Denumirea disciplinei	Tehnici de secretizare a informaţiei
Domeniul de studiu	Inginerie electronica si telecomunicaţii
Master	Tehnologii multimedia, Telecomunicatii
Codul disciplinei	TM17.40, TC17.40
Titularul disciplinei	Prof.dr.ing. Monica BORDA, Monica.Borda@com.utcluj.ro
Colaboratori	
Departament	Comunicaţii
Facultatea	Electronică, Telecomunicaţii şi Tehnologia Informaţiei

Sem.	Tipul disciplinei	Curs	Aplicaţii			Curs	Aplicaţii			Stud. Ind.	TOTAL	Credit	Forma de verificare
		[ore fizice/săpt.]				[ore fizice/sem.]							
			S	L	P		S	L	P				
3	**Optional 3 TM**	**2**		**1**		**28**		**14**		**58**	**100**	**4**	**E**
3	**Optional 3 TC**	**2**		**1**		**28**		**14**		**58**	**100**	**4**	**E**

Competenţe dobândite:

Cunoştinţe teoretice, (Ce trebuie sa cunoască)

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

Deprinderi dobândite: (Ce ştie să facă)

- Cunoasterea rolului unui criptosistem
- Cunoasterea tehnologiilor criptografice de baza
- Cunoasterea atacurilor si a modelelor de securitate in sisteme informatice

Abilităţi dobândite: (Ce echipamente, instrumente ştie să mânuiască)

- 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, marcare transparenta a datelor, amprentare, criptare de imagini

Cerinţe prealabile (Dacă este cazul)

Cunoştinţe 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 secvente pseudoaleatoare si cifruri bazate pe acestea (stream ciphers)	2 ore
7	Functii greu inversabile (one-way hash functions), algoritmi bazati pe functii hash (MD4, MD5, SHA)	2 ore
8	Algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC), algoritmi cu chei publice pentru semnaturi digitale (DSA – digital signature algorithm)	2 ore
9	Tehnici criptografice : lungimea si managementul cheilor, utilizarea algoritmilor	2 ore
10	Marcarea transparenta (watermarking): principii şi cerinţe	2 ore
11	Marcarea transparenta a imaginilor	2 ore
12	Marcarea transparenta a semnalului video. Alte aplicaţii	2 ore
13	Steganografie ADN.	2 ore
14	Curs recapitulativ. Pregătire pentru examen	2 ore

B1. Aplicaţii – **LUCRARI** (lista lucrări, teme de seminar, conţinutul proiectului de an)		
1	Introducere. Descrierea platformei de laborator	2 ore
2	Criptografie clasica	2 ore
3	Algoritmi simetrici	2 ore
4	Criptografie cu chei publice	2 ore
5	Marcare transparenta	2 ore
6	Criptarea imaginilor	2 ore
7	Criptografie ADN	2 ore
B2. Sala laborator (Denumire/sala) 210/A Dorobanţilor 71-73		

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

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

Structura studiului individual	Studiu materiale curs	Rezolvări teme, lab., proiecte	Pregătire aplicaţii	Timp alocat examinărilor	Studiu bibliografic suplimentar	Total ore pregătire individuală
Nr. ore	18	15	12	2	11	58

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

1. Titu Băjenescu, Monica Borda- *Securitatea în informatică şi telecomunicaţii*- 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 şi 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

_____