FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea din Bucureşti
1.2. Facultatea	Facultatea de Matematică şi Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Master
1.6. Programul de studii / Calificarea	Securitate şi logică aplicată
1.7. Forma de învăţământ	ZI

2. Date despre disciplină

2.1. Denumirea disciplinei	**Criptografie**							
2.2. Titularul activităţilor de curs				Lector Dr. Adela Georgescu				
2.3. Titularul activităţilor de seminar / laborator / proiect				Lector Dr. Adela Georgescu				
2.4. Anul de studiu	I	2.5. Semestrul	I	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	Conţinut[2)]	DF
							Obligativitate[3)]	DI

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1. Număr de ore pe săptămână	**3**	din care: 3.2. curs	**2**	3.3. seminar/ proiect	**1**
3.4. Total ore pe semestru	**42**	din care: 3.5. curs	**28**	3.6. SF	**14**

Distribuţia fondului de timp	**Ore**
3.4.1. Studiul după manual, suport de curs, bibliografie şi notiţe – nr. ore SI	50
3.4.2. Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	34
3.4.3. Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri	50
3.4.4.Examinări	4
3.4.5. Alte activităţi	

3.7. Total ore studiu individual	138
3.8. Total ore pe semestru	180
3.9. Numărul de credite	6

**** SI (din plan) + însumarea punctelor 3.4.2. şi 3.4.3. (vezi mai jos, în exemple, de unde rezultă nr. de ore pentru aceste puncte)**

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	Cursul se desfăşoară într-o sală cu videoproiector
5.2. de desfăşurare a seminarului/ laboratorului/ proiectului	

6. Competenţe specifice acumulate

Competenţe profesionale	Cunoasterea conceptelor de baza si a principiilor securitatii informatiei Utilizarea corecta a primitivelor si a sistemelor criptografice Studiul principalelor primitive criptografice actuale Analizarea securitatii sistemelor criptografice
Competenţe transversale	Preocuparea pentru perfectionarea securitatii sistemelor informatice Dezvoltarea gandirii critice (in particular, asupra sistemelor informatice) prin antrenarea capacitatilor de evidentiere a punctelor vulnerabile

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

7.1. Obiectivul general al disciplinei	Familiarizarea studentilor cu principiile criptografiei moderne si aplicarea primitivelor si a sistemelor criptografice in situatii concreteş din viata reala.
7.2. Obiectivele specifice	Intelegerea evolutiei criptografiei si a necesitatii criptografiei moderne Dezvoltarea capacitatii de alegere si utilizare corecta a mecanismelor criptografice. Dezvoltarea abilitatilor de analiza a securitatii.

8. Conţinuturi

8.1. Curs	Metode de predare	Observaţii
1. Introducere in criptografie.	Prelegere Videoproiector	Resurse folosite: - Videoproiector - Calculator - Tabla
2. Criptanaliza. Modele de adversari.		
3. Criptografie simetrica: criptare simetrica, inetgritatea mesajelor, functii hash, criptare autentificata.		
4. Criptografie asimetrica: criptare asimetrica, semnaturi digitale, protocoale de stabilire a cheilor, infrastructura cu chei publice, signcryption.		
5. Demonstrarea securitatii. Modele de securitate si tehnici de demonstratie.		
6. Commitment si Oblivious Transfer.		
7. Demonstratii zero-knowledge		
Bibliografie: 1. J.Katz, Y.Lindell - Introduction to Modern Cryptography, Chapman & Hall/CRC Press, 2008 2. N.Smart - Cryptography: An introduction. https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf 3. C. Paar – Understanding Cryptography, Springer, 2010 4. S.Vaudenay - A Classical Introduction to Cryptography: Applications for Communications Security, Springer, 2006. 5. A.J.Menezes, P.C.van Oorschot, S.A.Vanstone - Handbook of Applied Cryptography, CRC Press, 2001.		
8.2. Seminar [temele dezbătute în cadrul seminariilor]	Metode de predare-învăţare	Observaţii
Aplicatii ale temelor prezentate in cadrul cursului	Teme individuale şi/sau de grup.	
Bibliografie: Aceeaşi ca la curs.		
8.3. Laborator [temele de laborator, proiecte etc, conform calendarului disciplinei]	Metode de transmitere a informaţiei	Observaţii
Bibliografie		
8.4. Proiect [doar pentru disciplinele la care exista proiect semestrial normat in planul de invatamant]	Metode de predare-învăţare	Observaţii
Bibliografie:		

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţilor epistemice, asociaţilor profesionale şi angajatori reprezentativi din domeniul aferent programului

Notiunile introduse in acest curs vor dezvolta capacitatea de analiza a studentilor si vor duce la o mai buna si profunda intelegere a problemelor legate de securitate. Oferind acces la dezvoltari actuale – teoretice, dar cu aplicabilitate practica – cursul isi propune devolte aptitudini de cercetare si inovare, pregatind candidati care pot urma programe doctorale si care pot deveni membrii ai departamentelor de cercetare ale firmelor din domeniu.

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Cunoasterea sistemelor de criptare si a tehnicilor de criptanaliza prezentate pe parcursul cursului Abilitatea de a aplica cunostintele dobandite pe cazuri particulare Abilitatea de a argumenta utilizarea / inutilizarea unui anumit sistem criptografic in diferite scenarii Abilitatea de a analiza securitatea unui algoritm criptografic	Lucrare scrisă	50%
10.5.1. Seminar	Capacitatea de a aplica cunostintele dobandite in cadrul cursului pentru rezolvarea problemelor propuse	Activitate in cadrul seminarului Prezentare de referate	50%
10.5.2. Laborator			
10.5.3. Proiect [doar pentru disciplinele la care exista proiect semestrial norrmat in planul de invatamant]			
10.6. Standard minim de performanţă. Nota 5.			

Data completării
.....

Coordonator de disciplină
Lector Dr. Adela Georgescu

Tutore de disciplină
Lector Dr. Adela Georgescu

Data avizării în departament
.....

Director de departament
Conferențiar Dr. Alin Ștefănescu

Notă:

1) Regimul disciplinei (conţinut) - *pentru nivelul de licenţă se alege una din variantele:* **DF** (disciplină fundamentală) / **DD** (disciplină din domeniu) / **DS** (disciplină de specialitate) / **DC** (disciplină complementară).

2) Regimul disciplinei (obligativitate) - *se alege una din variantele:* **DI** (disciplină obligatorie) / **DO** (disciplină opţională) / **DFac** (disciplină facultativă).

3) SI – studiu individual; TC – teme de control; AA – activităţi asistate; SF – seminar faţă în faţă; L – activităţi de laborator; P – proiect, lucrări practic