

FIȘA DISCIPLINEI ¹⁾

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	Licență
1.6. Programul de studii universitare	Informatică

2. Date despre disciplină

2.1. Denumirea disciplinei	Criptografie și securitatea informației
2.2. Titularul activităților de curs	Conferențiar dr. Moise Gabriela
2.3. Titularul activităților aplicative	Inf. Georgiana Bărbuceanu
2.4. Anul de studiu	III
2.5. Semestrul *	5
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:	2	3.3. Seminar/laborator	2	3.4. Proiect	-
		3.2. curs					
3.5. Total ore din planul de învățământ	56	din care:	28	3.7. Seminar/laborator	28	3.8. Proiect	-
		3.6. curs					
3.9. Distribuția fondului de timp							ore
Studiu după manual, suport de curs, bibliografie și notițe							27
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren							15
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri							27
Tutoriat							0
Examinări							0
Alte activități							0
3.10. Total ore studiu individual	69						
3.11. Total ore pe semestru	125						
3.12. Numărul de credite	5						

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	➤ Fundamentele programării, Fundamente matematice pentru informatică
4.2. de competențe	➤ Programare

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	<ul style="list-style-type: none"> sală de curs multimedia necesară pentru realizare de expuneri, studii de caz, conversații, dezbateri, platforme online de predare și server pentru resurse educaționale
5.2. de desfășurare a seminarului/laboratorului	<ul style="list-style-type: none"> sală de laborator echipată cu rețea de calculatoare, platforme online de predare și server pentru resurse educaționale

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 integrarea cunoștințelor, abilităților și valorilor dobândite pe parcursul programului de licență 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..
7.2. Obiectivele specifice	Formarea următoarelor competențelor profesionale și transversale. După parcurgerea disciplinei studenții vor putea să: <ul style="list-style-type: none"> • definească termeni specifici criptării și securității informației, explice algoritmi de criptare, protocoale criptografice, să identifice probleme de securitate • descrie tehnici de criptare • clasifice algoritmi de criptare

8. Conținuturi

8.1. Curs	Nr.ore	Metode de predare	Observații
<ol style="list-style-type: none"> 1. Introducere în criptografie și securitatea datelor 2. Criptografie simetrică (Cifrul Caesar, Cifrul afin, Cifrul Vigenere) 3. Cifruri stream 4. One-Time Pads 5. Cifuri bloc 6. Cifrul DES 7. Cifrul DES 8. Cifrul AES 9. Funcții Hash 10. Criptarea cu chei publice 11. RSA 12. Managementul cheilor de criptare 13. Semnături digitale 14. Recapitulări, sinteze, subiecte examen 	14*2	Prelegerea, dezbateri, cercetarea documentelor	
Bibliografie 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. Trappe W., Washington L.C., Introduction to Cryptography with Coding Theory, Pearson Education, 2006. Resurse educaționale https://timf.upg-ploiesti.ro/www/resurse/			
8.2. Seminar / laborator/proiect	Nr. ore	Metode de predare	Observații
<ol style="list-style-type: none"> 1. Explicarea conceptelor, schemelor prezentate la curs. 2. Implementare algoritmi de criptare: 	1-4h, 2-9-2h, 10-4h, 11-4h Total 28h	Prelegere, expunere, exemplificare, exerciții	

Algoritmul Square and multiply, 3. Algoritmul lui Euclid/Euclid extins, 4. Cifrul Caesar, 5. Cifrul afin, 6. Cifrul Vigenere, 7. Cifrul de substitutie, 8. Cifrul Hill, 9. LFSR, 10. Atacuri asupra cifrurilor (la alegere unul din cifruri: Caesar, afin, Vigenere, substitutie, Hill), Cifrul DES, Cifrul RSA 11. Prezentare teme			
---	--	--	--

Bibliografie

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.
 Trappe W., Washington L.C., Introduction to Cryptography with Coding Theory, Pearson Education, 2006.
 Resurse educaționale <https://timf.upg-ploiesti.ro/www/resurse/>

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 pentru programele de studiu din domeniul 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. Se urmărește completitudinea și corectitudinea cunoștințelor acumulate, capacitatea de sinteză a cunoștințelor, grad de asimilarea a limbajului de specialitate	Proba scrisa Prezentare un subiect CSI în timpul orelor de curs	30% (1 pct din oficiu) 20% (1 pct din oficiu)
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.	Realizare și prezentare teme de laborator	50 % (1 pct din oficiu)

Pentru promovarea examenului este necesară obținerea notei 5 pentru fiecare probă (atât curs cât și laborator).

10.6. Standard minim de performanță

- Definirea corectă a termenilor din domeniul criptării, explicarea schemelor de criptare simetrică și asimetrică.
- Realizarea temelor de laborator (de minim nota 5)

Data completării
13 septembrie 2021

Semnătura titularului de curs
Conf. dr. Gabriela Moise

Semnătura titularului de seminar/laborator
Inf. Georgiana Bărbuceanu

Data avizării în departament
16 septembrie 2021

Semnătura directorului de departament
Conf. dr. Gabriela Moise