# F I Ş A  D I S C I P L I N E I

## 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 | Criptografie si securitate informationala |
| 2.2. Titularul activităților de curs | Prof.univ.dr.ing. Otilia Cangea |
| 2.3. Titularul activităților seminar/laborator | Prof.univ.dr.ing. Otilia Cangea<br>Drd. Ing. POTECĂ Luiza-Alexandra |
| 2.4. Titularul activității proiect | |
| 2.5. Anul de studiu | IV |
| 2.6. Semestrul * | 8 |
| 2.7. Tipul de evaluare | Examen |
| 2.8. Categoria formativă** / regimul*** disciplinei | DS/DOB |

* numărul semestrului este conform planului de învățământ;

** DF - Discipline fundamentale; DS - discipline de specializare; DC - discipline complementare

*** obligatorie/impusă = DOB; opțională = DOP; facultativă = DFA

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3.1. Număr de ore pe săptămână | 5 | din care: 3.2. curs | 3 | 3.3. Seminar/laborator | 2 | 3.4. Proiect | |
| 3.5. Total ore din planul de învățământ | 70 | din care: 3.6. curs | 42 | 3.7. Seminar/laborator | 28 | 3.8. Proiect | |
| 3. 9. Total ore studiu individual (studiu după suport de curs, bibliografie și notițe, documentare suplimentară în bibliotecă, pe platformele electronice de specialitate, pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri) | | | | | | | 55 |
| 3.10. Total ore pe semestru | | | | | | | 125 |
| 3.11. Numărul de credite | | | | | | | 5 |

## 4. Condiții (acolo unde este cazul)

| | |
|---|---|
| 4.1. de curriculum | ➢ Securitatea datelor |
| 4.2. de desfășurare a cursului | ➢ Sală cu dotări multimedia (proiector) |
| 4.3. de desfășurare a seminarului/laboratorului | ➢ Laborator dotat cu tehnică de calcul şi mediu de programare C++ |

## 5. Competențe specifice acumulate și rezultatele învățării* care stau la baza acestora

| Competențe profesionale | Rezultatele învățării* |
|---|---|
| 1. Operarea cu fundamente ştiințifice, ingineresti şi ale tehnologiei informației. | **C1 -** Studentul/absolventul identifică și descrie concepte, principii și metode de bază din matematică, fizică și informatică.<br>**A1** - Studentul/absolventul analizează sistemele utilizând teoriile studiate și proiectează, implementează, diagnostichează și depanează sisteme digitale.<br>**RA1 -** Studentul/absolventul selectează și utilizează surse bibliografice specifice domeniului. |

| | |
|---|---|
| 2. Soluționarea problemelor folosind instrumentele ştiinței şi ingineriei calculatoarelor | **C1** - Studentul/absolventul descrie, identifică, sumarizează concepte și metode elementare privitoare la limbaje de programare, medii de programare, tehnici de programare, baze de date, inteligență artificială și inginerie software și modul lor de aplicare în probleme concrete.<br>**A1** - Studentul/absolventul alege şi explică concepte proprii specifice proiectării algoritmilor, programării orientate pe obiecte, programării logice și funcționale.<br>**RA1** - Studentul/absolventul are o comportare onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei.<br>**RA2 -** Studentul/absolventul selectează și utilizează surse bibliografice specifice domeniului. |
| 3. Proiectarea, gestionarea ciclului de viață şi integrarea sistemelor informatice utilizând tehnologii şi medii de programare | **C1 -** Studentul/absolventul identifică, descrie si sumarizează concepte și metode elementare privitoare la limbaje de programare, medii de programare, tehnici de programare, baze de date, inteligență artificială și inginerie software și modul lor de aplicare.<br>**A1 -** Studentul/absolventul elaborează specificații și proiectează sisteme informatice folosind metode şi instrumente specifice.<br>**RA1 –** Studentul/absolventul arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională. |
| 4. Dezvoltarea de aplicații specifice de asigurare a securității informațiilor si a sistemelor informatice | **C1 -** Studentul/absolventul aprofundează cunoașterea tehnologiilor de securitate a informațiilor, a terminologiilor legate de utilizarea acestora, a cunoștințelor teoretice si practice care stau la baza acestora<br>**C2** – Studentul/absolventul cunoaște si interpretează evenimentele posibile, vulnerabilitățile și amenințările legate de aceste evenimente, a probabilităților de apariție și a pagubelor posibile și a controalelor de securitatea informației ce pot fi aplicate.<br>**A1** – Studentul/absolventul propune controale și măsuri pentru evenimente de securitatea informației produse de agenți necunoscuți (exploatarea unor vulnerabilități nedocumentate).<br>**A2** – Studentul/absolventul are abilitatea de a desfășura evaluări de risc, cu propunerea de controale de securitate de toate tipurile pentru limitarea probabilităților de exploatare a vulnerabilităților identificate și a efectelor previzionate.<br>**RA1** – Studentul/absolventul are o comportare onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei. |
| **Competențe transversale** | **Rezultatele învățării*** |
| 1. Aplicarea, in mod responsabil, a principiilor, normelor și valorilor eticii profesionale in realizarea sarcinilor profesionale si identificarea obiectivelor de realizat, a resurselor disponibile, a etapelor de lucru, a duratelor de execuție, a termenelor de realizare aferente și a riscurilor aferente. | **C1** - Studentul/absolventul descrie, identifică și sumarizează concepte fundamentale din știința calculatoarelor și tehnologia informației și modul lor de aplicare în probleme concrete.<br>**A1** - Studentul/absolventul specifică cerințe, elaborează scenarii de simulare, propune soluții de rezolvare a unor probleme de control, analizează și evaluează performanțele sistemelor informatice.<br>**RA1** - Studentul/absolventul are o comportare onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei.<br>**RA2 -** Studentul/absolventul aplică valorile eticii și deontologiei profesiei de inginer. |
| 2. Identificarea rolurilor și responsabilităților într-o echipă pluridisciplinară și aplicarea de tehnici de relaționare în munca în cadrul echipei. | **C1** - Studentul/absolventul descrie, identifică și sumarizează concepte fundamentale din sisteme automate, sisteme încorporate și inteligente, știința calculatoarelor și tehnologia informației și modul lor de aplicare în probleme concrete.<br>**A1** - Studentul/absolventul aplică tehnici moderne de management de proiect și de luare a deciziilor, inclusiv într-un cadru multidisciplinar. |

| | |
|---|---|
| | **RA1** - Studentul/absolventul derulează procese din managementul proiectelor specifice domeniului calculatoare si tehnologia informației, cu preluarea diferitelor roluri în echipă și descrierea clară și concisă, verbal și în scris, a rezultatelor.<br>**RA2 -** Studentul/absolventul lucrează eficient ca membru în echipă sau lider al acesteia. |
| 3. Identificarea oportunităților de formare continua și utilizarea eficientă pentru propria dezvoltare a surselor informaționale și a resurselor de comunicare și formare profesionala asistata de calculator (portaluri Internet, aplicații software de specialitate, baze de date, cursuri on-line) atât în limba romana, cât și într-o limbă de circulație internațională. | **C1** - Studentul/absolventul explică și interpretează rezultate teoretice și experimentale, documentație tehnică, fenomene și procese din domeniul calculatoare si tehnologia informației.<br>**A1** - Studentul/absolventul realizează responsabil proiecte pentru rezolvarea unor probleme specifice domeniului, cu evaluarea corecta a volumului de lucru, a resurselor disponibile, a timpului necesar de finalizare și a riscurilor, în condiții de aplicare a normelor deontologice și de etica profesionala in domeniu, precum și de securitate și sănătate in muncă.<br>**RA1** - Studentul/absolventul arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.<br>**RA3 -** Studentul/absolventul este angajat în învățarea pe tot parcursul vieții pentru dobândirea și implementarea cunoștințelor, după cum este necesar, folosind strategii de învățare adecvate. |

***** C – cunoștințe; A – aptitudini; RA – responsabilitate și autonomie.

## 6. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

| | |
|---|---|
| 6.1. Obiectivul general al disciplinei | ➢ La sfârşitul cursului, studentul va fi capabil să dezvolte si să analizeze aplicații software de implementare a algoritmilor de criptare a informației in scopul asigurării securității transmisiei |
| 6.2. Obiectivele specifice | La sfârşitul cursului, studentul va fi capabil să:<br>➢ identifice si să aplice conceptele fundamentale ale criptării informației;<br>➢ analizeze si să evalueze sistemele criptografice simulate prin tehnici software;<br>➢ implementeze software algoritmii de criptare a informației in vederea asigurării confidențialității si securității datelor din rețelele de calculatoare;<br>➢ dezvolte aplicații complete a algoritmilor de criptare a datelor (tema de casă, proiect de licență) |

## 7. Conținuturi

| **7.1. Curs** | Nr. ore | Metode de predare | Observații |
|---|---|---|---|
| Introducere in criptografie | 4 | Clasica, centrata pe student și pe rezultatele invățării | Suport de curs in format tiparit si in format electronic, suport multimedia |
| Criptosisteme clasice | 4 | | |
| Criptosisteme computaționale (RSA, Merkle-Helmann, Menezes-Vanstone) | 6 | | |
| Criptarea pe curbe eliptice | 6 | | |
| Sisteme de criptare fluida (Cifruri fluide, cifrul OTP-Vernam) | 6 | | |
| Criptare hibrida (sisteme criptografice, infrastructura sistemelor criptografice hibride) | 6 | | |
| Chei criptografice. Ciclul de viață al unei chei | 6 | | |
| Managementul distribuit al cheilor | 4 | | |

Bibliografie


1. Cangea, O., *Criptografie şi securitate informaţională*, Editura Universităţii Petrol-Gaze din Ploieşti, 2022
2. Cangea, O., *Transmisia si criptarea datelor,* Editura MatrixRom, Bucuresti, 2008
3. Dobrescu, R. , *Transmiterea datelor*, Editura Academiei Romane, Bucuresti, 2005
4. Dobrescu, R., Kevorchian, S., *Criptarea şi compresia datelor,* Editura Academiei Romane, Bucuresti, 2002
5. Howard, M., Le Blanc, D., *Writing Secure Code*, Microsoft Press, Redmond, WA, 2003


| **7.2. Seminar / laborator** | Nr. ore | Metode de predare | Observații |
|---|---|---|---|
| Criptosisteme clasice - cifrul lui Caesar generalizat, transpozitia pe coloane, substitutia monoalfabetica | 4 | Clasica, centrata pe student si pe rezultatele invatarii | |
| Algoritmi computationali de criptare a datelor 1 - algoritmul RSA, semnatura digitala RSA | 4 | | |
| Algoritmi computationali de criptare a datelor 2– algoritmul El-Gamal, algoritmul Merkle-Hellman | 6 | | |
| Criptare pe curbe eliptice | 4 | | |
| Algoritmi de criptare fluida | 4 | | |
| Aplicatie pentru managementul distribuit al cheilor criptografice. Pachetul software PGP. | 6 | | |

Bibliografie


1. Cangea, O., *Criptografie si securitate informationala*, Editura Universităţii Petrol-Gaze din Ploieşti, 2022.
2. Cangea, O., *Transmisia şi criptarea datelor,* Editura MatrixRom, Bucuresti, 2008
3. Cangea, O., *Algoritmi de criptare pentru securitatea sistemelor informatice ,* Editura Universităţii Petrol-Gaze din Ploieşti, 2012
4. Bernard John Poole, *Pretty Good Privacy - Downloading, Installing, Setting Up, and Using this Encryption Software. A Tutorial for Beginners to PGP*, disponibil la http://www.pitt.edu/~poole/PGP.htm


| **7.3. Proiect** | Nr. ore | Metode de predare | Observații |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

Bibliografie

## 8. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociaților profesionale și angajatori reprezentativi din domeniul aferent programului

- Conţinuturile disciplinei sunt specifice domeniului dezvoltării tehnicilor de transmisie a informaţiei codificate, fiind coroborate cu aşteptările comunităţii epistemice, ale asociaţiilor profesionale si ale angajatorilor care activează in domeniu

## 9. Evaluare

| Tip activitate | 9.1. Criterii de evaluare | 9.2. Metode de evaluare | 9.3. Pondere din nota finală |
|---|---|---|---|
| 9.4. Curs | Examinare finală | Lucrare scrisă cu subiecte teoretice si aplicaţii | 50% |

| | | | |
|---|---|---|---|
| | Prezenta la curs | Cuantificarea in nota a numărului de prezenţe la curs | 10% |
| 9.5. Seminar/laborator | Activitate laborator si verificări periodice | Examinare orală si lucrare scrisă laborator | 40% |
| | | | |
| 9.6. Proiect | | | |
| | | | |
| 9.7. Standard minim de performanță | | | |
| ➢ Cunoasterea conceptelor fumdamentale ale criptării datelor si securităţii informaţiei<br>➢ Simulare software funcţională a algoritmilor de criptare studiaţi. | | | |

| Data completării | Semnătura titularului de curs | Semnătura titularului de seminar/laborator | Semnătura titularului de proiect |
|---|---|---|---|
| 20.09.2025 | | | _____ |
| Data avizării în departament | Director de departament<br>*Conf. dr. ing. Pricop Emil* | | Decan<br>*Conf. dr. ing. Bădicioiu Marius* |
| 26.09.2025 | | | |