

FIȘA DISCIPLINEI¹⁾

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Petrol-Gaze din Ploiești
1.2. Facultatea	Inginerie Mecanică și Electrică
1.3. Departamentul	Automatică, Calculatoare și Electronică
1.4. Domeniul de studii universitare	Calculatoare și Tehnologia Informației
1.5. Ciclul de studii universitare	Licență
1.6. Programul de studii universitare	Calculatoare

2. Date despre disciplină

2.1. Denumirea disciplinei	Criptarea Informației
2.2. Titularul activităților de curs	Prof.univ.dr.ing. Otilia Cangea
2.3. Titularul activităților aplicative	Prof.univ.dr.ing. Otilia Cangea
2.4. Anul de studiu	IV
2.5. Semestrul *	8
2.6. Tipul de evaluare	E
2.7. Categoria formativă** / regimul*** disciplinei	S2/O

* numărul semestrului este conform planului de învățământ;

** fundamentală = F0; de domeniu = D1; de specialitate = S2; complementară = C3

*** obligatorie = O; opțională = A; facultativă = L

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Număr de ore pe săptămână	4	din care: 3.2. curs	2	3.3. Seminar/laborator	2
3.4. Total ore din planul de învățământ	40	din care: 3.5. curs	20	3.6. Seminar/laborator	20
3.7. Distribuția fondului de timp					ore
Studiu după manual, suport de curs, bibliografie și notițe					15
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					15
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					15
Tutoriat					
Examinări					15
Alte activități					
3.7. Total ore studiu individual	60				
3.8. Total ore pe semestru	100				
3.9. Numărul de credite	4				

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	➤ Transmisia Datelor
4.2. de competențe	➤

- 1) Adaptare după Ordinul Ministrului educației, cercetării, tineretului și sportului nr. 5 703/2011 privind implementarea Codului național al calificărilor din învățământul superior, publicat în Monitorul Oficial al României, partea I, nr.880 bis / 13.XII.2011

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	➤ Modalitate de predare convențională folosind suport de curs, cu interacțiune profesor-student și tehnici moderne multimedia
5.2. de desfășurare a seminarului/laboratorului	➤ Laborator dotat cu tehnică de calcul și mediu de programare C++

6. Competențe specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> ➤ Operarea cu metode și concepte moderne din știința sistemelor, a calculatoarelor, a tehnologiei informației și a comunicațiilor (CpS3) ➤ Dezvoltarea capacității de a interpreta și explica fundamentele teoretice ale tehnicilor și procedeele de criptare a informației (CpS1) ➤ Analiza și proiectarea sistemelor criptografice simulate prin tehnici software, în scopul aprecierii performanțelor (CpS4) ➤ Cunoașterea și utilizarea limbajelor, mediilor și tehnicilor de programare pentru implementarea software a algoritmilor de criptare a datelor (CpS4)
Competențe transversale	<ul style="list-style-type: none"> ➤ Manifestarea unei atitudini onorabile, responsabile, în concordanță cu statutul de student al specializării Calculatoare, față de importanța științifică a domeniului profesional (CtS1) ➤ Demonstrarea spiritului de integrare, de inițiativă și de identificare a problemelor și responsabilităților în cadrul unei echipe de lucru (CtS3) ➤ Capacitatea de a sesiza, înțelege și promova calitatea și creativitatea, pe baza informării și perfecționării continue (CtS6)

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1. Obiectivul general al disciplinei	➤ La sfârșitul cursului, studentul va fi capabil să dezvolte și să analizeze, în scopul îmbunătățirii performanțelor, aplicații software de simulare a criptării informației transmise
7.2. Obiectivele specifice	<p>La sfârșitul cursului, studentul va fi capabil să:</p> <ul style="list-style-type: none"> ➤ identifice și să aplice conceptele fundamentale ale criptării informației; ➤ analizeze și să evalueze sistemele criptografice simulate prin tehnici software; ➤ implementeze software algoritmi de criptare a informației în vederea asigurării confidențialității și securității datelor din rețelele de calculatoare; ➤ dezvolte aplicații complete a algoritmilor de criptare a datelor (tema de casă, proiect de licență)

8. Conținuturi

8.1. Curs	Nr.ore	Metode de predare	Observații
Introducere în criptografie	6	Interactivă și convențională, centrata pe student	Suport de curs în format tipărit și în
Criptosisteme clasice	4		

Criptosisteme computationale	6		format electronic, suport multimedia
Steganografia. Tehnici de marcare si verificare tip Digital Watermarking	4		
Bibliografie 1. Cangea, O., <i>Transmisia si criptarea datelor</i> , Editura MatrixRom, Bucuresti, 2008 2. Dobrescu, R. , <i>Transmiterea datelor</i> , Editura Academiei Romane, Bucuresti, 2005 3. Dobrescu, R., Kevorchian, S., <i>Criptarea și compresia datelor</i> , Editura Academiei Romane, Bucuresti, 2002 4. Howard, M., Le Blanc, D., <i>Writing Secure Code</i> , Microsoft Press, Redmond, WA, 2003			
8.2. Seminar / laborator/proiect	Nr. ore	Metode de predare	Observații
Studiul experimental al algoritmilor de criptare a datelor cu cheie simetrică - cifrul lui Caesar generalizat, transpozitia pe coloane, substitutia monoalfabetica	4	Clasica, centrata pe student si pe rezultatele invatarii	
Studiul experimental al algoritmilor de criptare a datelor cu cheie asimetrică. Algoritmul RSA. Semnatura digitala RSA	6		
Studiul experimental al algoritmilor de criptare a datelor cu cheie asimetrică – algoritmul El-Gamal, algoritmul Merkle-Hellman	6		
Protecția digitală a dreptului de proprietate în Internet folosind tehnici de marcare și verificare Digital Watermarking	4		
Bibliografie 1. Cangea, O., <i>Transmisia și criptarea datelor</i> , Editura MatrixRom, Bucuresti, 2008 2. Cangea, O., <i>Algoritmi de criptare pentru securitatea sistemelor informatice</i> , Editura Universității Petrol-Gaze din Ploiești, 2012			

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Conținuturile disciplinei sunt specifice domeniului dezvoltării tehnicilor de transmisie a informației codificate numeric, fiind coroborate cu așteptările comunității epistemice, ale asociațiilor profesionale si ale angajatorilor care activează in domeniu

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Examinare finala	Lucrare scrisa cu subiecte teoretice si aplicatii	40%
	Frecventa la curs	Tabel cu prezenta la curs	10%
10.5. Seminar/laborator/proiect	Activitate laborator si verificari periodice	Examinare orala si lucrare scrisa	30%
	Tema de laborator		20%
10.6. Standard minim de performanță			
<ul style="list-style-type: none">➤ Cunoasterea conceptelor fundamentale ale criptarii informatiei;➤ Simulare software functionala a algoritmilor de criptare studiatii.			

Data completării
20.09.2017

Semnătura titularului de curs

Semnătura titularului de seminar/laborator

Data avizării în departament

Semnătura directorului de departament