

FIȘA DISCIPLINEI

Denumirea disciplinei :		Compresia, Criptarea și Securitatea Datelor			
Codul disciplinei:		390457010612SO49			
Domeniul:		Calculatoare și Tehnologia Informației			
Specializarea:		Tehnologia Informației			
Catedra:		Calculatoare și Automatizări			
Facultatea:		Facultatea de Inginerie „Hermann Oberth”			
Universitatea:		Universitatea „Lucian Blaga” din Sibiu			
Anul de studiu:	4	Semestrul	7	Tipul de evaluare finală	Examen
Regimul disciplinei (DI=obligatorie/ DO=opțională/DF=liber aleasă):			DI	Numărul de credite:	5
Categoriza formativă a disciplinei (DF=fundamentală.; DI=ingineresci; DS=specialitate; DC=complementară)					DS
Total ore din planul de învățământ	4		Total ore pe semestru:	56	
Titularul disciplinei: conf. dr. ing. Macarie BREAZU					

Numărul total de ore (pe semestru) din planul de învățământ					
Total ore/ semestru	C	S	L	P	Total
	28	0	28	0	56

Obiective:	Cunoașterea de către studenți a metodelor consacrate de compresie, criptare și securitate a datelor și a soluțiilor impuse recent în domeniu, domeniu care a cunoscut o creștere explozivă odată cu dezvoltarea Internetului
Competențe specifice disciplinei	<p>1. Cunoaștere și înțelegere:</p> <ul style="list-style-type: none"> cunoașterea și înțelegerea principiilor generale ale disciplinei cunoașterea și operarea adecvată cu noțiunile specifice disciplinei dobândirea capacității de a integra cunoștințe dobândite la alte cursuri identificarea principalelor surse de informare <p>2. Explicare și interpretare:</p> <ul style="list-style-type: none"> analiza critică a modelelor teoretice, ideilor și a abordărilor consacrate aptitudini de realizare a unui proiect și a unui raport aferent familiarizarea cu munca în echipă <p>3. Instrumental – aplicative:</p> <ul style="list-style-type: none"> cunoașterea și stăpânirea mediilor de dezvoltare consacrate proiectarea pe diverse niveluri ale aplicațiilor utilizarea unei game variate de strategii, metode, tehnici de proiectare, implementare și evaluare

4. Atitudinale:

- renunțarea la atitudinea de dezinteres față de școală
- dobândirea unei atitudini pozitive față de activitatea de cercetare
- aprecierea muncii în echipă, responsabilizarea față de rezultatele echipei
- dobândirea unei atitudini pozitive față de (necesitatea validării aspectelor teoretice prin) aplicația practică
- conștientizarea necesității participării la propria dezvoltare profesională.

TEMATICA CURSURILOR		
Nr. crt.	Denumirea temei	Nr. ore
1	Introducere, modele generale, clasificări.	2
2	Elemente de teoria transmiterii informației și codării.	2
3	Compresie bazată pe modelare statistică: codare Shannon-Fano, codare Huffman statică și dinamică, codare aritmetică.	4
4	Compresie bazată pe modelare lingvistică: LZ77, LZ78, LZW	2
5	Codare bazată pe transformate, DCT, standarde de compresie a imaginilor JPEG și a secvențelor video MPEG.	4
6	Codare predictivă, DPCM, compresie cu pierderi controlate (near-lossless).	2
7	Criptografia computațională convențională (simetrică).	2
8	Criptografia computațională cu chei publice (asimetrică).	2
9	Securitatea transferului de date. Gestiunea cheilor de cifrare.	2
10	Autentificare, semnătură digitală,	2
11	Protecție și securitate la nivelul sistemului de operare	2
12	Aplicații: securitatea în Internet	2
TEMATICA LABORATOARELOR		
1	Introducere, codificare RLE, Formatul BinHex.	2
2	Codificare Shannon-Fano și Huffman static.	2
3	Codificare Huffman dinamic.	2
4	Codificare LZ77, LZ78, LZW.	2
5	Compresie de imagini bazată pe DCT - JPEG.	4
6	Compresie predictivă lossless și near-lossless.	4
7	Implementarea unui algoritm de criptare simetric.	2
8	Implementarea unui algoritm de criptare asimetric.	2
9	Implementarea unei scheme de criptare hibridă.	2
10	Implementarea semnăturii digitale folosind funcții hash și criptare cu cheie publică.	2
11	Instalarea protocolului SSL.	2
12	Configurarea unei aplicații de tip firewall.	2

Conținutul tematic (descriptori)

Metode de predare / seminarizare	Prelegeri, explicații, conversații, problematizări, demonstrații, studii de caz, exerciții, dezbateri
----------------------------------	---

Stabilirea notei finale (procentaje)	- răspunsurile la examen/colocviu (evaluare finală)	60%
	- teste pe parcursul semestrului	
	- răspunsurile finale la lucrările practice de laborator	20%
	- activități gen teme/referate/eseuri/traduceri/proiecte etc.	20%

	- teme de control	
	- alte activități(<i>precizați</i>).....	
	- TOTAL	100%

Evaluarea finală va cuprinde examen scris (subiecte descriptive și probleme).

Cerințe minime pentru nota 5
minim nota 5.00 la laborator/proiecte
minim nota 4.50 la examen

Cerințe pentru nota 10
medie ponderată note minim 9.50

TOTAL ore studiu individual (pe semestru) = 40

Bibliografia	<p>Minimală obligatorie:</p> <ol style="list-style-type: none"> Alexandru Spătaru - <i>Teoria transmisiunii informației</i> - Editura Didactică și Pedagogică, București, 1983 David Salomon, "<i>Data Compression: The Complete Reference</i>", Fourth Edition, ISBN 978-1846286025, Springer, 2006 Bruce Schneier, "<i>Applied Cryptography</i>", Second Edition, ISBN 0-471-11709-9, John Wiley & Sons, 1996 <p>Complementară:</p> <ol style="list-style-type: none"> Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "<i>Operating System Concepts</i>", ISBN 0-471-25060-0, John Wiley & Sons, 2003 Khalid Sayood, "<i>Introduction to Data Compression</i>", Third Edition, ISBN: 978-0126208627, Morgan Kaufmann, 2005
<p>Lista materialelor didactice utilizate în procesul de predare: note de curs, lista bibliografică, videoproiector, acces Internet</p>	

Coordonator de Disciplină	Grad didactic, titlul, prenume, numele	Semnătura
	Conf. dr. ing. Macarie BREAZU	