

SYLABUS
pentru disciplina:

“SECURITATEA INFORMATIEI”

FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
DOMENIUL /SPECIALIZAREA INFORMATICĂ /INFORMATICĂ APLICATĂ -

Anul de studii: II

Semestrul 2

Titularul cursului: Prof.dr.ing. Curiac Daniel-Ioan Colaboratori: Prof.dr.ing.Curiac Daniel-Ioan					
Numar de ore/saptamana/Verificarea/Credite					
Curs	Seminar	Laborator	Proiect	Examinare	Credite
2	0	2	0	Examen	5

A. OBIECTIVELE CURSULUI

- însușirea de către studenți a tehnicilor moderne de securizare a datelor, cu precădere a securizării datelor prin criptare;
- prezentarea principalelor breșe în securitatea sistemelor de calcul cuplate în rețele LAN, sau prin dial-up, precum și a modului de realizare a protecției împotriva atacurilor asupra securității;

B. SUBIECTELE CURSULUI

Capitolul 1: Introducere(6 ore)

1.1 Securitatea datelor; 1.2 Aspecte legate de securitatea informației; 1.3 Servicii de securitate; 1.4 Modelul unei rețele sigure; 1.5 Atacuri; 1.6 Criptologia.

Capitolul 2: Criptarea convențională clasică (3 ore)

2.1 Modelul criptării convenționale; 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 semnături digitale

Capitolul 5: Studii de caz relativ la probleme de securitate în conducerea la distanță a proceselor industriale, rețele de senzori, etc. (2 ore)

C. SUBIECTELE APLICATIILOR (laborator – 7 lucrări a câte 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: Corelația alfabet&cuvint, Codificarea busola, Codificarea Pig Latin,
Lucrarea 3: Tabela Viginere, Tabela Porta, Codificări matrice,
Lucrarea 4: Coduri monoalfabetice, Mașini rotative, Codificare Pig Pen,
Lucrarea 5: Codificare tip harta, Diagraphic substitution.
- Realizarea și susținerea orală a unui referat asupra unui topic ce intervine în securizarea sistemelor (Firewalls, viruși informatici, Programe antivirus, Sistemul Kerberos, Sistemul SESAME, PGP/PEM, securitatea sistemelor incorporate, criptarea pe curbe eliptice, criptarea cuantică, etc.) - *Lucrarea 6 și 7*

- Proiectarea și implementarea într-unul din limbajele cunoscute (de preferință C, pentru a satisface necesitățile de viteză) a unui algoritm modern de criptare destinat unor sisteme precizate prin tema de proiectare: un exemplu – securizarea informației prin criptare în rețele de senzori: alegerea tipului de algoritm (cheie secretă/cheie publică); alegerea algoritmului în funcție de lungimea mesajelor schimbate de senzori, de durata de viață a mesajelor, etc.; implementarea în C; testarea. (proiect pe durata a 14 ore – 2 ore/săptămână)

D. BIBLIOGRAFIE *Se indică maximum trei titluri bibliografice de referință*

1.	D.I. Curiac	Tehnici de securizare a datelor și programelor, Lito UPT, 2001
2.	D.I. Curiac	Algoritmi de criptare pentru securizarea datelor, Editura Orizonturi Universitare, 2001
3.	D.I. Curiac	Securitatea informației, Lito UPT, 2007

E. PROCEDURA DE EVALUARE

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

Tipul de calificativ	Notă	Condiția de acordare a notei 5	Efectuarea completă a aplicațiilor practice și realizarea a 50% răspunsuri corecte la partea scrisă
	Admis/Respins	Condiția de acordare a calificativului admis	-

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

F. COMPATIBILITATE INTERNAȚIONALĂ

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 informației din universități americane dar și europene (peste 50 cursuri): <http://avirubin.com/courses.html>

Data: 08.04.2008

DIRECTOR/SEF DEPARTAMENT/CATEDRA
Conf.dr.ing. Ioan Silea

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