Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti

Facultatea de Electronică, Telecomunicaţii şi

Tehnologia Informaţiei

FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti**
1.2 Facultatea	**Electronică, Telecomunicaţii şi Tehnologia Informaţiei**
1.3 Departamentul	**Telecomunicaţii**
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
1.5 Ciclul de studii	Licenţă
1.6 Specializarea	Tehnologii şi Sisteme de Telecomunicaţii

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Bazele criptologiei 2			
2.2 Titularul activităţilor de curs				Colaborator Dr. Adriana Clim			
2.3 Titularul activităţilor 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 activităţilor 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 învăţământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii şi eseuri					20
Tutorat					5
Examinări					6
Alte activităţi (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. Precondiţii (acolo unde este cazul)

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

5. Condiţii necesare pentru desfăşurarea optimă a activităţilor didactice (acolo unde este cazul)

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

6. Obiectiv general *(Se referă la intenţiile profesorilor pentru studenţi, la ceea ce studenţii vor fi învăţaţi în timpul cursului. Oferă o orientare cu privire la locul cursului în cadrul domeniului ştiinţific abordat, precum şi 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 învăţământ al specializării studiate etc.)*

Disciplina asigura insusirea cunostintelor de baza din domeniul criptologiei moderne: insusirea conceptelor de criptologie simetrica si asimetrica, insusirea conceptelor de securitate informatica si de evaluare a nivelului de securitate.
Insusirea practica a notiunilor predate la curs, prin implementarea de programe software in limbajul C#; rezolvarea unor probleme practice concrete care includ aspecte legate de securitatea datelor si verificarea /validarea nivelului de securitate al sistemului.

7. Competenţe *(Capacitatea dovedită de a utiliza cunoştinţe, aptitudini şi abilităţi personale, sociale şi/sau metodologice în situaţii de muncă sau de studiu şi pentru dezvoltarea profesională şi personală. Reflectă cerinţele angajatorilor.)*

Specifice	Crearea abilităţilor de a aplica cunoştinţe generale de matematici fundamentale si de algoritmica in analiza rezistentei sistemelor criptografice moderne. Posibilitatea de a realiza aplicatii software care implementeaza atacuri asupra sistemelor criptografice. Dezvoltarea calitatilor necesare evaluarii nivelului de securitate (din perspectiva criptografica) oferit de un sistem sau de o componenta a acestuia.
Transversale (generale)	Cresterea capacitatii de a analiza obiectiv nivelul de securitate oferit de un sistem.

8. Rezultatele învăţării *(Sunt enunţuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învăţării reflectă realizările studentului şi mai puţin intenţiile profesorului. Rezultatele învăţării informează studenţii despre ceea ce se aşteaptă de la ei din punct de vedere al performanţei, pentru a obţine notele şi creditele dorite. Sunt definite în termeni concreţi, folosind verbe similare exemplelor de mai jos şi indică ceea ce se va urmări prin evaluare. Rezultatele învăţării vor fi astfel redactate încât să fie evidenţiată clar relaţia faţă de competenţele definite la punctul 7.)*

Cunoştinţe	*Rezultatul asimilării de informaţii prin învăţare. Cunoştinţele reprezintă ansamblul de fapte, principii, teorii şi practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice şi/sau faptice.* Asimilarea de cunostinte teoretice si practice privind componenta criptografica a securitatii sistemelor care asigura potectia datelor.
Aptitudini	*Capacitatea de a aplica cunoştinţe şi de a utiliza know-how pentru a duce la îndeplinire sarcini şi a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive şi creative) sau practice (implicând dexteritate manuală şi utilizarea de metode, materiale, unelte şi instrumente).* Capacitatea de a estima nivelul de impact al unor vulnerabilitati teoretice sau practice, ce pot aparea asupra unui sistem cu componente criptografice.

Responsabilitate și autonomie	*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 contine componente criptografice.

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 rămâneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)*

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

10. Conţinuturi

CURS

Capitolul	**Conţinutul**	**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 reţele informatice. protocoale de securitate	8
4	Securitatea sistemelor informatice securitatea sistemuluicriptografic 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.
Understading Cryptography – Cristofor Paar, Jan Pelzl
Limbajul C# pentru incepatori, Liviu Negrescu, Lavinia Negrescu.

LABORATOR

Nr. crt.	**Conţinutul**	**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

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 realizat.e de titularii de curs/aplicaţii.		

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	- cunoaşterea noţiunilor teoretice fundamentale; - cunoaşterea modului de aplicare a teoriei la probleme specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice.	teste scrise de verificare în timpul semestrului; subiectele acoperă întreaga materie, realizând o sinteză între parcurgerea teoretică comparativă a materiei şi explicitarea prin exerciţii şi probleme a modelelor de aplicaţie.	50%
11.5 Seminar/laborator/proiect	cunoaşterea 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			
prezenta la laboratoare, participare activa la cursuri			

12. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor angajatorilor şi asociaţiilor profesionale reprezentative din domeniul aferent programului, precum şi cu stadiul actual al cunoaşterii în domeniul ştiinţific abordat şi practicile în instituţii de învăţământ superior din Spaţiul European al Învăţământului Superior (SEÎS)

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 dministratorilor de sisteme informatice și a multor altor tipuri de specialiști în domenii conexe.
Programa cursului răspunde vine în întâmpinareacerinţelor actuale de dezvoltare şi evoluţie în domeniul criptologiei, prezentările acoperind atât sisteme criptografice clasice, cât și principii de proiectare și implementare a sistemelor curente, moderne.

Componenta de programare orientată-obiect asigură suport pentru o mai bună dezvoltare a abilităţilor de programare a studenţilor, cu posibil impact pe termen scurt, mediu şi chiar lung, în evoluţia profesională a acestora.

Data completării	Titular de curs	Titular(i) de aplicaţii
21.09.2026	Colaborator Dr. Adriana Clim	Colaborator Dr. Gabriel Negara

Data avizării în departament	Director de departament
22.09.2026	Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultăţii	Decan
22.09.2026	Prof. Dr. Mihnea Udrea