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	Masterat
1.6 Specializarea	Comunicaţii Mobile

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Fundamente matematice ale criptografiei			
2.2 Titularul activităţilor de curs				Conf.dr.univ. Alina PETRESCU-NITA			
2.3 Titularul activităţilor de seminar / laborator				Conf.dr.univ. Alina PETRESCU-NITA			
2.4 Anul de studiu	1	2.5 Semestrul	I	2.6. Tipul de evaluare	V	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		DS	2.9 Codul disciplinei	UPB.04.M1.O.08-05		2.10 Tipul de notare	Nota

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

3.1 Număr de ore pe săptămână	1.5	Din care: 3.2 curs	1.00	3.3 seminar/laborator	0.5
3.4 Total ore din planul de învăţământ	21.00	Din care: 3.5 curs	14	3.6 seminar/laborator	7
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					26
Tutorat					0
Examinări					3
Alte activităţi (dacă există):					0

3.7 Total ore studiu individual	29.00
3.8 Total ore pe semestru	50
3.9 Numărul de credite	2

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Parcurgerea următoarelor discipline: – Algebra liniara, geometrie analitica si diferentiala (1)
4.2 de rezultate ale învăţării	Acumularea următoarelor cunoştinţe generale: – concepte fundamentale de algebra liniara .

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

5.1 Curs	Cursul se va desfășura într-o sală dotată cu videoproiector și computer.
5.2 Seminar/ Laborator/Proiect	– Laboratorul se va desfășura într-o sală cu dotare specifică, care trebuie să includă: videoproiector, computer, software specific și acces la Internet. – Prezența obligatorie la laboratoare (conform regulamentului studiilor universitare de masterat în UNSTPB).

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.)*

In era digitaa – cum este ¸si firesc – criptografia este omniprezenta. Tehnicile criptografice sunt folosite pentru a securiza comunicatiile derulate prin intermediul retelelor de calculatoare, pentru a efectua plati on-line, pentru a implementa scheme de vot electronic, in cadrul telefoanelor mobile sau cardurilor bancare. In viitorul apropiat se prefigureaza noi aplicatii ale criptografiei ˆın domenii precum Cloud Computing, Internet of Things (IoT), vehicule inteligente sau telemedicina

Algoritmii criptografici au la baza o serie de concepte matematice. Prin urmare, pentru a intelege criptografia, trebuie, mai ıntai, stapanite aceste concepte. Rolul acestei curs este de a familiariza stundetii cu fundamentele matematice ale criptografiei.

Un aspect foarte important este dat de faptul că, în cadrul disciplinei, masteranzii trebuie să devolte un proiect individual sau în echipă, prin care să demonstreze atât însuşirea aspectelor teoretice cât şi abilităţile de dezvoltare.

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	– Cunoștințe de bază privind conceptele teoretice și aplicatii ale algebrei liniare. – Aplicatii în practică cunoștințele teoretice dobândite și utilizează algoritimilor matematici – Aplică metode și instrumente standardizate, specifice domeniului securității cibernetice, identifică soluții de utilizare a algoritmilor matematici in criptografia clasica
Transversale (generale)	Lucrează în echipă și comunică eficient, coordonându-și eforturile cu ceilalți pentru rezolvarea de situații problemă de complexitate medie. Respectă principiile de etică academică: în activitatea de documentare citează corect sursele bibliografice utilizate.

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.* Intelegerea unor concepte de matematica ce se utilizeaza in algoritmii clasici criptografici, in criptografia simetrica si asimetrica. asigura studentilor background-ul matematic necesar pentru a intelege algoritmii criptografici.
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).* Identificarea şi evaluarea notiunilor matematice in algoritmii criptografici. Cercetare ştiinţifică în domeniul securităţii informaţiei şi a sistemelor informatice şi cibernetice
Responsabilitate şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi aptitudinile sale.* Aplicarea valorilor şi eticii profesiei de cercetător şi executarea responsabilă a sarcinilor profesionale în condiţii de autonomie şi luare de decizii bazate pe evaluare şi autoevaluare. Realizarea activităţilor şi exercitarea rolurilor specifice muncii în echipă, pe diferite paliere ierarhice, manifestând spirit de iniţiativă şi antreprenorial şi rol de lider bazat pe promovarea dialogului, cooperării, atitudinii pozitive, respectului reciproc, diversităţii şi multiculturalităţii şi îmbunătăţire continuă a propriei activităţi. Autoevaluarea obiectivă a nevoii de formare profesională, continuă, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia si pentru dezvoltarea personală şi profesională şi utilizarea eficientă a abilităţilor multilingvistice şi a cunoştinţelor de tehnologia informaţiei şi a comunicării.

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.)*

– Cursurile sunt predate într-o manieră interactivă, fiind încurajată participarea activă a studenţilor. Sunt folosite atât metode clasice de predare (prelegerea şi expunerea), utilizând prezentări PowerPoint prin intermediul mijloacelor multimedia, cât şi interactive, bazate pe întrebări – răspunsuri şi feedback-ul studenţilor, adaptând permanent demersul pedagogic la posibilităţile de asimilare şi învăţare a studenţilor (prin repetarea suplimentară a anumitor noţiuni şi concepte, dacă acest lucru se dovedeşte necesar).

Fiecare curs debutează cu recapitularea succintă a capitolelor anterioare, cu accent asupra noţiunilor parcurse la ultimul curs. Prezentările utilizează numeroase imagini şi scheme, astfel încât informaţiile prezentate să fie cât mai uşor de înţeles şi asimilat. Materialele complete de curs sunt disponibile în format electronic pe platforma Moodle a facultăţii.

– Predarea cunoștințelor în cadrul orelor de laborator se bazează pe comunicarea orală și explicarea detaliată a metodelor utilizate și a rezultatelor obținute, într-o manieră permanent interactivă. Studenții implementează și evaluează independent aceleași probleme prin utilizarea calculatorului, a mediului software și a echipamentelor hardware (atunci când este cazul). Aplicațiile realizate îi ajută pe studenți în dezvoltarea unor relații optime de comunicare într-un climat favorabil învățării prin descoperire. Materialele de laborator sunt disponibile studenților sub formă electronică pe platforma Moodle a facultății.

– Materialele de proiect sunt disponibile studenților sub formă electronică pe platforma Moodle a facultății.

10. Conținuturi

CURS		
Capitolul	**Conținutul**	**Nr. ore**
1	Structuri algebrice 1.1. Multimi, Functii, Relatii 1.2. Grupuri 1.3. Corpuri	2
2	Divizibiliate si congruenta 2.1.Factorizare si primalitate 2.2. Congruenta si inelul Zn 2.3. Teorema lui Euler, Fermat , Wilson	3
3	Polinoame si extensii Galois 3.1. Algebra polinoamelor de o nedeterminata 3.2. Circuite liniare (LF SR) pentru polinoame 3.3. Extensii Galois 3.4. Relatii de recurenta liniara	3
4	Aritmetica pe curbe eliptice 4.1. Grupul aditiv pe o curba eliptica 4.2. Multiplicarea punctelor 4.3.Curbe Koblitz	3
5	Elemente de probabilitati cu aplicattii ın criptografie 5.1.Probabilitati (Definitie, Probabilitati claseice si Probabilitati independente) 5.2.Variabile aleatoare 5.3.Algoritmi probabilistici (Algoritmi probabilistici de factorizare, paradoxul nasterii)	3
	Total:	14

Bibliografie:

N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

2. C. Koscielny, M. Kurkowski Modern Cryptography Primer , Springer, 2013

A. Atanasiu , Matematici in Criptografie Ed Infodata Cluj
V. Alexandru ,N.M. Gosoiu: ***Elemente De Teoria Numerelor*** E D.Univ.Bucuresti 1999 ;
A. Gica , L.Panaitopol: *O introducere in teoria numerelor* Ed Univ.Buc. 2005 ;
L. Ciungu: *Probleme de matematici aplicate in criptografie* Ed. Universitaria Craiova 2005.
A.Petrescu-Niță Algebră liniară aplicativă, Politehnica Press 2021

LABORATOR		
Nr. crt.	**Conținutul**	**Nr. ore**
1	Structuri algebrice (Grupuri , Corpuri)	1
2	Divizibiliate si congruenta(Congruenta si inelul Znt, Teorema lui Euler, Fermat , Wilson)	2
3	Polinoame si extensii Galois (Algebra polinoamelor de o nedeterminat, Extensii Galois)	1
4	Aritmetica pe curbe eliptice(Grupul aditiv pe o curba eliptica)	1
5	Probabilitati	1
	Total:	7

Bibliografie:

N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

2. C. Koscielny, M. Kurkowski Modern Cryptography Primer , Springer, 2013

A. Atanasiu , Matematici in Criptografie Ed Infodata Cluj
V. Alexandru ,N.M. Gosoiu: ***Elemente De Teoria Numerelor*** E D.Univ.Bucuresti 1999 ;
A. Gica , L.Panaitopol: *O introducere in teoria numerelor* Ed Univ.Buc. 2005 ;
L. Ciungu: *Probleme de matematici aplicate in criptografie* Ed. Universitaria Craiova 2005.
A.Petrescu-Niță Algebră liniară aplicativă, Politehnica Press 2021

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 rezolvarea unor probleme specifice domeniului.	Verificare pe parcurs	50%
11.5 Seminar/laborator/proiect	Înțelegerea tehnicilor fundamentale de analiză și prelucrare a vulnerabilităților calculatorului personal sau a rețelei în care aceste se află.	Fișă de laborator la fiecare lucrare de laborator	30%
	Proiectarea, implementarea și gestionarea metodelor matematice	Prezentarea și documentarea proiectului final	20%
11.6 Condiții de promovare			
– Obținerea a 50% din punctajul total. – Realizarea obligațiilor caracteristice activității de laborator/proiect (participarea la lucrările planificate).			

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 (SEÎS)

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

Cursul Fundamente Matematice ale Criptografiei se aliniază cerințelor și așteptărilor actuale ale angajatorilor și asociațiilor profesionale din domeniul securității informației și al criptografiei, având ca scop pregătirea studenților pentru cerințele complexe ale pieței muncii. Cursul abordează aspecte fundamentale ale criptografiei, cum ar fi aritmetica modulară, teoria numerelor și algoritmi de criptare, oferind cunoștințe de bază esențiale pentru aplicarea criptografiei în securitatea rețelelor și a comunicațiilor.

Conținutul disciplinei este dezvoltat în conformitate cu stadiul actual al cunoașterii științifice în domeniul criptografiei și cu practicile de predare folosite în instituțiile de învățământ superior din Spațiul European al Învățământului Superior (SEÎS). Astfel, cursul integrează atât perspective teoretice, cât și aplicații practice, în conformitate cu standardele europene, pentru a asigura compatibilitatea și transferabilitatea competențelor dobândite de studenți. Cursul contribuie la formarea abilităților critice și analitice necesare pentru rezolvarea problemelor din domeniul securității cibernetice și criptografiei, asigurând astfel un fundament solid pentru o carieră de succes în acest domeniu dinamic și în continuă evoluție.

Data completării	Titular de curs	Titular(i) de aplicații
	Conf. univ. dr. Alina Petrescu Nita	Conf. univ. dr. Alina Petrescu Nita

Data avizării în departament	Director de departament
27.10.2024	Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultății	Decan
25.10.2024	Prof. Dr. Mihnea Udrea