

FIȘA DISCIPLINEI¹⁾

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Petrol-Gaze din Ploiești
1.2. Facultatea	Litere și Științe
1.3. Departamentul	Informatică, Tehnologia Informației, Matematică și Fizică
1.4. Domeniul de studii universitare	Informatică
1.5. Ciclul de studii universitare	Master
1.6. Programul de studii universitare	Tehnologii Avansate pentru Prelucrarea Informației

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea informației
2.2. Titularul activităților de curs	Conferențiar dr. Moise Gabriela
2.3. Titularul activităților aplicative	Conferențiar dr. Constantinescu Zoran
2.4. Anul de studiu	I
2.5. Semestrul *	2
2.6. Tipul de evaluare	E
2.7. Categoria formativă** / regimul*** disciplinei	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	56	din care: 3.5. curs	28	3.6. Seminar/laborator	28
3.7. Distribuția fondului de timp					ore
Studiu după manual, suport de curs, bibliografie și notițe					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					45
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					50
Tutoriat					0
Examinări					19
Alte activități					0
3.7. Total ore studiu individual	144				
3.8. Total ore pe semestru	200				
3.9. Numărul de credite	8				

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	➤ Programare procedurala avansata, Algoritmi și structuri de date, Algebră
4.2. de competențe	➤ Limbaje de programare, elemente de teoria numerelor

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	• sală de curs multimedia necesară pentru realizare de expuneri, studii de caz, conversații, dezbateri
5.2. de desfășurare a	• sală de laborator echipată cu rețea de calculatoare

6. Competențe specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> ➤ Dobândirea cunoștințelor fundamentale, teoretice și practice, despre dezvoltarea de aplicații specifice și infrastructurile performante pentru prelucrarea acestora; ➤ Dobândirea cunoștințelor fundamentale, teoretice și practice în domeniul securității informației (algoritmi de criptare, sisteme și protocoale criptografice); ➤ Capacitatea de a participa la proiecte de dezvoltare de aplicații și instrumente informatice/software, respectiv de proiecte care implică folosirea acestora în cadrul unor sisteme complexe, tehnice sau socio-tehnice.
Competențe transversale	<ul style="list-style-type: none"> ➤ Folosirea eficientă a vocabularului profesional și a limbajului specific în domeniul securității informatice pentru prezentarea convingătoare a cunoștințelor, abilităților și valorilor proprii; ➤ Respectarea unei etici profesionale solide, adecvate societății moderne, ca bază a dezvoltării profesionale și personale în concordanță cu cerințele societății noastre dinamice; ➤ Capacitatea de a desfășura activități profesionale într-un cadru organizat, în mod eficient, cu responsabilitate, în conformitate cu codul de etică și practică profesională, pentru a rezolva probleme concrete prin transpunerea în practică a cunoștințelor, abilităților și valorilor dobândite pe parcursul programului de master; ➤ Dezvoltarea capacităților de integrare a cunoștințelor, abilităților și valorilor dobândite pe parcursul programului de masterat pentru o inserție rapidă pe piața muncii din domeniu, dar și pentru construirea unei cariere solide și care să ofere împlinire profesională; ➤ Conștientizarea impactului social, economic și moral al informaticii în societatea noastră bazată pe informație și cunoaștere, precum și a implicațiilor etice ale dezvoltării și utilizării sistemelor, aplicațiilor și instrumentelor informatice.

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

7.1. Obiectivul general al disciplinei	Formarea de competențe profesionale și transversale necesare obținerii calificării. Obiectivul principal al disciplinei constă în însușirea și înțelegerea tehnicilor și algoritmilor de criptare, primitivelor criptografice, protocoalelor criptografice, identificarea vulnerabilităților sistemelor de securitate, realizarea de comparații între diferite cifruri.
7.2. Obiectivele specifice	Formarea următoarelor competențelor profesionale și transversale. După parcurgerea disciplinei studenții vor putea să: <ul style="list-style-type: none"> • definească criptarea, criptografia, algoritmi de criptare, protocoale criptografice, identifice problemele din sistemele de securitate • descrie tehnici de criptare • clasifice algoritmi de criptare • clasifice și compare tehnici de criptare • modifice algoritmi de criptare

8. Conținuturi

8.1. Curs	Nr.ore	Metode de predare	Observații
1. Introducere în criptografie și securitatea datelor	1. 2 2. 2	Prelegerea, dezbatere, cercetarea documentelor	
2. Criptografie simetrică	3. 2		
3. Funcții Hash	4. 2		
	5. 4		

4. Cifruri de tip stream	6. 3		
5. Cifruri de tip bloc	7. 2		
6. Cifrul DES	8. 3		
7. Cifrul AES	9. 2		
8. Criptarea cu chei publice	10. 2		
9. Criptosistemul RSA	11. 4		
10. Managementul cheilor de criptare			
11. Semnături digitale			

Bibliografie

Atanasiu, A., Cursul de criptografie, www.galaxzng.com/adrian_atanasiu/cript.htm
Kessler G., C., An overview of Cryptography, 2018, www.garykessler.net/library/crypto.html
Paar, Christof and Pelzl, Jan, Understanding Cryptography, A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010.
Menezes, Alfred, van Oorschot, Paul and Vanstone, Scott - Handbook of Applied Cryptography, 2001.
Constantinescu Zoran, Moise Gabriela, Criptarea informației - ghid practic, Ed. Universității Petrol-Gaze din Ploiești, 2013.

8.2. Seminar / laborator/proiect	Nr. ore	Metode de predare	Observații
1. Sistemul Cezar, Vigenere – aplicații	8 8	Prelegere, expunere, exemplificare, exerciții.	
2. Sisteme de criptare de tip stream (RC4) – aplicații	12		
3. Sistemul de criptare DES, AES - aplicații			

Bibliografie

Atanasiu, A., Cursul de criptografie, www.galaxzng.com/adrian_atanasiu/cript.htm
Kessler G., C., An overview of Cryptography, 2018, www.garykessler.net/library/crypto.html
Paar, Christof and Pelzl, Jan, Understanding Cryptography, A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010.
Menezes, Alfred, van Oorschot, Paul and Vanstone, Scott - Handbook of Applied Cryptography, 2001.
Constantinescu Zoran, Moise Gabriela, Criptarea informației - ghid practic, Ed. Universității Petrol-Gaze din Ploiești, 2013.

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

- Cursul și seminarul sunt astfel concepute încât, prin competențele formate, să răspundă cerințelor pieței muncii. Ocupațiile absolvenților sunt cele din COR.
- Cursul respecta recomandările IEEE și ACM legate de Curricula pentru specializarea Informatică.

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Calitatea răspunsurilor, coerența argumentării, calitatea corelațiilor, etc.	Proba scrisă	45%

	Se urmărește completitudinea și corectitudinea cunoștințelor acumulate, capacitatea de sinteză a cunoștințelor, grad de asimilarea a limbajului de specialitate		
10.5. Seminar/laborator/ proiect	Participarea la activitățile de laborator prin realizarea temelor propuse. Se urmărește capacitatea de aplicare în practică a cunoștințelor predate, capacitatea de a implementa tehnici de criptare.	Realizarea temelor de laborator	45%
			Din oficiu 10%
Pentru promovarea examenului este necesară obținerea notei 5 pentru fiecare probă (curs și laborator).			
10.6. Standard minim de performanță			
<ul style="list-style-type: none"> ➤ Definirea corectă a termenilor din domeniul criptării, explicarea schemelor de criptare simetrică și asimetrică. ➤ Realizarea temelor de laborator. 			

Data completării

Semnătura titularului de curs

Semnătura titularului de laborator

Conf. dr. Gabriela Moise

Conf. dr. Zoran Constantinescu

Data avizării în departament

Semnătura directorului de departament

Conf. dr. Gabriela Moise