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 1			
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	3	2.5 Semestrul	2	2.6. Tipul de evaluare	V	2.7 Regimul disciplinei	Op
2.8 Tipul disciplinei		S	2.9 Codul disciplinei	04.S.06.A.229		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					8
Tutorat					8
Examinări					2
Alte activităţi (dacă există):					2

3.7 Total ore studiu individual	8.00
3.8 Total ore pe semestru	50
3.9 Numărul de credite	2

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Programare
4.2 de rezultate ale învăţării	Cunoştinţe generale de matematică şi informatică (nivel începător/mediu intr-un limbaj de programare orientată-obiect, uşurinţă în utilizarea calculatorului)

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

5.1 Curs	Atentie la conceptele noi.

5.2 Seminar/ Laborator/Proiect	Prezenta obligatorie pentru a intelege, prin implementare, conceptele predate.

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 clasice si moderne: insusirea conceptelor de baza din matematica necesare in introducerea domeniului cripto; tipuri de sisteme clasice de baza, evolutia sistemelor criptografice pana la trecerea spre criptologia moderna, infuenta teoriei informatiei, principiile criptologiei moderne, clasificarea si insusirea conceptelor de securitate informatica, atacuri 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 estimarea nivelului de rezistenta a sistemului criptografic, metodele de atac, notiuni de securitatea datelor si verificarea/validarea nivelului de securitate asigurat de sistemul criptografic.

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. Posibilitatea de a realiza aplicatii software care implementeaza atacuri asupra sistemelor criptografice.
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 şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi 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 studenţilor la stabilirea propriului parcurs de învăţare, cum se identifică eventualele rămâneri în urmă şi ce măsuri remediale se adoptă în astfel de cazuri.)*

Metode active de invatare, participare interactiva in cadrul cursului si laboratorului.

10. Conţinuturi

CURS

Capitolul	Conţinutul	Nr. ore
1	Fundamente matematice, elemente de algebra superioara, teoria numerelor, elemente de teoria informatiei aspecte de istoria cripto, clasificari	6
2	Criptologie clasica. Sisteme de tip substitutie - simpla, neuniforma, multipla, polialfabetica	6
3	Sisteme de tip transpozitie - cu careu complet sau incomplet	4
4	Sisteme combinate, masini de cifrat, sisteme perfecte.	6
5	Introducere in criptologia moderna. Tipuri de sisteme, concepte avansate de securitate a sistemelor moderne, standarde si evaluare.	6
	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	Introducere in limbajul C# - principii de programare, sintaxă, tipuri de aplicaţii Visual Studio, structurarea codului, exemple de clase .NET şi proprii	4
2	Prezentarea e elemente avansate de limbaj – tipuri de instrucţiuni, operatori, tipuri de date .NET şi definite de utilizator, scenarii de lucru	2

3	IProiectarea şi implementarea de aplicaţii software care utilizează şi exemplifică conceptele, noţiunile şi tipurile de sisteme criptografice prezentate în cadrul cursului.	6
4	Componentă de implementare în cadrul testelor de evaluare.	2
	Total:	14

Bibliografie:
Surse publice online – www.msdn.com, ş.a., după caz.
Materiale realizate de titularii de curs/aplicatii.

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, cu subiecte ce 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 noţiunilor necesare analizei nivelului de securitate oferit de anumite aplicaţii, precum şi implementarea software a acestor aplicaţii; - modul de programare, tipul soluţiilor identificate; - implicarea pe durata desfăşurării laboratoarelor.	Componenta de implementare din cadrul testelor parţiale. Bonus pentru implicare. Minim o evaluare a componentei aplicative, de deprinderi practice.	50%
11.6 Condiţii de promovare			
- asimilarea, înţelegerea noţiunilor de bază de la curs; - cunostinte de baza din C#, elaborare aplicatii tip consola si pe baza de forme Windows - proiectarea şi implementarea de aplicaţii care să pună în practică noţiunile şi sistemele criptografice din cadrul cursului.			

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)

Criptologia este o componenta regasita in orice metoda care asigura securitatea comunicatiilor si a datelor in format electronic.

Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti
Facultatea de Electronică, Telecomunicaţii şi
Tehnologia Informaţiei

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

