

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Facultatea de Electronică, Telecomunicații și Tehnologia Informației
1.3 Departamentul	Comunicații
1.4 Domeniul de studii	Inginerie electronică, telecomunicații și tehnologii informaționale
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Tehnologii Multimedia (TM) / Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	TM17.40

### 2. Date despre disciplină

2.1 Denumirea disciplinei	Tehnici de secretizare a informației						
2.2 Aria de conținut	Arie teoretică						
	Arie metodologică						
	Arie de analiză						
2.3 Responsabil de curs	Prof.dr.ing. Monica BORDA – <a href="mailto:Monica.Borda@com.utcluj.ro">Monica.Borda@com.utcluj.ro</a>						
2.4 Titularul activităților de seminar / laborator / proiect	Conf.dr.ing. Raul MALUTAN – <a href="mailto:Raul.Malutan@com.utcluj.ro">Raul.Malutan@com.utcluj.ro</a>						
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 învățământ	42	din care: 3.5 curs	14	3.6 seminar / laborator	28
Distribuția fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					12
Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri					20
Tutoriat					3
Examinări					3
Alte activități: .....					
3.7 Total ore studiu individual	58				
3.8 Total ore pe semestru	100				
3.9 Numărul de credite	4				

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	-
4.2 de competențe	Cunoștințe de matematica, teoria informației, prelucrări de semnale, circuite analogice și digitale, programare

### 5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Cluj-Napoca
--------------------------------	-------------

5.2. de desfășurare a seminarului / laboratorului / proiectului	Cluj-Napoca
---	-------------

## 6. Competențele specifice acumulate

Competențe profesionale	C2. Aplicarea metodelor de bază pentru achiziția și prelucrarea semnalelor C4. Conceperea, implementarea și operarea serviciilor de date, voce, video, multimedia, bazate pe înțelegerea și aplicarea notiunilor fundamentale din domeniul comunicațiilor și transmisiunii informației
Competențe transversale	N/A

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

7.1 Obiectivul general al disciplinei	Dezvoltarea de competențe în domeniul sistemelor criptografice.
7.2 Obiectivele specifice	<ol style="list-style-type: none"> <li>Asimilarea cunoștințelor teoretice privind tehnologiile criptografice de bază.</li> <li>Asimilarea cunoștințelor teoretice privind atacurile și a modelelor de securitate în sisteme informatice</li> <li>Obținerea deprinderilor pentru dezvoltarea de aplicații software și sisteme hardware în domeniul criptografiei, marcarii transparente a datelor și criptării de imagini</li> </ol>

## 8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Bibliografie. Notiuni introductive: definire de termeni și scurt istoric	Expunere, discuții	Video-proiector și tablă interactivă
2. Criptografie clasică		
3. Protocoale criptografice: generalități, protocoale pentru comunicații criptografice simetrice, protocoale pentru comunicații criptografice asimetrice și hibride		
4. Protocoale pentru semnături 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 secvențe pseudoaleatoare și cifruri bazate pe acestea (stream ciphers)		
7. Funcții greu inversabile (one-way hash functions), algoritmi bazati pe funcții hash (MD4, MD5, SHA)		
8. Algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC), algoritmi cu chei publice pentru semnături digitale (DSA – digital signature algorithm)		

9. Tehnici criptografice : lungimea si managementul cheilor, utilizarea algoritmilor		
10. Marcarea transparenta (watermarking): principii și 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 și telecomunicații, 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

<b>8.2 Laborator</b>	Metode de predare	Observații
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 și telecomunicații, 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 conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului**

Competențele dobândite vor fi folosite în următoarele ocupații conform COR (Clasificarea Ocupațiilor din România): Inginer emisie; Inginer electronist, transporturi, telecomunicații; Inginer imagine; Inginer sunet; Proiectant inginer electronist; Proiectant inginer de sisteme și calculatoare; Inginer șef car reportaj; Inginer șef schimb emisie; Inginer proiectant comunicații; Inginer sisteme de securitate; Inginer suport vânzări; Dezvoltator de aplicații multimedia; Inginer operare rețea; Inginer testare sisteme de comunicații; Manager proiect; Inginer de trafic; Consultant pentru sisteme de comunicații.

## 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 întrebări de tip test grila (T), fiecare întrebare fiind ponderată cu 0.3, și sintetizarea a două 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 temă de proiect (P). Acesta trebuie să conțină: <ul style="list-style-type: none"> <li>• Aplicație în domeniul temei alese</li> <li>• Documentație științifică (minim 5 pagini)</li> <li>• Prezentare care să includă atât o descriere teoretică a proiectului cât și descrierea aplicației</li> </ul>	P, max. 10 pct. 50%

### 10.6 Standard minim de performanță

#### **Nivel calitativ:**

##### *Cunoștințe minimale:*

- ✓ Să cunoască rolul unui criptosistem
- ✓ Să cunoască protocoale pentru comunicatii criptografice simetrice, asimetrice și hibride
- ✓ Să cunoască protocoale pentru semnături digitale, pentru schimbul de chei și protocoale de autentificare
- ✓ Să identifice generatoarele de secvențe pseudoaleatoare și cifruri bazate pe acestea
- ✓ Să cunoască funcții greu inversabile (one-way hash functions)
- ✓ Să cunoască algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC), algoritmi cu chei publice pentru semnături digitale (DSA – digital signature algorithm)
- ✓ Să cunoască tehnici criptografice: lungimea și managementul cheilor

##### *Competențe 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 aplicații: marcarea transparentă a datelor (watermarking), criptare de imagini

#### **Nivel cantitativ:**

- ✓  $T \geq 5$  (răspuns corect la 10 întrebări de tip test grila și sintetizarea a unui subiect de teorie)
- ✓  $P \geq 5$  (prezentarea mini-proiectului, obținerea unei note minime 5 la evaluarea în cadrul activităților aplicative)
- ✓  $(T+P)/2 \geq 5$

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
20.06.2024	Curs	Prof.dr.ing. Monica BORDA	
	Aplicații	Conf.dr.ing. Raul MALUTAN	

Data avizării în Consiliul Departamentului COM 10.07.2024	Director Departament Comunicații Prof.dr.ing. Virgil DOBROTĂ
Data aprobării în Consiliul Facultății ETTI 11.07.2024	Decan Prof.dr.ing. Ovidiu POP