UNIVERSITATEA „LUCIAN BLAGA” DIN SIBIU
FACULTATEA DE ŞTIINȚE
CATEDRA DE INFORMATICĂ
Domeniul de studii de master: INFORMATICĂ
Specializarea: SISTEME ŞI TEHNOLOGII INFORMATICE AVANSATE

FIŞĂ DISCIPLINĂ

Denumirea disciplinei: Criptografie
Codul disciplinei:
Anul de studiu şi semestrul în care se studiază disciplina: anul II, semestrul I
Discipline anterioare cerute *:
Regimul disciplinei (obligatorie O, opțională A sau facultativă L): O
Categoria formativă (Cunoaştere aprofundată CA, Complementară CO, Cercetare CC): CA
Forma de evaluare (examen E, verificare V, colocviu C): E
Catedra care coordonează disciplina: Catedra Informatică
Titularul / titularii disciplinei: Lector univ.dr. Mircea I. NEAMTU

* disciplinele studiate anterior a căror cunoaştere este necesară pentru însuşirea disciplinei

Extinderea disciplinei în planul de învățământ *:				
Curs	Seminar	Laborator	Proiect	Total ($NOAD_{sem}$)
28		28		56

* numărul semestrial de ore de activități didactice directe

Obiectivele disciplinei
Obiectivele cursului Insusirea tehnicilor de criptare, codare, identificare respectiv corectie a erorilor si vulnerabilitatilor. Protectia impotriva atacurilor informatice.
Obiectivele activităților aplicative (seminar, laborator, proiect) Implementarea principalilor algoritmi de criptare, codare. Validarea tranzacțiilor. Securitatea si securizarea tranzacțiilor.

Conținutul disciplinei (capitolele cursului / tematica seminarului / lucrărilor practice / etapele proiectului)		
CURS		
Nr. crt.	**Tema**	**Nr.ore**
1	Scurt istoric al criptografiei. Concepte de baza.	2
2	Tehnologii criptografice	4

3	Ascunderea informatiilor	2
4	Sisteme criptate prin chei secrete (simetrice).	4
5	Sisteme de criptare prin chei publice (asimetrice). Sisteme de certificare a cheilor publice.	4
6	Semnatura digitala.	2
8	Infrastructura cheilor publice.	2
9	Atacuri informatice	4
10	Validarea tranzacțiilor. Securitatea si securizarea tranzacțiilor.	4

Conținutul disciplinei (capitolele cursului / tematica seminarului / lucrărilor practice / etapele proiectului)		
SEMINAR / LABORATOR / PROIECT		
Nr. crt.	**Tema**	**Nr.ore**
1	Algoritmul criptografic, textul cifrat, cheia, codurile, criptanaliza, criptarea.	2
2	Cifrul lui Cezar, Criptografia prin chei simetrice, cifrul lui Vernam, grila lui Cardan.	4
3	Ascunderea informatiei (Steganografia, Filigranarea, Securitatea tiparirii hartiilor de valoare).	2
4	Sisteme criptate prin chei secrete (simetrice: DES, AES, IDEA).	4
5	Sisteme de criptare prin chei publice (asimetrice: Shimbul de chei Diffie-Hellman, RSA). Sisteme de certificare a cheilor publice.	4
6	Semnatura digitala.	2
8	Infrastructura cheilor publice (PKI).	2
9	Atacuri criptografice (forta bruta, text clar (cunoscut, ales, selectat, ...), atac zi de nastere, intalnire la mijloc, om la mijloc, ...)	4
10	Validarea tranzacțiilor. Securitatea si securizarea tranzacțiilor. Erorile sistemelor, calculatoare moleculare.	4

Descrierea metodelor de predare
La curs se va folosi expunerea, explicatia, exemplificarea si conversatia frontala. La laborator se va folosi explicatia, exemplificarea, invatarea prin descoperire. Pentru curs si laborator exista suport electronic care se da studentilor la inceputul cursului. La curs se vor folosi si slide-uri si exemplificare pe calculator.

Descrierea formelor şi metodelor de evaluare a cunoştinţelor
Evaluarea cunostintelor se va face continuu in cadrul lucrarilor de laborator, fiind urmarita si evaluata activitatea studentilor la fiecare laborator. Nota finala este formata din: a) Media notelor acordate pentru activitatea la laborator 20% b) Nota proiect de laborator 40% c) Nota de la examenul scris 40%

Bugetul de timp pentru studiul individual			
Denumirea activităţii	**Nr. ore**	**Denumirea activităţii**	**Nr. ore**
1. Descifrarea şi studierea notiţelor de curs	20	6. Elaborarea temelor de casă, referatelor …	40
2. Studiul după manual sau suport de curs		7. Pregătirea pentru evaluările periodice	
3. Studierea bibliografiei minimale indicate	20	8. Pregătirea pentru examinarea finală	20
4. Documentarea suplimentară *		9. Participarea la consultaţii	
5. Pregătirea seminariilor şi/sau laboratoarelor	40	10. Alte activităţi …	
Numărul total al orelor alocate studiului individual $NOSI_{sem}$			140

- în bibliotecă, pe INTERNET, pe teren …

Bugetul de timp şi creditele alocate disciplinei			
$NOAD_{sem}$	$NOSI_{sem}$	$NOT_{sem} = NOAD_{sem} + NOSI_{sem}$	**Numărul de credite**
56	140	196	7

Criteriile de evaluare a cunoştinţelor şi promovarea disciplinei	
Evaluările considerate pentru stabilirea notei finale:	**Ponderea evaluării în nota finală, %**
• Media notelor acordate la seminar	
• Media notelor acordate pentru activitatea la laborator	10
• Notele obţinute la testele periodice sau parţiale	40 (nota pe activitatea de proiect)
• Nota acordată pentru frecvenţa la curs	
• Notele acordate pentru temele de casă, referate, eseuri, traduceri, studii de caz …	
• Notele acordate pentru participarea la cercuri ştiinţifice şi/sau la concursuri profesiobnale	
• Nota acordată la examinarea finală	50
• Alte note	

Modalitatea de examinare finală *:
Lucrare scrisă cu subiecte teoretice şi aplicaţii

* lucrare scrisă descriptivă, lucrare scrisă cu subiecte teoretice şi aplicaţii, test grilă, examinare orală cu bilete …

Competenţele specifice disciplinei *	
1. Competenţe privind cunoaşterea şi înţelegerea:	Cunoaşterea şi utilizarea adecvată a noţiunilor teoretice fundamentale legate de criptografie
2. Competenţe în domeniul explicării şi interpretării:	●Capacitatea de a explica modul de constructie a algoritmilor croptografici ●Capacitatea de a interpreta rezultatele obtinute

3. Competențe instrumental - aplicative:	●Capacitatea de a implemnta algoritmi criptografici ●Capacitatea de a utiliza si modifica conform cerinteleor algoritmii deja implementati ●Capacitatea de a proiecta şi realiza aplicații complexe care utilizeaza algoritmii si tehnicile invatate
4. Competențe atitudinale	Dezvoltarea atitudinii pozitive față de muncă şi responsabilitate pentru propria pregătire profesională. Dezvoltarea spiritului de munca in echipa.

* competențele generale sunt menționate în Fişa specializării

Bibliografie:

1) T.H. Cormen, C.E. Leiserson, R.R. Rivest, Introducere in algoritmi, Editia in limba romana, Computer Libris AGORA, 2002
2) B. Schneier - *Applied Cryptography – Protocols, Algorithms and Source Code in C. Second Edition*- John Willey & Sons, 1996
3) A. J. Menezes, Paul von Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography* – CRC Press, 1997
4) V. Patriciu, M.Pietrosanu, I. Bica, N. Voicu, C. Vaduva, - *Securitatea în comerțul electronic*-Ed. All, 2001
5) M. Howard, D. LeBlanc, *Writing Secure Code, Practical strategies and techniques for secure application coding in a networked world*, Second Edition, Microsoft, 2002
6) D. Oprea, *Protectia si securitatea informatiilor*, Ed. Polirom, Iasi, 2003
7) M.I. Neamtu, *Programare orientata obiect, Programare Java*. Ed. Alma Mater, ibiu, 2003
8) M.I. Neamtu, *Programare distribuita*, Ed. Alma Mater, Sibiu, 2005

Data elaborării:
01.02.2010

Titularul / titularii disciplinei
Lector univ. dr. Mircea I. NEAMTU