FIŞA DISCIPLINEI

1. Date despre program

1.1	Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2	Facultatea	Electronică, Telecomunicaţii şi Tehnologia Informaţiei
1.3	Departamentul	Comunicatii
1.4	Domeniul de studii	Inginerie electronică, telecomunicații și tehnologii Informaționale
1.5	Ciclul de studii	Master
1.6	Programul de studii/Calificarea	Sisteme Integrate de Comunicații cu Aplicații Speciale/ Master
1.7	Forma de învăţământ	IF - Învăţământ cu frecvenţă
1.8	Codul disciplinei	SICAS08.20

2. Date despre disciplină

2.1	Denumirea disciplinei					Tehnici de secretizare a informatiei					
2.2	Aria tematică (subject area)					Inginerie electronică, telecomunicații și tehnologii Informaționale					
2.3	Responsabil curs					Prof.dr.ing. Monica Borda					
2.4	Responsabil aplicatii					Conf.dr.ing. Raul Malutan					
2.5	Anul de studii	I	2.6	Semestrul	1	2.7	Evaluarea	E	2.8	Regimul disciplinei	DA/DO

3. Timpul total estimat

An/ Sem	Denumirea disciplinei	Nr. săpt.	Curs	Aplicaţii			Curs	Aplicaţii			Stud. Ind.	TOTAL	Credite
			[ore/săpt.]				[ore/sem.]						
				S	L	P		S	L	P			
	Tehnici de secretizare a informatiei		2		1		28		14		58	100	4

3.1	Număr de ore pe săptămână	3	3.2	din care curs	2	3.3	aplicaţii	1
3.4	Total ore din planul de înv.	100	3.5	din care curs	28	3.6	aplicaţii	14

Studiul individual	Ore
Studiul după manual, suport de curs, bibliografie şi notiţe	24
Documentare suplimentară în bibliotecă, pe platformele electronice şi pe teren	20
Pregătire seminarii/laboratore, teme, referate, portofolii, eseuri	20
Tutoriat	7
Examinări	3
Alte activităţi	14

3.7	Total ore studiul individual	58
3.8	Total ore pe semestru	100
3.9	Număr de credite	4

4. Precondiţii (acolo unde este cazul)

4.1	De curriculum	
4.2	De competenţe	Cunoştinţe de matematica, teoria informaţiei, prelucrări de semnale, circuite analogice si digitale, programare

5. Condiţii (acolo unde este cazul)

5.1	De desfăşurare a cursului	Cluj Napoca

5.2	De desfăşurare a aplicaţiilor	Cluj Napoca

6. Competenţe specifice acumulate

Competenţe profesionale	C2. Aplicarea metodelor de bază pentru achiziţia şi prelucrarea semnalelor C4 Conceperea, implementarea si operarea serviciilor de date, voce, video, multimedia, bazate pe întelegerea si aplicarea notiunilor fundamentale din domeniul comunicatiilor si transmisiunii informatiei
Competenţe transversale	N/A

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

7.1	Obiectivul general al disciplinei	Dezvoltarea de competente in domeniul sistemelor criptografice
7.2	Obiectivele specifice	1. Asimilarea cunoștințelor teoretice privind tehnologiilor criptografice de baza 2. Asimilarea cunoștințelor teoretice privind atacurilor si a modelelor de securitate in sisteme informatice 3. Obținerea deprinderilor pentru dezvoltarea de aplicații software si sisteme hardware în domeniul criptografiei, marcării transparenta a datelor, şi criptării de imagini

8. Conţinuturi

8.1. Curs (programa analitică)		Metode de predare	Observaţii
1	Bibliografie. Notiuni introductive: definire de termeni si scurt istoric	Expunere, discuţii	Video-proiector și tablă interactivă
2	Criptografie clasică		
3	Protocoale criptografice: generalitati, protocoale pentru comunicatii criptografice simetrice, protocoale pentru comunicatii criptografice asimetrice si hibride		
4	Protocoale pentru semnaturi digitale, protocoale pentru schimbul de chei, protocoale de autentificare		
5	Algoritmi criptografici: baze matematice, algoritmi simetrici - standardul de criptare a datelor (DES), alte cifruri bloc (LUCIFER, IDEA, RC2, RC4), combinarea cifrurilor bloc		
6	Generatoare de secvente pseudoaleatoare si cifruri bazate pe acestea (stream ciphers)		
7	Funcții greu inversabile (one-way hash functions), algoritmi bazati pe functii hash (MD4, MD5, SHA)		
8	Algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC), algoritmi cu chei publice pentru semnaturi digitale (DSA – digital signature algorithm)		
9	Tehnici criptografice : lungimea si managementul cheilor, utilizarea algoritmilor		
10	Marcarea transparenta (watermarking): principii şi cerinţe		
11	Marcarea transparenta a imaginilor		

12	Marcarea transparenta a semnalului video. Alte aplicaţii		
13	Stenografie ADN.		
14	Curs recapitulativ. Pregătire pentru examen		
8.4. Aplicaţii (proiect)		Metode de predare	Observaţii
1	Introducere in Matlab	Experimentul didactic, simularea, lucrul în echipă	Se utilizează calculator, tablă inteligenta
2	Criptografie clasica		
3	Algoritmi simetrici		
4	Criptografie cu chei publice		
5	Marcare transparenta		
6	Criptarea imaginilor		
7	Criptografie ADN. Certificate digitale		

Bibliografie

1. M. Borda, Fundamentals in Information Theory and Coding – Springer 2011, ISBN 978-3-642-20346-6, 509p
2. Titu Băjenescu, Monica Borda- *Securitatea în informatică şi telecomunicaţii*- Ed. Dacia 2001
3. Bruce Schneier - *Applied Cryptography – Protocols, Algorithms and Source Code in C. Second Edition*- John Willey & Sons, 1996
4. William Stallings – *Cryptography and network security. Principles and practice*- Prentice-Hall, 2nd edition, 1999
5. Alfred J. Menezes, Paul von Oorschot, Scott A. Vanstone- *Handbook of Applied Cryptography* - CRC Press, 1997
6. I. Cox, J. Bloom, M. Miller-*Digital Watermarking: Principles & Practice*- Morgan Kaufmann Publishers, 2001

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

Competențele dobândite vor fi necesare angajaţilor care îşi desfăşoară activitatea în domeniul dezvoltării (programării) și utilizării de aplicații de securitate

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Ponderea din nota finală
10.4 Curs	Nivelul achiziției cunoștințelor teoretice și nivelul deprinderilor dobândite	20 intrebari de tip test grila, fiecare intrebare fiind ponderata cu 0.3, si sintetizarea a doua subiecte de teorie, fiecare subiect fiind ponderat cu 1.5.	50%
10.5 Aplicații	Nivelul abilităților dobândite	Fiecare student va alege o tema de proiect. Mini-proiectul trebuie sa conțină: - O aplicație in domeniul temei alese - Documentație științifica (minim 5 pagini) - O prezentare care sa includa atat o descriere teoretica a proiectului cat si descrierea aplicatiei	50%
10.6 Standard minim de performanţă			

Nivel calitativ:

Cunoştinţe minimale:

- Să cunoască rolul unui criptosistem
- Să cunoască protocoale pentru comunicatii criptografice simetrice
- Să cunoască protocoale pentru comunicatii criptografice asimetrice şi hibride
- Să cunoască protocoale pentru semnaturi digitale

- Să cunoască protocoale pentru schimbul de chei şi protocoale de autentificare
- Să impelmenteze algoritmi criptografici: algoritmi simetrici - standardul de criptare a datelor (DES)
- Să implementeze cifruri bloc (LUCIFER, IDEA, RC2, RC4, AES)
- Să identifice generatoarele de secvente pseudoaleatoare si cifruri bazate pe acestea (stream ciphers)
- Să cunoască functii greu inversabile (one-way hash functions)
- Să cunoască algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC)
- Să cunoască algoritmi cu chei publice pentru semnaturi digitale (DSA – digital signature algorithm);
- Să cunoască tehnici criptografice: lungimea si managementul cheilor
- Să utilizeze diverse aplicatii: marcarea transparenta a datelor (watermarking),criptare de imagini

Competenţe minimale:

- Să analizeze metodic problemele întâlnite în activitate, şi să identifice elementele pentru care există soluții consacrate, asigurând astfel îndeplinirea sarcinilor
- Să se adapteze la noile tehnologii, să se dezvolte profesional şi personal, prin formare continuă folosind surse de documentare tipărite, software specializat şi resurse electronice în limba română și, cel puțin, într-o limbă de circulație internațională.
- Dezvoltarea abilitatilor de lucru, atat in echipa, cat si in mod independent; de rezolvare de probleme si luare de decizii

Nivel cantitati

- Raspuns corect la 10 intrebari de tip test grila si sintetizarea a unui subiect de teorie
- prezentarea mini-proiectului
- obtinerea unei note minime 5 la evaluarea în cadrul activităţilor aplicative

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
19.06.2023	Curs	Conf.dr.ing. Raul MALUTAN	
	Aplicații	Conf.dr.ing. Raul MALUTAN	

Data avizării în departament
11.07.2023

Director departament
Prof.dr.ing. Virgil DOBROTA

Data aprobării în Consiliul Facultății ETTI
12.07.2023

Decan
Prof.dr.ing. Ovidiu POP