FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea “Alexandru Ioan Cuza” din Iaşi**
1.2 Facultatea	**Facultatea de Matematică**
1.3 Departamentul	**Matematică**
1.4 Domeniul de studii	**Matematică**
1.5 Ciclul de studii	**Licenţă**
1.6 Programul de studii / Calificarea	**Matematică**

2. Date despre disciplină

2.1 Denumirea disciplinei			**Criptografie**				
2.2 Titularul activităţilor de curs			**Prof. dr. Răzvan Liţcanu**				
2.3 Titularul activităţilor de seminar			**Asist. dr. A. Cuzub**				
2.4 An de studiu	**II**	**2.5** Semestru	**IV**	**2.6** Tip de evaluare	**EVP**	**2.7** Regimul discipinei*	**Op**

** OB – Obligatoriu / OP – Opţional*

3. Timpul total estimat (ore pe semestru şi activităţi didactice)

3.1 Număr de ore pe săptămână	**4**	din care: **3.2** curs	**2**	**3.3** seminar/laborator		**2**
3.4 Total ore din planul de învăţământ	**56**	din care: **3.5** curs	**28**	**3.6** seminar/laborator		**28**
Distribuţia fondului de timp						Ore
Studiu după manual, suport de curs, bibliografie şi altele						**10**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren						**10**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri						**20**
Tutoriat						
Examinări						**4**
Alte activităţi						

3.7 Total ore studiu individual	**40**
3.8 Total ore pe semestru	**100**
3.9 Număr de credite	**4**

4. Precondiţii (dacă este cazul)

4.1 De curriculum	Aritmetică, Algebră liniară, Algoritmică şi programare. Limbajul C++
4.2 De competenţe	Operarea cu noţiuni de bază de aritmetică şi algebră liniară. Implementarea unor algoritmi simpli în limbajul C++.

5. Condiţii (dacă este cazul)

5.1 De desfăşurare a cursului	Amfiteatru, calculator, proiector
5.2 De desfăşurare a seminarului/ laboratorului	Sală de seminar / laborator de informatică

6. Competenţe specifice acumulate

Competenţe profesionale	C2. Prelucrarea matematica a datelor, analiza si interpretarea unor fenomene si procese (1 credit) • Interpretarea rezultatelor prelucrării datelor prin sisteme de criptare • Analiza comparativă a rezultatelor obţinute prin utilizarea diverselor sisteme de criptare C3. Elaborarea si analiza unor algoritmi pentru rezolvarea problemelor (1 credit) • Identificarea notiunilor de baza folosite în constructia si specificarea algoritmilor de criptare a informaţiei şi a altor protocoale criptografice • Explicarea etapelor care intervin în algoritmii criptografici • Aplicarea tehnicilor si metodelor specifice pentru proiectarea algoritmilor • Stabilirea comparativă a avantajelor şi limitelor algoritmilor studiaţi C4. Conceperea modelelor matematice pentru descrierea unor fenomene (1 credit) • Explicarea si interpretarea noţiunilor matematice folosite pentru modelarea metodelor de criptare a informaţiei
Competenţe transversale	CT1. Aplicarea regulilor de munca riguroasa si eficienta, manifestarea unor atitudini responsabile fata de domeniul stiintific si didactic, pentru valorificarea optima si creativa a propriului potential în situatii specifice, cu respectarea principiilor si a normelor de etica profesionala (1 credit) • Realizarea si expunerea unui proiect pe o temă dată, riguros si inteligibil

7. Obiectivele disciplinei (din grila competenţelor specifice acumulate)

7.1 Obiectivul general	1. Insuşirea de către studenţi a noţiunilor, conceptelor şi exemplelor fundamentale din criptografie şi securitatea datelor 2. Familiarizarea studenţilor cu tehnici de bază din criptografie şi criptanaliză 3. Construcţia şi analiza unor algoritmi criptografici de bază
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să : • Explice funcţionarea principalilor algoritmi criptografici • Utilizeze noţiuni şi rezultate de bază din aritmetică • Analizeze metode de securizare a informaţiei • Calculeze cheile, mesajele în clar şi mesajele criptate în cadrul pri ncipalelor criptosisteme studiate • Compare principalele metode de criptare sau de semnătură digitală

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1	Preliminarii. Repere istorice	Expunerea, conversaţia, demonstraţia, problematizarea	2 ore
2	Elemente de aritmetică (recapitulare)	Expunerea, conversaţia, demonstraţia, problematizarea	2 ore
3	Teste de primalitate. Algoritmi de factorizare	Expunerea, conversaţia, demonstraţia, problematizarea	2 ore
4	Criptosisteme simetrice	Expunerea, conversaţia, demonstraţia, problematizarea	4 ore
5	Criptosisteme cu cheie publică. RSA	Expunerea, conversaţia, demonstraţia, problematizarea	6 ore

6	Funcţii hash. Semnătura digitală		4 ore
7	Protocoale criptografice.	Expunerea, conversaţia, demonstraţia, problematizarea	4 ore
8	Curbe eliptice. Aplicaţii în criptografie	Expunerea, conversaţia, demonstraţia, problematizarea	4 ore

Bibliografie

Referinţe principale:

1. Koblitz N.: A Course in Number Theory and Cryptography, Springer, 1994
2. Liţcanu R.: Criptografie, note de curs, www.math.uaic.ro/~criptografie
3. Menezes A., van Oorschot P., Vanstone, S.: Handbook of applied cryptography, http://www.cacr.math.uwaterloo.ca/hac/
4. Tamas V., Leoreanu V.: Curs de Aritmetică, Ed. Matrix, 2002

Referinţe suplimentare:

1. Buchmann J.: Introduction to Cryptography, Springer, 2004
2. Languasco A.; Zaccagnini A.: Introduzione alla Crittografia, Hoepli, Milano, 2004

8.2	**Seminar / Laborator**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Elemente de aritmetică	Exerciţiul, conversaţia	3 ore
2.	Teste de primalitate. Algoritmi de factorizare	Exerciţiul, conversaţia	3 ore
3.	Criptosisteme simetrice	Exerciţiul, conversaţia	6 ore
4.	Criptosisteme cu cheie publică	Exerciţiul, conversaţia	8 ore
5.	Semnătura digitală	Exerciţiul, conversaţia	3 ore
6.	Protocoale criptografice	Exerciţiul, conversaţia	3 ore
7.	Curbe eliptice. Aplicaţii în criptografie	Exerciţiul, conversaţia	2 ore

Bibliografie

1. Buchmann J.: Introduction to Cryptography, Springer, 2004
2. Koblitz N.: A Course in Number Theory and Cryptography, Springer, 1994
3. Tamas V., Leoreanu V. : Curs de Aritmetică, Ed. Matrix, 2002

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

Cursul şi seminarul vor furniza studenţilor aplicaţii ale noţiunilor şi rezultatelor de aritmetică studiate în anul I, precum şi informaţii şi competenţe referitoare la principalii algoritmi criptografici.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs	Cunoaşterea şi utilizarea corectă a noţiunilor şi rezultatelor fundamentale, aplicarea corectă a rezultatelor teoretice	Verificarea periodică scrisă (2 lucrari scrise)	30 %
10.5 Seminar/ Laborator	Identificarea metodelor pentru rezolvarea unor exerciţii şi probleme, dobândirea unor deprinderi de calcul, realizarea şi implementarea unor algoritmi	Verificarea periodică scrisă (lucrare scrisă), verificarea curentă (orală, practică, temă), proiectul	70 %

10.6 Standard minim de performanţă

1. Identificarea si selectarea metodelor pentru rezolvarea unor exerciţii concrete simple
2. Elaborarea unor algoritmi pentru criptarea/decriptarea şi semnarea digitală a unor mesaje
3. Cunoaşterea şi utilizarea unor noţiuni şi concepte matematice de bază folosite în criptografie, în conformitate cu o listă minimală legată de conţinutul cursului
4. Realizarea şi expunerea unui proiect pe o temă dată

Nota finală = (L1 + L2 + P)/3
Criterii de promovabilitate: Obtinerea notei finale minim 5: (L1+L2+P)/3 >= 5; obtinerea notei minim 5 la evaluarea proiectului: P>= 5

L1, L2 = note lucrari scrise, saptamanile 8, 14.
P = evaluare proiect (poate include maxim două puncte pentru portofoliul cu teme seminar / laborator)

Data completării	Titular de curs	Titular de seminar
03.10.2019	Prof. dr. Răzvan Liţcanu	Asist. dr. Andrei Cuzub

Data avizării în departament	Director de departament
22.10.19	Prof. Dr. Ioan Bucataru