FIŞA DISCIPLINEI
Elemente de Criptografie

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea "Ovidius" din Constanta
1.2 Scoala doctorala	Matematica
1.3 Domeniul	Matematica
1.4 Ciclul de studii	Doctorat, anul I
1.5 Anul universitar	**2022-2023**

2. Date despre disciplină

2.1 Denumirea disciplinei			**Elemente de Criptografie**					
2.2 Cod disciplină			SDM83					
2.3 Titularul activităţilor de curs			Prof. univ. dr. Cristina FLAUT					
2.4 Titularul activităţilor aplicative			Prof. univ. dr. Cristina FLAUT					
2.5 Anul de studii	**I**	2.6 Semestrul	**II**	2.7 Tipul de evaluare	**E**	2.8 Regimul disciplinei		**DS/DO**

** DF – disciplină fundamentală, DD – disciplină în domeniu, DS – disciplină de specialitate, DC – disciplină complementară, DAP – disciplină de aprofundare, DSI – disciplină de sinteză, DCA – disciplină de cunoaştere avansată*
*** DI – disciplină impusă; DO – disciplină opţională*

3. Timpul total estimat (ore pe semestru alocate disciplinei)

3.1 Număr de ore activităţi directe pe săptămână	**2**	din care: 3.2 curs	**2**	3.3 aplicaţii***	**0**
3.4 Total ore activităţi directe pe semestru	**24**	din care: 3.5 curs	**24**	3.6 aplicaţii	**0**
3.7 Total ore de studiu individual					**126**
Distribuţia fondului de timp					*[ore]*
Studiul după manual, suport de curs, bibliografie şi notiţe					60
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					30
Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri					20
Tutorial					10
Examinări					6
Alte activităţi					-
3.8 Total ore pe semestru	*150*				
3.9 Numărul de credite	**6**				

**** S - seminar; L - laborator; P - proiect*

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	-
4.2 de competenţe	-

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Sala cu videoproiector, Sala de curs disponibila, platforma online webex
5.2. de desfăşurare a laboratorului /proiectului	-

6. Competenţele specifice acumulate

Competenţe profesionale	Cunoasterea tehnicilor si modelelor de baza utilizate in studiul matematicii, Utilizarea instrumentelor specifice matematicii in context interdisciplinar.

Competențe transversale	Utilizarea modelelor si instrumentelor matematice pentru rezolvarea problemelor specifice. Utilizarea adecvata a softurilor specifice.

Rezultatele învățării

Cunoștințe

Rî1 - Știe să definească termeni şi concepte referitoare la

Rî2 - Utilizează principii şi metode avansate pentru explicarea şi interpretarea, din perspective multiple, a unor situaţii/probleme teoretice şi practice noi şi complexe, specifice domeniului

Aptitudini

Rî3 - Poate să prelucreze creator informaţia achiziţionată şi să-şi prezinte rezultatele studiului într-o formă corectă şi convingătoare, prin proiecte eligibile.

Responsabilitate și autonomie

Rî4 - Are o atitudine etică și responabilă în utilizarea domeniului

Rî5 - Dezvoltă proiecte centrate pe creativitate, ca temei al autorealizării

7. Obiectivele disciplinei (din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Sa se familiarizeze cu unele tehnici de criptare.
7.2 Obiectivele specifice	Insuşirea de către doctoranzi a principalelelor rezultate referitoare la anumite tehnici de criptare si aplicarea lor.

8. Conţinuturi

8.1 Curs	**Metode de predare**	**Număr ore alocate**
1. Tipuri de criptosisteme simetrice-I	Prelegerea Explicația Conversația Problematizarea Lectura	2
2. Tipuri de criptosisteme simetrice-II		2
3. Tipuri de criptosisteme simetrice-III		2
4. Tipuri de criptosisteme simetrice-IV		2
5. Tipuri de criptosisteme cu cheie publica-I		2
6. Tipuri de criptosisteme cu cheie publica-II		2
7. Tipuri de criptosisteme cu cheie publica-III		2
8. Tipuri de criptosisteme cu cheie publica-IV		2
9. Algoritmi de factorizare si primalitate (Miller-Rabin, Metoda *p-1* a lui Pollard, Metoda ‚rho', Lenstra, Number Field Sieve)-I		2
10. Algoritmi de factorizare si primalitate (Miller-Rabin, Metoda *p-1* a lui Pollard, Metoda ‚rho', Lenstra, Number Field Sieve)-II		2
11. Algoritmi de factorizare si primalitate (Miller-Rabin, Metoda *p-1* a lui Pollard, Metoda ‚rho', Lenstra, Number Field Sieve)-III		2
12. Algoritmi de factorizare si primalitate (Miller-Rabin, Metoda *p-1* a lui Pollard, Metoda ‚rho', Lenstra, Number Field Sieve)-IV		2

Bibliografie obligatorie

[1] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, New-York, 1994.

[2] I. Shparlinski, *Computational and Algorithmic Problems in Finite Field*, Kluver Academic Publishers, Dordrecht,1992.

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Stabilirea de corelaţii între problematica discutată şi realităţile cotidiene, dezvoltarea de abilităţi şi deprinderi necesare actualilor absolvenţi - viitorilor angajaţi în câmpul muncii.
- Cursul ajută absolvenţii să devină: bine pregatiti pentru a face fata cerintelor pietei dar si exigentelor unor programe de cercetare.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs		examen	100 %
Standard minim de performanţă: cifrul Vigener, Crisptosistemul RSA.			
Studenţii trebuie să cunoască înţelesul anumitor concepte, precum: criptosisteme simple, criptosteme cu chei publice, etc. Studenţii trebuie să demonstreze că au inţeles legăturile dintre concepte şi textele studiate, să aplice un metalimbaj adecvat. Se impune parcurgerea “bibliografiei obligatorii.”			

Data completării, Titular activități de curs,

20.09.2022 Director Scoala doctorala
Data avizarii CSD,

25.09.2022