FIŞA DISCIPLINEI
Anul universitar 2021-2022

Decan,
Prof. Vasile-Ion Manta

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică „Gheorghe Asachi" din Iaşi
1.2 Facultatea	Automatică şi Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare şi tehnologia informației
1.5 Ciclul de studii[1]	Master
1.6 Programul de studii	Securitatea spaţiului cibernetic

2. Date despre disciplină

2.1 Denumirea disciplinei/Cod			Criptologie / SCC.IA.102				
2.2 Titularul activităților de curs			Prof.dr. Mitică Craus				
2.3 Titularul activităților de aplicații			Prof.dr. Mitică Craus				
2.4 Anul de studii[2]	1	2.5 Semestrul[3]	1	2.6 Tipul de evaluare[4]	examen	2.7 Tipul disciplinei[5]	DA

3. Timpul total estimat al activităților zilnice (ore pe semestru)

3.1 Număr de ore pe săptămână	4	din care 3.2 curs	2	3.3a sem.		3.3b laborator	2	3.3c proiect	
3.4 Total ore din planul de învățământ[6]	56	din care 3.5 curs	28	3.6a sem.		3.6b laborator	28	3.6c proiect	

Distribuția fondului de timp[7]	Nr. ore
Studiul după manual, suport de curs, bibliografie şi notițe	30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	30
Pregătire seminarii/laboratoare/proiecte, teme, referate şi portofolii	23
Tutoriat[8]	7
Examinări[9]	4
Alte activități:	

3.7 Total ore studiu individual[10]	94
3.8 Total ore pe semestru[11]	150
3.9 Numărul de credite	6

4. Precondiții (acolo unde este cazul)

4.1 de curriculum[12]	• Algebră, Analiză matematică, Statistică şi prelucrarea datelor, Structuri de date, Proiectarea algoritmilor, Algoritmi paraleli şi distribuiți
4.2 de competențe	• Utilizarea adecvată în comunicarea profesională a conceptelor proprii matematicii, calculabilității, complexității, paradigmelor de programare şi modelării sistemelor de calcul şi comunicații • Utilizarea de teorii şi instrumente specifice (concepte şi instrumente matematice specifice, algoritmi, scheme, modele, protocoale etc.) pentru explicarea funcționării şi structurii sistemelor hardware, software şi de comunicații

5. Condiții (acolo unde este cazul)

5.1 de desfăşurare a cursului[13]	• Tablă, videoproiector
5.2 de desfăşurare a seminarului / laboratorului / proiectului[14]	• Sală de laborator dotată cu reţea de calculatoare; acces la internet; medii de programare de nivel înalt

[1] *Licență / Master*
[2] *1-4 pentru licență, 1-2 pentru master*
[3] *1-8 pentru licență, 1-3 pentru master*
[4] *Examen, colocviu sau VP A/R – din planul de învățământ*
[5] *DF - disciplină fundamentală, DID - disciplină în domeniu, DS – disciplină de specialitate sau DC - disciplină complementară - din planul de învățământ*
[6] *Este egal cu 14 săptămâni* x *numărul de ore de la punctul 3.1 (similar pentru 3.5, 3.6abc)*
[7] *Liniile de mai jos se referă la studiul individual; totalul se completează la punctul 3.7.*
[8] *Între 7 şi 14 ore*
[9] *Între 2 şi 6 ore*
[10] *Suma valorilor de pe liniile anterioare, care se referă la studiul individual.*
[11] *Suma dintre numărul de ore de activitate didactică directă (3.4) şi numărul de ore de studiu individual (3.7); trebuie să fie egală cu numărul de credite alocat disciplinei (punctul 3.9)* x *24 de ore pe credit.*
[12] *Se menționează disciplinele obligatoriu a fi promovate anterior sau echivalente*
[13] *Tablă, videoproiector, flipchart, materiale didactice specifice etc.*
[14] *Tehnică de calcul, pachete software, standuri experimentale, etc.*

6. Competențele specifice acumulate[15]

		Număr de credite alocat disciplinei[16]: **6**	Repartizare credite pe competențe[17]
Competențe profesionale	CP1	Cunoașterea conceptelor avansate din domeniul științei calculatoarelor și tehnologiei informației și capacitatea de a opera cu aceste concepte.	1.2
	CP2	Cercetarea științifică și practică privind securitatea sistemelor informatice complexe.	1.2
	CP3	Rezolvarea problemelor pe baza metodelor și tehnologiilor de securizare a sistemelor informatice complexe.	1.1
	CP4	Utilizarea de instrumente specifice domeniului în vederea identificării vulnerabilităților și a amenințărilor de securitate cibernetică.	1
	CP5	Proiectarea și dezvoltarea de soluții software cu un înalt grad de securitate orientate pe prevenția și răspunsul la incidente de securitate cibernetică.	1
	CP6		
	CPS1		
	CPS2		
Competențe transversale	CT1	Aplicarea, în contextul respectării legislației, a drepturilor de proprietate intelectuală, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă.	0.1
	CT2	Identificarea rolurilor și responsabilităților într-o echipă specializată, luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei.	0.2
	CT3	Dezvoltarea spiritului de creativitate, inițiativă și acțiune, pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.	0.2
	CTS		

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1 Obiectivul general al disciplinei	• Inițiere în știința criptografiei și criptanalizei
7.2 Obiective specifice	• Cunoașterea tehnicilor clasice de criptare și a metodelor de criptanaliză • Intelegerea algoritmilor de criptare și a tipurilor de atac

8. Conținuturi

8.1 Curs[18]	Metode de predare[19]	Observații

[15] *Competențele din Grilele G1 și G1bis ale programului de studii, adaptate la specificul disciplinei, pentru care se repartizează credite (www.rncis.ro sau site-ul facultății)*
[16] *Din planul de învățământ*
[17] *Creditele alocate disciplinei se distribuie pe competențe profesionale și transversale în funcție de specificul disciplinei*
[18] *Titluri de capitole și paragrafe*
[19] *Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții (pentru fiecare capitol, dacă este cazul)*

Criptografie şi criptanaliză - concepte de bază (1h) Elemente de teoria numerelor, combinatorică şi teoria probabilităţilor utilizate în criptologie (3h) Criptografie: Criptografie simetrică Criptare cu cifru orientat pe bloc de date Standardele de criptare a datelor DES, 3DES (2h) Standardul avansat de criptare AES (2h) Criptare cu cifru orientat pe flux de date (2h) Criptografie asimetrică Criptosistemul RSA (Rivest–Shamir–Adleman) (3h) Criptare cu cheie publică bazată pe problema logaritmului discret (3h) Criptare cu funcţii hash (2h) Criptanaliză : Criptanaliză liniară (2h) Criptanaliză diferenţială (2h) Criptanaliza DES (2h) Criptanaliza AES (2h) Criptanaliza RSA (2h)	Utilizarea videoproiectorului la prelegeri; Intrebări adresate studenţilor după prezentarea unor noțiuni; Intrebări adresate studenţilor în timpul şi după prezentarea unor algoritmi; Scrierea pe tablă a unor explicaţii şi exemple suplimentare; Implicarea studenţilor în acest proces.	Recomandarea, pentru studiul individual, a unor capitole din bibliografia indicată, în vederea aprofundării sau extinderii cunoştinţelor acumulate la curs.

Bibliografie curs:

[1] Koshy, T., Elementary number theory with applications, 2nd edition, Academic Press, 2007
[2] Paar, C.; Pelzl, J., Understanding Cryptography - A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg, 2010
[3] Stinson, D., Cryptography: Theory and Practice, (Textbooks in Mathematics) 4th Edition, Chapman and Hall/CRC, 2018
[4] Antoine, J., Algorithmic cryptanalysis , Taylor and Francis Group, 2009
[5] Howard M. and Heys, A., Tutorial on Linear and Differential Cryptanalysis, Electrical and Computer Engineering, Faculty of Engineering and Applied Science, Memorial University of Newfoundland St. John's, NF, Canada

8.2a Seminar	Metode de predare[20]	Observaţii

8.2b Laborator	Metode de predare[21]	Observaţii
Biblioteca PyCrypto (4h) Generatoare de numere pseudo-aleatoare (2h) Algoritmul lui Euclid extins (2h) Algoritmul DES (2h) Algoritmul AES (2h) Algoritmul RSA (4h) Atacuri brute-force (2h) Atacuri bazate pe analiza frecvenţelor (2h) Atacuri asupra algoritmului DES (2h) Atacuri asupra algoritmului AES (2h) Atacuri bazate pe metoda factorului comun (RSA factorization attack) (4h)	Utilizarea video-proiectorului pentru prezentarea temei; Scrierea pe tablă a unor exemple şi implicarea studenţilor în acest proces. Asistarea studenţilor la îndeplinirea sarcinilor propuse	

8.2c Proiect	Metode de predare[22]	Observaţii

Bibliografie aplicaţii (seminar / laborator / proiect):

[1] Python Cryptography Toolkit (https://www.dlitz.net/software/pycrypto/doc/)
[2] Stinson, D., Cryptography: Theory and Practice, (Textbooks in Mathematics) 4th Edition, Chapman and Hall/CRC, 2018
[3] Antoine, J., Algorithmic cryptanalysis , Taylor and Francis Group, 2009
[4] The DES Algorithm Illustrated (http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm)
[5] AES proposal (https://web.archive.org/web/20070203204845/https://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf)
[6] Breaking AES-128 in realtime, no ciphertext required (https://news.ycombinator.com/item?id=1937902)
[7] Understanding Common Factor Attacks: An RSA-Cracking Puzzle (http://www.loyalty.org/~schoen/rsa/)

[20] *Discuţii, dezbateri, prezentare şi/sau analiză de lucrări, rezolvare de exerciţii şi probleme*
[21] *Demonstraţie practică, exerciţiu, experiment*
[22] *Studiu de caz, demonstraţie, exerciţiu, analiza erorilor etc*.

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului[23]

Actualizarea continuă a conținuturilor și metodelor de predare în funcție de rezultatele cercetării în domeniu pe plan național și mondial, cerințele mediului academic, economic și social.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare		10.3 Pondere din nota finală
10.4a Examen / Colocviu	● Cunoștințe teoretice și practice însușite (cantitatea, corectitudinea, acuratețea)	Teste pe parcurs[24]:	%	60% (minim 5)
		Teme de casă:	%	
		Alte activități[25]:	%	
		Evaluare finală:	100% (minim 5)	
10.4b Seminar	● Frecvența/relevanța intervențiilor sau răspunsurilor	Evidența intervențiilor, portofoliu de lucrări (referate, sinteze științifice)		% (minim 5)
10.4c Laborator	● Cunoașterea aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea și interpretarea unor rezultate	● Chestionar scris ● Răspuns oral ● Demonstrație practică		40% (minim 5)
10.4d Proiect	● Calitatea proiectului realizat, corectitudinea documentației proiectului, justificarea soluțiilor alese	● Autoevaluarea, prezentarea și/sau susținerea proiectului ● Evaluarea critică a unui proiect		% (minim 5)
10.5 Standard minim de performanță[26]				

Data completării,

13.01.2021

Semnătura titularului de curs,

.....

Semnătura titularului de aplicații,

.....

Data avizării în departament,

13.01.2021

Director departament,

Conf.dr.ing. Andrei Stan

[23] *Legătura cu alte discipline, utilitatea disciplinei pe piața muncii*
[24] *Se va preciza numărul de teste și săptămânile în care vor fi susținute.*
[25] *Cercuri științifice, concursuri profesionale etc.*
[26] *Se particularizează la specificul disciplinei standardul minim de performanță din grila de competențe a programului de studii, dacă este cazul.*