F I Ş A D I S C I P L I N E I [1)]

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea Petrol-Gaze din Ploiești
1.2. Facultatea	Litere și Științe
1.3. Departamentul	Informatică, Tehnologia Informaţiei, Matematică şi Fizică
1.4. Domeniul de studii universitare	Informatică
1.5. Ciclul de studii universitare	Licenţă
1.6. Programul de studii universitare	Informatică

2. Date despre disciplină

2.1. Denumirea disciplinei	Criptografie şi securitatea informaţiei
2.2. Titularul activităţilor de curs	Conferenţiar dr. Moise Gabriela
2.3. Titularul activităţilor aplicative	Conferenţiar dr. Moise Gabriela
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 învăţământ; **DF - Discipline fundamentale; DD - discipline de domeniu; DS - discipline de specialitate; DC - discipline complementare, DA - disciplina de aprofundare, DSI- disciplina de sinteza. ***obligatorie = O; opţională = A; facultativă = L

3. Timpul total estimat (ore pe semestru al activităţilor 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 învăţământ	56	din care: 3.5. curs	28	3.6. Seminar/laborator	28

3.7. Distribuţia fondului de timp	ore
Studiu după manual, suport de curs, bibliografie şi notiţe	30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	19
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	20
Tutoriat	0
Examinări	0
Alte activităţi	0

3.7. Total ore studiu individual	69
3.8. Total ore pe semestru	175
3.9. Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	➢ Programare, Algebră
4.2. de competenţe	➢ Limbaje de programare, elemente de teoria numerelor

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• sală de curs multimedia necesară pentru realizare de expuneri, studii de caz, conversaţii, dezbateri
5.2. de desfăşurare a seminarului/laboratorului	• sală de laborator echipată cu reţea de calculatoare

6. Competenţe specifice acumulate

Competenţe profesionale	➢ Dobândirea cunoştinţelor fundamentale, teoretice şi practice, despre dezvoltarea de aplicaţii specifice și infrastructurile performante pentru prelucrarea acestora; ➢ Dobândirea cunoştinţelor fundamentale, teoretice şi practice în domeniul securităţii informaţiei (algoritmi de criptare, sisteme și protocoale criptografice); ➢ Capacitatea de a participa la proiecte de dezvoltare de aplicaţii şi instrumente informatice/software, respectiv de proiecte care implică folosirea acestora în cadrul unor sisteme complexe, tehnice sau socio-tehnice.

Competenţe transversale	➢ Folosirea eficientă a vocabularului profesional şi a limbajului specific în domeniul securitatii informatice pentru prezentarea convingătoare a cunoştinţelor, abilităţilor şi valorilor proprii; ➢ Respectarea unei etici profesionale solide, adecvate societăţii moderne, ca bază a dezvoltării profesionale și personale în concordanță cu cerinţele societăţii noastre dinamice; ➢ Capacitatea de a desfăşura activităţi profesionale într-un cadru organizat, în mod eficient, cu responsabilitate, în conformitate cu codul de etică şi practică profesională, pentru a rezolva probleme concrete prin transpunerea în practică a cunoştinţelor, abilităţilor şi valorilor dobândite pe parcursul programului de master; ➢ Dezvoltarea capacităţilor de integrarea cunoştinţelor, abilităţilor şi valorilor dobândite pe parcursul programului de masterat pentru o inserţie rapidă pe piaţa muncii din domeniu, dar şi pentru construirea unei cariere solide şi care să ofere împlinire profesională; ➢ Conştientizarea impactului social, economic şi moral al informaticii în societatea noastră bazată pe informaţie şi cunoaştere, precum şi a implicaţiilor etice ale dezvoltarii şi utilizării sistemelor, aplicaţiilor şi instrumentelor informatice.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1. Obiectivul general al disciplinei	Formarea de competențe prefesionale și transverale 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 studenţii vor putea să: • definească criptarea, criptografia, algoritmi de criptare, protocoale criptografice, identifice problemele din sistemele de securitate • descrie tehnici de criptare • clasifice algoritmi de criptare

8. Conţinuturi

8.1. Curs	Nr.ore	Metode de predare	Observaţii
1. Introducere în criptografie si securitatea datelor 2. Criptografie simetrica (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. Functii Hash 10. Criptarea cu chei publice 11. RSA 12. Managementul cheilor de criptare 13. Semnaturi digitale 14. Recapitulari, sinteze, subiecte examen	14*2	Prelegerea, dezbatere, 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 Oorchot, Paul and Vanstone, Scott - Handbook of Applied Cryptography, 2001.
Constantinescu Zoran, Moise Gabriela, Criptarea informației - ghid practic, Ed. Universităţii Petrol-Gaze din Ploieşti, 2013.
Trappe W., Washington L.C., Introduction to Cryptography with Coding Theory, Pearson Education, 2006.

8.2. Seminar / laborator/proiect	Nr. ore	Metode de predare	Observaţii
Repetarea conceptelor, explicare schemelor prezentate la curs, Programarea algoritmilor criptografici Lista algoritmilor abordate: Algoritmul Square and multiply, Algoritmul lui Euclid/Euclid extins, Cifrul Caesar, Cifrul afin, Cifrul Vigenere, Cifrul de substitutie, Cifrul Hill, LFSR, Atacuri asupra cifrurilor (la alegere unul din cifruri: Caesar, afin, Vigenere, substitutie, Hill), Cifrul DES, Cifrul RSA	28	Prelegere, expunere, exemplificare, exerciţii.	

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 Oorchot, Paul and Vanstone, Scott - Handbook of Applied Cryptography, 2001.
Constantinescu Zoran, Moise Gabriela, Criptarea informației - ghid practic, Ed. Universităţii Petrol-Gaze din Ploieşti, 2013.
Trappe W., Washington L.C., Introduction to Cryptography with Coding Theory, Pearson Education, 2006.

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţilor profesionale şi 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.
- Conţinuturile disciplinei corespund cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului.
- Disciplina respectă recomandările IEEE şi ACM legate de conținuturile programelor de studii de licență 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 urmăreşte completitudinea și corectitudinea cunoștințelor acumulate, capacitatea de sinteză a cunoștințelor, grad de asimilarea a limbajului de specialitate	Proba scrisa	50% (1 pct din oficiu)
10.5. Seminar/laborator/ proiect	Participarea la activitățile de laborator prin realizarea temelor propuse. Se urmăreşte capacitatea de	Realizarea temelor de laborator	50% (1 pct din oficiu)

	aplicare în practică a cunoștințelor predate, capacitatea de a implementa tehnici de criptare.		
Pentru promovarea examenului este necesară obţinerea notei 5 pentru fiecare probă (atât curs cât şi laborator).			
10.6. Standard minim de performanţă			
➢ Definirea corectă a termenilor din domeniul criptării, explicarea schemelor de criptare simetrică şi asimetrică. ➢ Realizarea temelor de laborator (de minim nota 5)			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar/laborator
21 septembrie 2020	Conf. dr. Gabriela Moise	Conf. dr. Gabriela Moise

Data avizării în departament
21 septembrie 2020

Semnătura directorului de departament

Conf. dr. Gabriela Moise