FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei
1.3 Departamentul	Comunicații
1.4 Domeniul de studii	Inginerie electronică, telecomunicații şi tehnologii informaţionale
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Tehnologii Multimedia (TM) / Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	TM17.40

2. Date despre disciplină

2.1 Denumirea disciplinei	Tehnici de secretizare a informatiei						
2.2 Aria de conţinut	Arie teoretică Arie metodologică Arie de analiză						
2.3 Responsabil de curs	Prof.dr.ing. Monica Borda – Monica.Borda@com.utcluj.ro						
2.4 Titularul activităţilor de seminar / laborator / proiect	Conf.dr.ing. Raul Malutan – Raul.Malutan@com.utcluj.ro						
2.5 Anul de studiu	2	2.6 Semestrul	3	2.7 Tipul de evaluare	E	2.8 Regimul disciplinei	DS/ DO

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care: 3.2 curs	1	3.3 seminar / laborator	2
3.4 Total ore din planul de învăţământ	42	din care: 3.5 curs	14	3.6 seminar / laborator	28
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					12
Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri					20
Tutoriat					3
Examinări					3
Alte activităţi:					

3.7 Total ore studiu individual	58
3.8 Total ore pe semestru	100
3.9 Numărul 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 seminarului / laboratorului / proiectului	Cluj-Napoca

6. Competenţele 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 specifice acumulate)

7.1 Obiectivul general al disciplinei	Dezvoltarea de competente in domeniul sistemelor criptografice.
7.2 Obiectivele specifice	1. Asimilarea cunostintelor teoretice privind tehnologiilor criptografice de baza. 2. Asimilarea cunostinţelor 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, marcarii transparente a datelor si criptarii de imagini

8. Conţinuturi

8.1 Curs	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 cerinte		
11. Marcarea transparenta a imaginilor		
12. Marcarea transparenta a semnalului video. Alte aplicatii		
13. Stenografie ADN.		
14. Curs recapitulativ. Pregătire pentru examen		

Bibliografie

1. M. Borda, Fundamentals in Information Theory and Coding, Springer 2011, ISBN 978-3-642-20346-6.
2. T. Băjenescu, M. Borda, Securitatea în informatică şi telecomunicaţii, Editura Dacia, Cluj-Napoca 2001
3. B. Schneier, Applied Cryptography – Protocols, Algorithms and Source Code in C. Second Edition, John Willey & Sons, 1996
4. W. Stallings, Cryptography and network security. Principles and practice, Prentice-Hall, Second edition, 1999
5. A.J. Menezes, P. von Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
6. I. Cox, J. Bloom, M. Miller, Digital Watermarking: Principles & Practice, Morgan Kaufmann Publishers, 2001

8.2 Laborator	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.
2. T. Băjenescu, M. Borda, Securitatea în informatică şi telecomunicaţii, Editura Dacia, Cluj-Napoca 2001
3. B. Schneier, Applied Cryptography – Protocols, Algorithms and Source Code in C. Second Edition, John Willey & Sons, 1996
4. W. Stallings, Cryptography and network security. Principles and practice, Prentice-Hall, Second edition, 1999
5. A.J. Menezes, P. von Oorschot, S. 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 angajatorilor reprezentativi din domeniul aferent programului

Competentele dobandite vor fi folosite in urmatoarele ocupatii conform COR (Clasificarea Ocupațiilor din România): Inginer emisie; Inginer electronist, transporturi, telecomunicatii; Inginer imagine; Inginer sunet; Proiectant inginer electronist; Proiectant inginer de sisteme si calculatoare; Inginer sef car reportaj; Inginer sef schimb emisie; Inginer proiectant comunicatii; Inginer sisteme de securitate; Inginer suport vânzari; Dezvoltator de aplicatii multimedia; Inginer operare retea; Inginer testare sisteme de comunicatii; Manager proiect; Inginer de trafic; Consultant pentru sisteme comunicatii.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Nivelul achiziției cunoștințelor teoretice și nivelul deprinderilor dobândite	20 intrebari de tip test grila (T), fiecare intrebare fiind ponderata cu 0.3, si sintetizarea a doua subiecte de teorie, fiecare subiect fiind ponderat cu 1.5.	T, max 10 pct. 50%
10.5 Laborator	Nivelul abilităților dobândite	Fiecare student va alege o tema de proiect (P). Acesta trebuie sa conțină: • Aplicație in domeniul temei alese • Documentație științifica (minim 5 pagini) • Prezentare care sa includa atat o descriere teoretica a proiectului cat si descrierea aplicatiei	P, max. 10 pct. 50%
10.6 Standard minim de performanţă			

Nivel calitativ:

Cunoştinţe minimale:

- ✓ Să cunoască rolul unui criptosistem
- ✓ Să cunoască protocoale pentru comunicatii criptografice simetrice, asimetrice şi hibride
- ✓ Să cunoască protocoale pentru semnaturi digitale, pentru schimbul de chei şi protocoale de autentificare
- ✓ 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), algoritmi cu chei publice pentru semnaturi digitale (DSA – digital signature algorithm)
- ✓ Să cunoască tehnici criptografice: lungimea si managementul cheilor

Competenţe minimale:

- ✓ Să implementeze algoritmi criptografici: algoritmi simetrici - standardul de criptare a datelor (DES)
- ✓ Să implementeze cifruri bloc (LUCIFER, IDEA, RC2, RC4, AES)
- ✓ Să utilizeze diverse aplicatii: marcarea transparenta a datelor (watermarking), criptare de imagini

Nivel cantitativ:

- ✓ T ≥ 5 (raspuns corect la 10 intrebari de tip test grila si sintetizarea a unui subiect de teorie)
- ✓ P≥ 5 (prezentarea mini-proiectului, obtinerea unei note minime 5 la evaluarea în cadrul activităţilor aplicative)
- ✓ (T+P)/2≥ 5

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
27.09.2021	Curs	Prof.dr.ing. Monica Borda	
	Aplicații	Conf.dr.ing. Raul Malutan	

Data avizării în Consiliul Departamentului COM 27.09.2021	Director Departament Comunicații Prof.dr.ing. Virgil DOBROTĂ
Data aprobării în Consiliul Facultății ETTI 27.09.2021	Decan Prof.dr.ing. Gabriel OLTEAN