



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Națională de Știință și Tehnologie Politehnica București
1.2 Facultatea	Electronică, Telecomunicații și Tehnologia Informației
1.3 Departamentul	Telecomunicații
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
1.5 Ciclu de studii	Licență
1.6 Specializarea	Tehnologii și Sisteme de Telecomunicații

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)	Bazele criptologiei 2						
2.2 Titularul activităților de curs	Colaborator Dr. Adriana Clim						
2.3 Titularul activităților de seminar / laborator	Colaborator Dr. Gabriel Negara						
2.4 Anul de studiu	4	2.5 Semestrul	1	2.6 Tipul de evaluare	V	2.7 Regimul disciplinei	Op
2.8 Tipul disciplinei	S	2.9 Codul disciplinei	04.S.07.A.222	2.10 Tipul de notare	Nota		

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

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					20
Tutorat					5
Examinări					6
Alte activități (dacă există):					2
3.7 Total ore studiu individual	33.00				
3.8 Total ore pe semestru	75				
3.9 Numărul de credite	3				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Cunostinte de algebra superioara si teria numerelor.
4.2 de rezultate ale învățării	Cunoasterea unui limbaj de programare.

5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)

5.1 Curs	De preferat, participare la BC1 sau cunostinte de criptologie clasica.
5.2 Seminar/ Laborator/Proiect	Prezența obligatorie la laboratoare.



6. Obiectiv general (Se referă la intențiile profesorilor pentru studenți, la ceea ce studenții vor fi învățați în timpul cursului. Oferă o orientare cu privire la locul cursului în cadrul domeniului științific abordat, precum și la rolul pe care acesta îl are în cadrul specializării studiate. Vor fi descrise de o manieră generală tematicile abordate, justificarea includerii cursului în planul de învățământ al specializării studiate etc.)

Disciplina asigură însușirea cunoștințelor de bază din domeniul criptologiei moderne: însușirea conceptelor de criptologie simetrică și asimetrică, însușirea conceptelor de securitate informatică și de evaluare a nivelului de securitate.

Însușirea practică a noțiunilor predate la curs, prin implementarea de programe software în limbajul C#; rezolvarea unor probleme practice concrete care includ aspecte legate de securitatea datelor și verificarea /validarea nivelului de securitate al sistemului.

7. Competențe (Capacitatea dovedită de a utiliza cunoștințe, aptitudini și abilități personale, sociale și/sau metodologice în situații de muncă sau de studiu și pentru dezvoltarea profesională și personală. Reflectă cerințele angajatorilor.)

Specifice	Crearea abilităților de a aplica cunoștințe generale de matematici fundamentale și de algoritmică în analiza rezistenței sistemelor criptografice moderne. Posibilitatea de a realiza aplicații software care implementează atacuri asupra sistemelor criptografice. Dezvoltarea calitatilor necesare evaluării nivelului de securitate (din perspectiva criptografică) oferit de un sistem sau de o componentă a acestuia.
Transversale (generale)	Cresterea capacității de a analiza obiectiv nivelul de securitate oferit de un sistem.

8. Rezultatele învățării (Sunt enunțuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învățării reflectă realizările studentului și mai puțin intențiile profesorului. Rezultatele învățării informează studenții despre ceea ce se așteaptă de la ei din punct de vedere al performanței, pentru a obține notele și creditele dorite. Sunt definite în termeni concreți, folosind verbe similare exemplurilor de mai jos și indică ceea ce se va urmări prin evaluare. Rezultatele învățării vor fi astfel redactate încât să fie evidențiată clar relația față de competențele definite la punctul 7.)

Cunoștințe	Rezultatul asimilării de informații prin învățare. Cunoștințele reprezintă ansamblul de fapte, principii, teorii și practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice și/sau factice. Asimilarea de cunoștințe teoretice și practice privind componenta criptografică a securității sistemelor care asigură protecția datelor.
Aptitudini	Capacitatea de a aplica cunoștințe și de a utiliza know-how pentru a duce la îndeplinire sarcini și a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive și creative) sau practice (implicând dexteritate manuală și utilizarea de metode, materiale, unelte și instrumente). Capacitatea de a estima nivelul de impact al unor vulnerabilități teoretice sau practice, ce pot apărea asupra unui sistem cu componente criptografice.



Responsabilitate și autonomie	<i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale. Capacitatea de a estima realist nivelul de securitate oferit de un sistem care conține componente criptografice.</i>
--------------------------------------	--

9. Metode de predare (Se vor avea în vedere metode care să asigure predarea centrată pe student. Se va descrie modul în care se asigură participarea studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămânări în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)

Predarea se bazează pe folosirea videoproiectorului (acoperind funcția de comunicare și demonstrativă); metodele de comunicare orală utilizată sunt metoda expozitivă și metoda problematizării, utilizate frontal. Materialele de curs sunt: notele și prezentările de curs, exercitii propuse pentru laborator sau ca tema (teoretice și cu rezolvare pe calculator). Toate materialele sunt disponibile în format electronic.

10. Conținuturi

CURS		
Capitolul	Conținutul	Nr. ore
1	Sisteme criptografice simetrice cifruri stream/cifruri bloc, clasificări, tipuri de sisteme, moduri de lucru, metode de atac;	6
2	Sisteme criptografice asimetrice. semnătură digitală, scheme de autentificare și schimb de chei, autorități decertificare;	6
3	Securitatea datelor în rețele informatice. protocoale de securitate	8
4	Securitatea sistemelor informatice securitatea sistemului criptografic vs securitatea implementării acestuia.	8
Total:		28
Bibliografie: Applied cryptography – Bruce Schneier, ed II Design, Principle and Practical Applications – Cryptography Engineering – Niels Ferguson, Bruce Schneier, Tadayoshi Kohno A guide to computer Network Security, Joseph Migga Kizza Fundamentals of cryptology, Henk C.A. van Tilborg Handbook of applied cryptography – Alfred Menezes, Oorschot, Vastone. Understanding Cryptography – Cristofor Paar, Jan Pelzl Limbajul C# pentru incepatori, Liviu Negrescu, Lavinia Negrescu.		

LABORATOR		
Nr. crt.	Conținutul	Nr. ore
1	Reluare notiuni de C# - principii de programare, sintaxă, tipuri de aplicații Visual Studio, structurarea codului, exemple de clase .NET și proprii	2



Universitatea Națională de Știință și Tehnologie Politehnică București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



2	Reluare elemente avansate de limbaj – tipuri de instrucțiuni, operatori, tipuri de date .NET și definite de utilizator, scenarii de lucru	2
3	Proiectarea și implementarea de aplicații software care utilizează și exemplifică conceptele, noțiunile și tipurile de sisteme criptografice prezentate în cadrul cursului.	8
4	Componentă de implementare în cadrul testelor parțiale	2
Total:		14

Bibliografie:

Surse publice online – www.msdn.com, ș.a., după caz. Materiale realizate de titularii de curs/aplicații.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	- cunoașterea noțiunilor teoretice fundamentale; - cunoașterea modului de aplicare a teoriei la probleme specifice; - analiza diferențială a tehnicilor și metodelor teoretice.	teste scrise de verificare în timpul semestrului; subiectele acoperă întreaga materie, realizând o sinteză între parcurgerea teoretică comparativă a materiei și explicitarea prin exerciții și probleme a modelelor de aplicație.	50%
11.5 Seminar/laborator/proiect	cunoașterea noțiunilor necesare analizei nivelului de securitate oferit de anumite aplicații, precum și implementarea software a acestor aplicații; - modul de programare, tipul soluțiilor identificate; - implicarea pe durata desfășurării laboratoarelor.	Componenta de implementare din cadrul testelor parțiale. Bonus pentru implicare. Minim o evaluare a componentei aplicative, de deprinderi practice.	50%
11.6 Condiții de promovare			
prezența la laboratoare, participare activă la cursuri			

12. Coroborarea conținutului disciplinei cu așteptările reprezentanților angajatorilor și asociațiilor profesionale reprezentative din domeniul aferent programului, precum și cu stadiul actual al cunoașterii în domeniul științific abordat și practicile în instituții de învățământ superior din Spațiul European al Învățământului Superior (SEIS)

Criptografia este o componentă esențială a mecanismului complex de asigurare a securității comunicațiilor. Înțelegerea principiilor de bază ale sistemelor criptografice moderne are un aport semnificativ în pregătirea viitorilor programatori din domeniul securității datelor, a specialiștilor din domeniul cyber-security, a administratorilor de sisteme informatice și a multor alți tipuri de specialiști în domenii conexe.

Programa cursului răspunde vine în întâmpinarea cerințelor actuale de dezvoltare și evoluție în domeniul criptologiei, prezentările acoperind atât sisteme criptografice clasice, cât și principii de proiectare și implementare a sistemelor curente, moderne.



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



Componenta de programare orientată-obiect asigură suport pentru o mai bună dezvoltare a abilităților de programare a studenților, cu posibil impact pe termen scurt, mediu și chiar lung, în evoluția profesională a acestora.

Data completării

Titular de curs

Titular(i) de aplicații

25.09.2025

Colaborator Dr. Adriana Clim

Colaborator Dr. Gabriel Negara

Data avizării în departament

Director de departament

26.09.2025

Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultății

Decan

26.09.2025

Prof. Dr. Mihnea Udrea