Denumirea disciplinei	**Tehnici de secretizare a informației**
Domeniul de studiu	**Inginerie electronica si Telecomunicatii**
Specializarea	**Master in Telecomunicatii**
Codul disciplinei	
Titularul disciplinei	Prof.dr.ing. Monica Borda
Colaboratori	
Catedra	Comunicatii
Facultatea	Electronica si Telecomunicatii

Sem	Tipul disciplinei Disc.Fundamentala, Disc.Ing.din Dom, Disc. de Spec, Disc Optionala, Disc.Facultativa	Curs [ore/ sapt]	Aplicații [ore/sapt]			Curs [ore/ sem]	Aplicații [ore/sem]			Studiul Individual [ore/ sem]	Practica	TOTAL	Puncte credit	Forma de verificare
			S	L	P		S	L	P					
III	**Disciplină de specialitate**	**2**				**24**				**57**	**-**		**3**	**Examen**

Cerințe prealabile - prerequisites
Cunoştinţe de matematica, teoria informatiei,prelucrari de semnale, circuite analogice si digitale, programare

A. Conținutul Disciplinei (Titlul cursurilor/laboratorului)

Curs 1 – Bibliografie. Notiuni introductive: definire de termeni si scurt istoric
Curs 2 – Criptografie clasica
Curs 3 – Protocoale criptografice: generalitati, protocoale pentru comunicatii criptografice simetrice, protocoale pentru comunicatii criptografice asimetrice si hibride
Curs 4 – Protocoale pentru semnaturi digitale, protocoale pentru schimbul de chei, protocoale de autentificare
Curs 5 – Algoritmi criptografici: baze matematice, algoritmi simetrici - standardul de criptare a datelor (DES), alte cifruri bloc (LUCIFER, IDEA, RC2, RC4), combinarea cifrurilor bloc
Curs 6 – Generatoare de secvente pseudoaleatoare si cifruri bazate pe acestea (stream ciphers)
Curs 7 – Functii greu inversabile (one-way hash functions), algoritmi bazati pe functii hash (MD4, MD5, SHA)
Curs 8 – Algoritmi cu chei publice (principii, algoritmi de tip rucsac, RSA, LUC), algoritmi cu chei publice pentru semnaturi digitale (DSA – digital signature algorithm)
Curs 9 – Tehnici criptografice : lungimea si managementul cheilor, utilizarea algoritmilor
Curs 10 – Marcarea transparenta (watermarking)
Curs 11 – Criptare de imagini
Curs 12 – Comert electronic, posta electronica, politici criptografice

B. Tematica studiului individual (Tematica studiilor bibliografice, materiale de sinteza, proiecte, aplicatii, etc)

2 sinteze bazate pe materiale bibliografice aflate pe Internet
1 proiect

Structura pregătirii individuale	Studiu materiale curs	Studiu materiale tutoriale	Rezolvări teme/elaborare proiect	Pregătire aplicații	Timp alocat examinărilor	Total ore pregătire individuală
Nr. ore	24	15	15		3	57

Bibliografie

1. Titu Băjenescu, Monica Borda- *Securitatea în informatică şi 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. H.M. Deitel, P.J. Deitel, T.R. Nieto- *E-Business & e-Commerce. How to Program* –Prentice Hall, 2001
5. Alfred J. Menezes, Paul von Oorschot, Scott A. Vanstone- *Handbook of Applied Cryptography* - CRC Press, 1997

6. V. Patriciu, M.Pietrosanu, I. Bica, N. Voicu, C. Vaduva, - *Securitatea în comerțul electronic*-Ed. All, 2001
I. Cox, J. Bloom, M. Miller-*Digital Watermarking: Principles & Practice*- Morgan Kaufmann Publishers, 2001

Competente Dobindite:
Cunostinte teoretice - Programa analitică
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

Abilitati dobândite: (Ce ştie să facă)
■ Cunoasterea rolului unui criptosistem ■ Cunoasterea tehnologiilor criptografice de baza ■ Cunoasterea atacurilor si a modelelor de securitate in sisteme informatice ■ 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 precum : comert electronic, marcare transparenta a datelor, amprentare, criptare de imagini

Modul de examinare şi atribuire a notei	
Modul de examinare	Examenul constă dintr-un test scris (3 ore). Proiectul este notat individual
Componentele notei	Laborator (nota L); Teme (nota T); Examen (nota E)
Formula de calcul a notei	N=0,6E+0,3T+0,1L se calculează dacă: E>4 şi L>4

Informații suplimentare despre disciplină		
Discipline similare	Nume disciplină la www.utcluj.ro : Tehnici de secretizare a informatiei (master PSI Sibiu)	
Baza materială disponibilă	Spațiu: Sala 210A Dorobantilor 71-73	Echipamente specifice: calculatoare
Entități interesate de curs	Firme/Absolvenți/ - se ataşează susținerea exprimată	

Discipline similare in cadrul unor alte programe de master:

1. Universita degli studi di Catania- http://www.dmi.unict.it/~barba/Socrates/Courses/Master/Criptography.doc
2. UPC - Universitat Politècnica de Catalunya http://www.emagister.com/master-science-information-communication-technologies-mint-cursos-2292533.htm
3. Escola Tecnica Superior de d'Enginyeria de Barcelona de Telecomunication de Barcelona - http://www.etsetb.upc.edu/info_sobre/estudis/guia_docent/guia_docent_html.html?idSeccio=829
4. Academia Tehnica Militara - http://www.mta.ro/master-infosec/master_managementul_securitatii_informatiilor.htm