D.						
2.5 Year	I	2.6 Semester	2	2.7 Evaluation	C	2.8 Course type	SC/OC

* 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	2	of which: 3.2 lecture	1	3.3 applications***	1
3.4 Number of teaching hours/semester	28	of which: 3.5 lecture	14	3.6 applications	14
3.7 Individual study workload					97
Workload distribution					[hours]
Reading (books, coursebooks, course reader, lecture notes, course bibliography)					42
Additional library / specialised platform research and fieldwork					14
Seminar / lab / project preparation, home assignments, research papers, portfolios and essays					25
Presentation or test preparation					8
Final examination preparation					8
Other activities: tutorials					0
3.8 Total hours/semester	28 + 97 = 125				
3.9 Number of credits	5				

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

4. Prerequisites (where applicable)

4.1 curriculum-related	
4.2 skills-related	



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

5.1. for running the lecture	Lecture Room / Lecture Hall
5.2. for running the seminar/ lab / project*	Computer Laboratory

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

6. Course objectives

6.1 The general objective of the course	Prezentarea principalelor tipuri de sisteme criptografice și a noilor tendințe în criptografie.
6.2 Specific objectives	Formarea și dezvoltarea competențelor în materie de alegere a sistemelor criptografice și de analiză a securității

7. Learning outcomes

Knowledge	Cunoașterea conceptelor de bază ale criptografiei și securității cibernetice Cunoașterea principalelor sisteme criptografice actuale
Skills	Capacitatea de a analiza sistemele criptografice Capacitatea de a dezvolta strategii de securitate a informațiilor pentru a maximiza integritatea, disponibilitatea și confidențialitatea datelor.
Responsibility and autonomy	Capacitatea de a utiliza în mod eficient resursele de documentare și comunicare. Capacitatea de a redacta și prezenta proiecte atât individual, cât și în echipă. Capacitatea de a efectua analize de date, de a colecta date și statistici pentru testare și evaluare, în vederea generării de situații și previziuni de modele, pentru a descoperi informații utile în procesul decizional.

8. Contents

8.1 Lecture	Teaching methods	No. of hours
Bazele matematice: clase de complexitate, probabilitate, aritmetică modulară, câmpuri finite, reziduuri cuadractice, testarea primalității.	Metode interactive de predare-învățare	1
Introducere în criptografie: sisteme criptografice simple, cifruri bloc.	Problematizare Metode active și interactive	2
DES (Data Encryption Standard): algoritmi DES și DES interativ	Metode care contribuie la dezvoltarea gândirii critice	1
Criptare cu cheie publică: RSA, ElGamal, Rabin, criptare probabilistică cu cheie publică	Dialog Sintetizarea/esențializarea informațiilor	2
Semnătura digitală: sistemul de semnătură digitală RSA, sistemul ElGamal, sistemul Rabin, semnături probabilistice	Învățare independentă și cooperativă Generalizare	2
Criptografia bazată pe curbe eliptice: grupul de puncte ale unei curbe eliptice, curbe eliptice peste câmpuri finite, scheme de semnătură	Conversație Argumentare	3



Criptografia bazată pe structuri algebrice finite: probleme și algoritmi, scheme de criptare cu cheie publică bazate pe structuri algebrice finite		3
Bibliography: [1]. S. Goldwasser, M. Bellare, Lecture Notes on Cryptography, 2008, available at https://cseweb.ucsd.edu/~mihir/papers/gb.pdf [2]. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Universității din București, 2005. [3]. D. Boneh, V. Soup, A Graduate Course in Applied Cryptography, 2023, version 0.6, available at https://toc.cryptobook.us/book.pdf [4]. J. Katz, Y. Lindell, Introduction to Modern Cryptography, Chapman &Hall/CRC Press, 2008. [5]. N. Smart, Cryptography: An introduction, available at: https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf [6]. C. Paar, J. Pelzl, Understanding Cryptography. A Textbook for students and Practitioners, Springer 2010. [7]. C.Peickert, A Decade of Lattice Cryptography, Foundations and Trends in Theoretical Computer Science: Vol. 10: No. 4, pp. 283-424, available at: https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf		
8.2 Applications (seminar/lab/project)* <i>* Type of application to be chosen according to the nature of the course</i>	Teaching methods	No. of hours
Bazele matematice	Teme individuale și de echipă Rapoarte	1
Introducere în criptografie		2
DES (Data Encryption Standard)		2
Criptare cu cheie publică		2
Semnătura digitală		2
Criptografia bazată pe curbe eliptice		3
Criptografia bazată pe structuri algebrice finite		2
Bibliography: 1. S. Goldwasser, M. Bellare, Lecture Notes on Cryptography, 2008, available at https://cseweb.ucsd.edu/~mihir/papers/gb.pdf 2. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Universității din București, 2005. 3. D. Boneh, V. Soup, A Graduate Course in Applied Cryptography, 2023, version 0.6, available at https://toc.cryptobook.us/book.pdf 4. J. Katz, Y. Lindell, Introduction to Modern Cryptography, Chapman &Hall/CRC Press, 2008. 5. N. Smart, Cryptography: An introduction, available at: https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf 6. C. Paar, J. Pelzl, Understanding Cryptography. A Textbook for students and Practitioners, Springer 2010. 7. C.Peickert, A Decade of Lattice Cryptography, Foundations and Trends in Theoretical Computer Science: Vol. 10: No. 4, pp. 283-424, available at: https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf		

9. Evaluation

Type of activity	9.1 Evaluation criteria	9.2 Evaluation methods	9.3 Percentage of final grade
9.4 Lecture	Capacitatea de a analiza un sistem criptografic	Examinare	60%



OUC-PO-10 Annex 3a

9.5 Applications* <i>*Type of application to be chosen according to the nature of the course</i>	Capacitatea de a aplica rezultatele teoretice în situații concrete	Proiect	20%
	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			
Cunoașterea a cel puțin două sisteme de criptare prezentate în curs și analiza securității acestora.			

Date of
completion,
18.09.2025

Lecture instructor,
Prof. Racuciu Ciprian, Ph. D.

Application instructor,
Prof. Racuciu 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