UNIVERSITATEA „POLITEHNICA”DIN TIMIŞOARA

SYLLABUS
pentru disciplina:

“SECURITATEA INFORMATIEI”

FACULTATEA *AUTOMATICĂ ŞI CALCULATOARE*
DOMENIUL/SPECIALIZAREA *INGINERIA SISTEMELOR*

Anul de studii: **III**
Semestrul *2*

Titularul cursului: Prof.dr.ing. Daniel-Ioan CURIAC				
Colaboratori: *(Nume şi prenume, titul ştiinţific, grad didactic; departamentul de care aparţine)*	*Ovidiu BANIAS*	*Drd.ing.*	*asistent*	*Automatica si InformaticaAplicata*
	Daniel IERCAN	*Dr.ing.*	*asistent*	*Automatica si InformaticaAplicata*

Număr de ore/săptămână / Verificarea / Credite					
Curs	**Seminar**	**Laborator**	**Proiect**	**Examinare**	**Credite**
2	**0**	**1**	**1**	**E**	**4**

Statul disciplinei	Fundamentală □	În domeniu **X**	De specialitate □	Complementară □
	Obligatorie: Impusă **X**	Opţională □		Facultativă □

A. OBIECTIVELE DISCIPLINEI
Obiectivele disciplinei*: însuşirea de către studenţi a tehnicilor moderne de securizare a datelor, cu precădere a securizării datelor prin criptare; prezentarea principalelor breşe în securitatea sistemelor de calcul cuplate în reţele, precum şi a modului de realizare a protecţiei împotriva atacurilor asupra securităţii;* ***Rezultatele invatarii:*** *considerarea componentei de „securizare a informaţiei” in proiectarea, implementarea, testarea oricărui sistem informatic; abilitatea de a implementa sisteme informatice cu un grad ridicat de securitate a informaţiei;* ***competente:*** *proiectarea, implementarea, testarea, administrarea, mentenanţa şi utilizarea reţelelor de calculatoare şi de alte echipamente numerice şi dezvoltarea aplicaţiilor de tehnologia informaţiei: 0.95%; Dezvoltarea şi administrarea de aplicaţii informatice, inclusiv de tip web, destinate domeniilor administrativ, medical, de afaceri, educaţional, etc.: 0,95%;*

B. SUBIECTELE CURSULUI
Capitolul 1: Introducere(6 ore)
1.1 Securitatea datelor; 1.2 Aspecte legate de securitatea informaţiei; 1.3 Servicii de securitate; 1.4 Modelul unei reţele sigure; 1.5 Atacuri; 1.6 Criptologia.
Capitolul 2: Criptarea convenţionala clasică (3 ore)
2.1 Modelul criptării convenţionale; 2.2 Algoritmi de criptare clasici
Capitolul 3: Algoritmi moderni de criptare (12 ore)
3.1 Principiile codurilor bloc; 3.2 Structura codului Feistel; 3.3 DES (Data Encryption Standard); 3.4 Triple DES; 3.5 Algoritmul IDEA; 3.6 Algoritmul Blowfish; 3.7 Algoritmul RC5; Algoritmul RC2
Capitolul 4: Criptarea cu chei publice (5 ore)
4.1 Principii; 4.2 Algoritmul RSA; 4.3 Administrarea cheilor; 4.4 Algoritmul Diffie-Hellman; 4.5 Standardul pentru semnaturi digitale
Capitolul 5: Studii de caz relativ la probleme de securitate in conducerea la distanta a proceselor industriale, retele de senzori, etc. (2 ore)

C. SUBIECTELE APLICATIILOR (laborator – 7 lucrari a cite 2 ore, proiect 7x2=14 ore)
- Aprofundarea prin lucrări aplicative a tehnicilor de criptare clasice:

Lucrarea 1: Codul Caesar, Roata alfabetica, Codificarea cu ceasul spiral,
Lucrarea 2: Corelaţia alfabet&cuvint, Codificarea busola, Codificarea Pig Latin,

Lucrarea 3: Tabela Viginere, Tabela Porta, Codificări matrice,
Lucrarea 4: Coduri monoalfabetice, Maşini rotative, Codificare Pig Pen,
Lucrarea 5: Codificare tip harta, Diagraphic substitution.

- Realizarea si sustinerea orala a unui referat asupra unui topic ce intervine in securizarea sistemelor (Firewalls, viruşi informatici, Programe antivirus, Sistemul Kerberos, Sistemul SESAME, PGP/PEM, securitatea sistemelor incorporate, criptarea pe curbe eliptice, criptarea cuantica, etc.) - *Lucrarea 6 si 7*
- Proiectarea si implementarea intr-unul din limbajele cunoscute (de preferinta C, pentru a satisface necesitatile de viteza) a unui algoritm modern de criptare destinat unor sisteme precizate prin tema de proiectare: un exemplu – securizarea informatiei prin criptare in retele de senzori: alegerea tipului de algoritm (cheie secreta/cheie publica); alegerea algoritmului in functie de lungimea mesajelor schimbate de senzori, de durata de viata a mesajelor, etc.; implementarea in C; testarea. (*proiect pe durata a 14 ore – 2 ore/saptamina*)

D. METODE DIDACTICE FOLOSITE *(Exemple: expunere, prelegere, conversaţie, explicaţie, exemplu, experiment, demonstraţie, analiză comparativă, simulare, studiu de caz, problematizare, brainstorming, portofoliul didactic, metoda proiectelor etc.)*

- *Curs: expunere, prelegere, conversatie*
- *Laborator: expunere, analiza comparativa, brainstorming, studiu de caz*
- *Proiect: expunere, analiza comparativa, brainstorming, studiu de caz*

E. PROCEDURA DE EVALUARE

Examen	Oral	Scris		Scris şi oral	
		elaborarea unei lucrări	tip grilă	scris	oral
nr.mediu de întrebări	-	**5**	**-**	-	-

Tipul de calificativ	Notă	Condiţia de acordare a notei 5	**Efectuarea completa a aplicaţiilor practice si realizarea a 50% răspunsuri corecte la partea scrisa**
	Admis/Respins	Condiţia de acordare a calificativului admis	**-**

Ponderea cu care activitatea din cursul semestrului intră în nota finală este de **33**% (in nota pentru activitatile aplicative intra cu ponderi egale nota la lucrarea de control – cu care se incheie partea de laborator - si nota pe proiect).

F. BIBLIOGRAFIE *Se indică minimum trei titluri bibliografice de referinţă dintre care, cel puţin unul, poate fi găsit în biblioteca UPT.*

	D.I. Curiac	Tehnici de securizare a datelor si programelor, Lito UPT, 2001
	D.I.Curiac	Algoritmi de criptare pentru securizarea datelor, Editura Orizonturi Universitare, 2001
	D.I.Curiac	Securitatea informatiei, Lito UPT, 2008

G.COMPATIBILITATE INTERNATIONALA

1. MIT - Network and Computer Security
http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/6-857Fall2003/CourseHome/index.htm
2. Stanford – Computer and Network Security http://crypto.stanford.edu/cs155/
3. Berkeley – Computer Security http://inst.eecs.berkeley.edu/~cs161/fa05/
4. lista cu cursuri pe tematica de securitate a informatiei din universitati americane dar si europene (peste 50 cursuri): http://avirubin.com/courses.html

Data: 04.04.2009

DIRECTOR/SEF DEPARTAMENT/CATEDRA
Prof.dr.ing. Ioan SILEA

TITULAR DE DISCIPLINĂ,
Prof.dr.ing. Daniel-Ioan CURIAC