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 Wireless Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Algoritmi criptografici pentru comunicaţii wireless Cryptographic Algorithms for Wireless Communications			
2.2 Titularul activităţilor de curs				Conf. Dr. Octaviana DATCU			
2.3 Titularul activităţilor de seminar / laborator				Conf. Dr. Octaviana DATCU			
2.4 Anul de studiu	1	2.5 Semestrul	II	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		DS	2.9 Codul disciplinei	UPB.04.M2.O.21-05		2.10 Tipul de notare	Nota

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

3.1 Număr de ore pe săptămână	2.5	Din care: 3.2 curs	1.5	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	35.00	Din care: 3.5 curs	21	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					57
Tutorat					0
Examinări					8
Alte activităţi (dacă există):					0

3.7 Total ore studiu individual	65.00
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Studentul este familiarizat cu cel puţin un limbaj de programare. Exemplu: Python, Matlab.
4.2 de rezultate ale învăţării	Noţiuni elementare de procesare a semnalului.

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

5.1 Curs	Cursul se va desfăşura într-o sală dotată cu videoproiector şi calculator.
5.2 Seminar/ Laborator/Proiect	Laboratorul se va desfăşura într-o sală dotată cu calculatoare.

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.)*

Prelegerile şi lucrările de laborator sunt îndreptate spre a permite studenţilor să acumuleze cunoştinţe despre elementele de bază ale criptoanalizei. Cunoştinţele acumulate sunt relevante în zilele noastre în contextul academic, industrial şi economic, în care schimbul de informaţii sensibile este tot mai mare.

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	Studenţii: • cunosc, înţeleg şi folosesc limbajul specific domeniului; • corelează cunoştinţele specifice domeniului criptografiei cu cele ale celorlalte discipline aparţinând zonei de inginerie electronică, telecomunicaţii şi tehnologii informaţionale. • aplică cunoştinţe, metode şi instrumente standardizate, specifice în practica domeniului, pentru realizarea procesului de evaluare şi diagnosticare a unei situaţii, în funcţie de problemele semnalate şi identifică soluţii. • argumentează şi analizează în mod coerent şi corect contextul de aplicare a cunoştinţelor de bază ale domeniului, folosind concepte cheie ale disciplinei şi metodologia specifcă. • foloseşte vocabularul stiintific specific domeniului, pentru a comunica eficient, în scris şi oral.
Transversale (generale)	Studenţii: • lucrează în chipă şi comunică eficient, coordonând eforturile cu ceilalţi colegi la rezolvarea unor situaţii problematice de complexitate medie. • au autonomie şi gândire critică: capacitatea de a gândi în termeni ştiinţifici, de a căuta şi analiza datele în mod independent, precum şi a extrage şi prezenta concluziile / identificarea solutiilor. • au capacitatea de a analiza şi de a sintetiza cunoştinţele dobândite pe cale sintetică, urmând un proces sistematic de analiză. • respectă principiile eticii academice: citează corect în documentaţia realizată sursele bibliografice utilizate. • pune în practică elemente de inteligenţă emoţională în gestionarea contextului socio-emoţional. • se comportă adecvat situaţiilor din viaţa reală/academică/profesională, demonstrând stăpânirea sinelui şi obiectivitatea în luarea deciziilor sau în situatii stresante.

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 exemplelor 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 faptice.* Studenții: • enumeră cele mai importante etape care au marcat dezvoltarea domeniului. • definesc noțiuni specifice domeniului. • descriu și aplică noțiuni/procese/algoritmi. • evidențiază consecințele și relațiile dintre algoritmi.
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).* Studenții: • descriu, comparativ, algoritmii si metodele invatate. • implementează algoritmul de criptare al lui Caesar pentru criptarea și decriptarea textelor. • implementează algoritmul pentru a sparge cifrul lui Caesar. • implementează cifrul Vigenere pentru criptarea și decriptarea textelor. • implementează algoritmii pentru a sparge cifrul lui Vigenere. • implementează cifrul lui Baptista pentru criptarea și decriptarea imaginilor. • implementează algoritmii pentru metricile care evaluează calitatea criptării și decriptării pe imagini.

Responsabilitate și autonomie	*Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.* Studenții: • selectează sursele bibliografice adecvate și le analizează. • respectă principiile eticii academice, citând corect sursele bibliografice utilizate. • demonstrează receptivitate la noile contexte de învățare. • demonstrează colaborarea cu alți colegi și cu personalul didactic în desfășurarea activității didactice. • dau dovadă de autonomie în organizarea situației de învățare/contextului sau a situației problemă pe care o rezolvă. • demonstrează responsabilitate socială prin implicarea activă în viața socială studențească/ implicarea in evenimentele comunitatii academice. • promovează/contribuie la noi soluții legate de domeniul de expertiză pentru îmbunătățirea calității vieții sociale. • sunt conștienți de valoarea contribuției lor la domeniul ingineriei și la identificarea de soluții viabile/durabilei pentru rezolvarea problemelor din viața socială și economică (responsabilitate socială). • aplică principiile eticii profesionale/ deontologiei în analiza impactului tehnologic al soluţiilor propuse în domeniul specific mediului. • analizează și valorifică oportunitățile de dezvoltare a afacerilor/antreprenoriale în domeniul de specialitate. • demonstrează abilități de gestionare a situațiilor din viața reală (gestionarea timpului, colaborare vs. conflict).

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.)*

Pornind de la analiza caracteristicilor de învăţare ale elevilor şi a nevoilor lor specifice, procesul de predarea va explora atât metodele de predare expozitive (prelegeri, expunere), cât şi interactive conversaţionale bazate pe modele de învăţare prin descoperirea facilităţii de explorarea directă şi indirectă a realităţii (experiment, demonstraţie, modelare), dar şi pe metode bazate pe acţiune, precum exerciţii, activităţi practice şi rezolvarea problemelor.

În activitatea didactică se vor folosi prelegeri, bazate pe prezentări Power Point sau diferite videoclipuri care vor fi puse la dispoziţia studenţilor. Fiecare curs va începe cu recapitularea capitolelor acoperite, cu accent pe conceptele abordate în ultimul curs.

Prezentările folosesc imagini şi diagrame astfel încât informaţiile prezentate să fie uşor de înţeles şi asimilat.

Acest subiect acoperă informaţii şi activităţi practice menite să sprijine studenţii în eforturile lor la învăţare şi dezvoltarea unor relaţii optime de colaborare şi comunicare într-un climat propice învăţării prin descoperire.

Se va avea în vedere exersarea abilităţilor de ascultare activă şi comunicare asertivă, precum şi mecanisme de construcţie a feedback-ului, ca modalităţi de reglare a comportamentului în diverse situaţii şi de adaptare a abordării pedagogice a nevoilor de învăţare ale elevilor.

Abilităţile de lucru în echipă vor fi exersate pentru a rezolva diferite sarcini de învăţare.

10. Conținuturi

CURS		
Capitolul	**Conținutul**	**Nr. ore**
1	Criptologie - terminologie și noțiuni de bază, utilizând [1 - 5].	2
2	Criptografie cu cheie simetrică, utilizând [1 - 3].	3
3	Criptografie cu cheie publică, utilizând [7].	3
4	Criptanaliză cu cheie simetrică, utilizând [2 - 5].	3
5	Criptanaliză cu cheie publică, utilizând [7].	4
6	Analiza calității decriptării imaginilor, folosind [8].	2
7	Subiecte relevante conexe criptografiei - criptoeconomie, gestionarea drepturilor digitale.	2
8	Pregătire pentru examen.	2
	Total:	21

Bibliografie:

Bibliography:
[1] Caesar's cipher, mentioned in paragraph 56 of 'SVETONI TRANQVILII VITA DIVI IVLI', online at http://thelatinlibrary.com/suetonius/suet.caesar.html#56 on 28th of February 2021.
[2] Breaking Caesar's cipher, available online at https://en.wikipedia.org/wiki/Caesar_cipher on 7.03.2022.
[3] MA/CS358 Cryptography, Automating Vigenère Cipher Cracking, online at https://macs358.org/chapters/08/4/find-keylength-with-ic#Determining-the-Key-Length-using-Index-of-Coincidence, October 2023.
[4] Henk C.A. van Tilborg, ed. (2005). Encyclopedia of Cryptography and Security(First ed.). Springer. p. 115. ISBN 0-387-23473-X.
[5] Practical Cryptography, online at http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/, October 2023.
[6] MS Baptista, Physics letters A 240 (1-2), 50-54, online at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.9974&rep=rep1&type=pdf, October 2023.
[7] Imam, Raza, et al. "Systematic and critical review of RSA based public key cryptographic schemes: Past and present status." IEEE Access 9 (2021): 155949-155976.
[8] Mahendiran, N., and C. Deepa. "A comprehensive analysis on image encryption and compression techniques with the assessment of performance evaluation metrics." SN Computer Science 2.1 (2021): 29.
[9] Ferdous, Md Sadek, Mohammad Jabed Morshed Chowdhury, and Mohammad A. Hoque. "A survey of consensus algorithms in public blockchain systems for crypto-currencies." Journal of Network and Computer Applications 182 (2021): 103035.

LABORATOR		
Nr. crt.	**Conținutul**	**Nr. ore**
1	Implementarea cifrurilor lui Caesar și Vigenere, folosind [1, 3, 4, 5].	4
2	Criptanaliza cifrurilor lui Caesar și Vigenere, folosind [2 - 5].	4
3	Analiza comparativă a calității decriptării imaginilor utilizând propria implementare a criptosistemului lui Baptista și implementarea unui alt algoritm, dată, folosind [6, 7].	4
4	Colocviu.	2

		Total:	14

Bibliografie:
[1] Caesar's cipher, mentioned in paragraph 56 of 'SVETONI TRANQVILII VITA DIVI IVLI', online at http://thelatinlibrary.com/suetonius/suet.caesar.html#56 on 28th of February 2021.
[2] Breaking Caesar's cipher, available online at https://en.wikipedia.org/wiki/Caesar_cipher on 7.03.2022.
[3] MA/CS358 Cryptography, Automating Vigenère Cipher Cracking, online at https://macs358.org/chapters/08/4/find-keylength-with-ic#Determining-the-Key-Length-using-Index-of-Coincidence, October 2023.
[4] Henk C.A. van Tilborg, ed. (2005). Encyclopedia of Cryptography and Security(First ed.). Springer. p. 115. ISBN 0-387-23473-X.
[5] Practical Cryptography, online at http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/, October 2023.
[6] MS Baptista, Physics letters A 240 (1-2), 50-54, online at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.9974&rep=rep1&type=pdf, October 2023.
[7] Mahendiran, N., and C. Deepa. "A comprehensive analysis on image encryption and compression techniques with the assessment of performance evaluation metrics." SN Computer Science 2.1 (2021): 29.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	• cunoaşterea terminologiei folosite în criptologie. • utilizarea adecvată a notiuni din criptologie. • înţelegerea principiilor de bază ale algoritmilor în criptologie. • capacitatea de a construi şi analiza cifruri mai complexe pornind de la algoritmii de bază.	Examen scris - implementări Matlab/ Python şi aspecte teoretice - assignment Moodle.	40
11.5 Seminar/laborator/proiect		Teme (assignments Moodle) şi colocviu - implementări Matlab/ Python şi teorie.	60
11.6 Condiţii de promovare			

Studenţii trebuie să fie capabili să :

-
- răspundă la întrebări specifice, cum ar fi ce este un cifru, care este diferenţa dintre codificare şi criptare, ce este un criptosistem de tip cheie secretă/ cheie publică, ce înseamnă un cifru de substituţie simplă/multiplă.
- cum funcţionează un cifru de substituţie simplă precum cifrul lui Caesar - algoritmul şi cum se implementează software-ul care îl pune în aplicare.
- cum poate fi atacat un cifr de simplă substituţie.
- aplice atacuri criptoanalitice: forţă brută (doar text cifrat), text simplu cunoscut (sau text cifrat), criptoanaliza prin statistici, atacuri de frecvenţă.

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)

Prin activităţi, elevii îşi dezvoltă abilităţile de a oferi soluţii la probleme şi de a propune idei de îmbunătăţire a situaţiei existente în domeniul comunicaţiilor fără fir avansate.

Cursul are un conţinut similar cu cursurile susţinute de Institutul de Tehnologie din Massachusetts în Cambridge, Massachusetts.

Prin activităţi de laborator şi curs, se realizează dezvoltarea abilităţilor de management ale masterului considerând situaţii practice cu care elevii se pot confruna în viaţa reală pentru a-şi spori contribuţia la îmbunătăţirea mediului socio-economic.

Data completării	Titular de curs	Titular(i) de aplicaţii
	Conf. Dr. Octaviana DATCU, Prof. Dr. Calin Vladeanu	Conf. Dr. Octaviana DATCU
		Prof. Dr. Calin Vladeanu
Data avizării în departament	Director de departament	
27.10.2024	Conf. Dr. Serban Georgica Obreja	

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

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