

Denumirea disciplinei	Tehnici de secretizare a informației
Domeniul de studiu	Inginerie electronica si telecomunicații
Master	Tehnologii multimedia, Telecomunicații
Codul disciplinei	TM11.00, TC14.10
Titularul disciplinei	Prof.dr.ing. Monica BORDA, Monica.Borda@com.utcluj.ro
Colaboratori	
Departament	Comunicații
Facultatea	Electronică, Telecomunicații și Tehnologia Informației

Sem.	Tipul disciplinei	Curs			Aplicații			Stud. Ind.	TOTAL	Credit	Forma de verificare		
		[ore fizice/săpt.]			[ore fizice/sem.]								
			S	L	P		S					L	P
3	Specialitate TM	2		1		28		14		88	130	5	E
3	Optional 3 TC	2		1		28		14		88	130	5	E

Competențe dobândite:
Cunoștințe teoretice, (Ce trebuie sa cunoască)
<p>Protocoale criptografice: generalitati • protocoale pentru comunicatii criptografice simetrice • protocoale pentru comunicatii criptografice asimetrice si hibride • protocoale pentru semnaturi digitale • protocoale pentru schimbul de chei • protocoale de autentificare ; Algoritmi criptografici: baze matematice • algoritmi simetrici - standardul de criptare a datelor (DES) • alte cifruri bloc (LUCIFER, IDEA, RC2, RC4, AES) • combinarea cifrurilor bloc • generatoare de secvente pseudoaleatoare si cifruri bazate pe acestea (stream ciphers) • functii greu inversabile (one-way hash functions) • algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC) • algoritmi cu chei publice pentru semnaturi digitale (DSA – digital signature algorithm); Tehnici criptografice: lungimea si managementul cheilor • utilizarea algoritmilor ; Politici criptografice; Aplicatii: marcarea transparenta a datelor (watermarking) • comert electronic • posta electronica • criptare de imagini</p>
Deprinderi dobândite: (Ce știe să facă)
<ul style="list-style-type: none"> • Cunoasterea rolului unui criptosistem • Cunoasterea tehnologiilor criptografice de baza • Cunoasterea atacurilor si a modelelor de securitate in sisteme informatice
Abilități dobândite: (Ce echipamente, instrumente știe să mănuiască)
<ul style="list-style-type: none"> • Capacitatea de a intelege functionarea, rolul si utilizarea cifrurilor simetrice si cu chei publice precum si a semnaturilor digitale • Capacitatea de a proiecta sisteme de securitate pentru sisteme informatice • Capacitatea de proiecta si implementa software si hardware aplicatii criptografice: comert electronic, marcarea transparenta a datelor, amprentare, criptare de imagini

Cerințe prealabile (Dacă este cazul)
Cunoștințe de matematica, Teoria informatiei, Prelucrari de semnale, Circuite analogice si digitale, Programare

A. Curs (titlul cursurilor + programa analitica)		
1	Bibliografie. Notiuni introductive: definire de termeni si scurt istoric	2 ore
2	Criptografie clasică	2 ore
3	Protocoale criptografice: generalitati, protocoale pentru comunicatii criptografice simetrice, protocoale pentru comunicatii criptografice asimetrice si hibride	2 ore
4	Protocoale pentru semnaturi digitale, protocoale pentru schimbul de chei, protocoale de autentificare	2 ore
5	Algoritmi criptografici: baze matematice, algoritmi simetrici - standardul de criptare a datelor (DES), alte cifruri bloc (LUCIFER, IDEA, RC2, RC4),	2 ore

	combinarea cifrurilor bloc	
6	Generatoare de secvențe pseudoaleatoare și cifruri bazate pe acestea (stream ciphers)	2 ore
7	Funcții greu inversabile (one-way hash functions), algoritmi bazati pe funcții hash (MD4, MD5, SHA)	2 ore
8	Algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC), algoritmi cu chei publice pentru semnături digitale (DSA – digital signature algorithm)	2 ore
9	Tehnici criptografice : lungimea și managementul cheilor, utilizarea algoritmilor	2 ore
10	Marcarea transparentă (watermarking): principii și cerințe	2 ore
11	Marcarea transparentă a imaginilor	2 ore
12	Marcarea transparentă a semnalului video. Alte aplicații	2 ore
13	Steganografie ADN.	2 ore
14	Curs recapitulativ. Pregătire pentru examen	2 ore

B1. Aplicații – LUCRARI (lista lucrări, teme de seminar, conținutul proiectului de an)

1	Introducere. Descrierea platformei de laborator	2 ore
2	Criptografie clasică	2 ore
3	Algoritmi simetrici	2 ore
4	Criptografie cu chei publice	2 ore
5	Marcare transparentă	2 ore
6	Criptarea imaginilor	2 ore
7	Criptografie ADN	2 ore

B2. Sala laborator (Denumire/sala) 210/A Dorobanților 71-73

C. Studiul individual (tematica studiilor bibliografice, materiale de sinteză, proiecte, aplicații etc.)

1 miniproiect din tematica studiată la curs și la laborator. Miniproiectul se finalizează cu o aplicație implementată în C/C++ sau MatLab și cu prezentarea rezultatelor sub forma unei lucrări științifice.

Structura studiului individual	Studiu materiale curs	Rezolvări teme, lab., proiecte	Pregătire aplicații	Timp alocat examinărilor	Studiu bibliografic suplimentar	Total ore pregătire individuală
Nr. ore	28	25	12	2	21	88

Bibliografie – 5 (numar de titluri aflate in biblioteca UTC-N)

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

Modul de examinare și atribuire a notei

Modul de examinare	Examen scris (3 ore)
Componentele notei	Miniproiect M (nota M); Examen (nota E)
Formula de calcul a notei	$N=0,6E+0,4M$; se calculează dacă: $E>4$

Responsabil disciplina
Prof.dr.ing. Monica BORDA