FIŞA DISCIPLINEI

1. Date despre program

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

2. Date despre disciplină

2.1 Denumirea disciplinei			**Introducere in Criptografie**				
2.2 Titularul activităţilor de curs			**Prof.Dr. Tiplea Ferucio Laurentiu**				
2.3 Titularul activităţilor de seminar			**Prof.Dr. Tiplea Ferucio Laurentiu**				
2.4 An de studiu	**II**	**2.5** Semestru	**1**	**2.6** Tip de evaluare	**M**	**2.7** Regimul disciplinei*	**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					**14**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					**14**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					**28**
Tutoriat					**-**
Examinări					**4**
Alte activităţi					**-**

3.7 Total ore studiu individual	**56**
3.8 Total ore pe semestru	**114**
3.9 Număr de credite	**5**

4. **Precondiţii** (dacă este cazul)

4.1 De curriculum	**-**
4.2 De competenţe	**-**

5. **Condiţii** (dacă este cazul)

5.1 De desfăşurare a cursului	Este recomandata prezenta la curs
5.2 De desfăşurare a seminarului	Prezenta la seminar

6. Competenţe specifice acumulate

Competenţe profesionale	**C1.** Expunerea unor noţiuni şi rezultate de bază din domeniul codurilor si criptografiei, în vederea însuşirii lor **C2.** Aplicarea conceptelor asimilate în domenii fundamentale informaticii, precum securitatea informatiei
Competenţe transversale	**CT1.** Eficientizarea activităţilor desfăşurate în cadru organizat, prin aplicarea regulilor academice de muncă riguroasă şi creativă **CT2.** Utilizarea optimă a surselor informaţionale şi a resurselor de comunicare din domeniu **CT3.** Exprimarea unei atitudini responsabile faţă de înţelegerea rolului domeniului în informatică **CT4.** Valorificarea eficace a potenţialului stiinţific însuşit în domeniu

7. **Obiectivele disciplinei** (din grila competenţelor specifice acumulate)

7.1 Obiectivul general	Cursul introduce studentilor o tematica majora in informatica, si anume criptografia, utilizata in principal pentru obtinerea de tehnici de securitate a informatiei.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: ▪ Utilizeze corespunzator concepte de criptografie; ▪ Inteleaga corespunzator, la nivel ridicat, securitatea sistemelor informatice.

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)

1.	Introducere in criptografie	Expunere si demonstratii realizate la tabla	2
2.	Secret perfect (partea I)	Expunere si demonstratii realizate la tabla	2
3.	Secret perfect (partea II)	Expunere si demonstratii realizate la tabla	2
4.	Criptografie simetrica (partea I)	Expunere si demonstratii realizate la tabla	2
5.	Criptografie simetrica (partea II)	Expunere si demonstratii realizate la tabla	2
6.	Criptografie simetrica (partea III)	Expunere si demonstratii realizate la tabla	2
7.	Criptografie cu chei publice (partea I)	Expunere si demonstratii realizate la tabla	2
8.	Criptografie cu chei publice (partea II)	Expunere si demonstratii realizate la tabla	2
9.	Criptografie cu chei publice (partea III)	Expunere si demonstratii realizate la tabla	2
10.	Functii hash si MAC (partea I)	Expunere si demonstratii realizate la tabla	2
11.	Functii hash si MAC (partea II)	Expunere si demonstratii realizate la tabla	2
12.	Semnaturi digitale (partea I)	Expunere si demonstratii realizate la tabla	2
13.	Semnaturi digitale (partea II)	Expunere si demonstratii realizate la tabla	2
14.	Scheme de partajare a secretelor	Expunere si demonstratii realizate la tabla	2

Bibliografie

Referinţe principale:

- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997

Referinţe suplimentare:

- F.L. Tiplea. Fundamentele Algebrice ale Informaticii, Ed. Polirom, 2006

8.2	**Seminar / Laborator**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Introducere in criptografie	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2

2.	Secret perfect (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
3.	Secret perfect (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
4.	Criptografie simetrica (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
5.	Criptografie simetrica (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
6.	Criptografie simetrica (partea III)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
7.	Criptografie cu chei publice (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
8.	Criptografie cu chei publice (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
9.	Criptografie cu chei publice (partea III)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
10.	Functii hash si MAC (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
11.	Functii hash si MAC (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
12.	Semnaturi digitale (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
13.	Semnaturi digitale (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
14.	Scheme de partajare a secretelor	Exercitii realizate la tabla prin participarea studentilor	2

		si propunerea de implementari	

Bibliografie

- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997

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

Cursul este corelat cu asteptarile moderne in securitatea informatiei (de exemplu, Amazon si-a format recent echipe de securitatea informatiei, multi dintre fostii studenti ai masterului de securitatea informatiei fiind membri ai acestor echipe).

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu; Abilitatea de aplicare a lor	Test scris	50%
10.5 Seminar/ Laborator	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu; Abilitatea de aplicare a lor	Exercitii realizate in clasa de fiecare student, precum si evaluarea de implementari	50%
10.6 Standard minim de performanţă			
Minim nota 5 atat la testul scris cat si la activitatea de seminar/laborator			

Data completării

Titular de curs
Prof.Dr. Tiplea Ferucio Laurentiu

Titular de seminar
Prof.Dr. Tiplea Ferucio laurentiu

Data avizării în departament

Director de departament