



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 Ciclul de studii	Masterat
1.6 Specializarea	Comunicații Wireless Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei (ro)		Algoritmi criptografici pentru comunicații wireless					
(en)		Cryptographic Algorithms for Wireless Communications					
2.2 Titularul activităților de curs		Conf. Dr. Octaviana DATCU					
2.3 Titularul activităților 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 activităților 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 învățământ	35.00	Din care: 3.5 curs	21	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					57
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					
Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					
Tutorat					0
Examinări					8
Alte activități (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. Precondiții (acolo unde este cazul)

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

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



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

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.)

Prelegerile și lucrările de laborator sunt îndreptate spre a permite studenților să acumuleze cunoștințe despre elementele de bază ale criptoanalizei. Cunoștințele acumulate sunt relevante în zilele noastre în contextul academic, industrial și economic, în care schimbul de informații sensibile este tot mai mare.

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	<p>Studenții:</p> <ul style="list-style-type: none">• cunosc, înțeleg și folosesc limbajul specific domeniului;• corelează cunoștințele specifice domeniului criptografiei cu cele ale celorlalte discipline aparținând zonei de inginerie electronică, telecomunicații și tehnologii informaționale.• aplică cunoștințe, metode și instrumente standardizate, specifice în practica domeniului, pentru realizarea procesului de evaluare și diagnosticare a unei situații, în funcție de problemele semnalate și identifică soluții.• argumentează și analizează în mod coerent și corect contextul de aplicare a cunoștințelor de bază ale domeniului, folosind concepte cheie ale disciplinei și metodologia specifică.• folosește vocabularul științific specific domeniului, pentru a comunica eficient, în scris și oral.
Transversale (generale)	<p>Studenții:</p> <ul style="list-style-type: none">• lucrează în chipă și comunică eficient, coordonând eforturile cu ceilalți colegi la rezolvarea unor situații problematice de complexitate medie.• au autonomie și gândire critică: capacitatea de a gândi în termeni științifici, de a căuta și analiza datele în mod independent, precum și a extrage și prezenta concluziile / identificarea soluțiilor.• au capacitatea de a analiza și de a sintetiza cunoștințele dobândite pe cale sintetică, urmând un proces sistematic de analiză.• respectă principiile eticii academice: citează corect în documentația realizată sursele bibliografice utilizate.• pune în practică elemente de inteligență emoțională în gestionarea contextului socio-emoțional.• se comportă adecvat situațiilor din viața reală/academică/profesională, demonstrând stăpânirea sinelui și obiectivitatea în luarea deciziilor sau în situații 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 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	<p>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.</p> <p>Studenții:</p> <ul style="list-style-type: none">• 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	<p>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).</p> <p>Studenții:</p> <ul style="list-style-type: none">• descriu, comparativ, algoritmi și metodele învățate.• 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 algoritmi pentru a sparge cifrul lui Vigenere.• implementează cifrul lui Baptista pentru criptarea și decriptarea imaginilor.• implementează algoritmi pentru metricile care evaluează calitatea criptării și decriptării pe imagini.



Responsabilitate și autonomie	<p><i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.</i></p> <p>Studentii:</p> <ul style="list-style-type: none">• 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 studentescă/ implicarea în evenimentele comunității 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/durabile pentru rezolvarea problemelor din viața socială și economică (responsabilitate socială).• aplică principiile eticii profesionale/ deontologiei în analiza impactului tehnologic al soluțiilor 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 rămăneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)*

Pornind de la analiza caracteristicilor de învățare ale elevilor și a nevoilor lor specifice, procesul de predare va explora atât metodele de predare expositive (prelegeri, expunere), cât și interactive conversaționale bazate pe modele de învățare prin descoperirea facilității de explorarea directă și indirectă a realității (experiment, demonstrație, modelare), dar și pe metode bazate pe acțiune, precum exerciții, activități practice și rezolvarea problemelor.

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

Prezentările folosesc imagini și diagrame astfel încât informațiile prezentate să fie ușor de înțeles și asimilat.

Acest subiect acoperă informații și activități practice menite să sprijine studenții în eforturile lor la învățare și dezvoltarea unor relații optime de colaborare și comunicare într-un climat propice învățării prin descoperire.

Se va avea în vedere exersarea abilităților de ascultare activă și comunicare asertivă, precum și mecanisme de construcție a feedback-ului, ca modalități de reglare a comportamentului în diverse situații și de adaptare a abordării pedagogice a nevoilor de învățare ale elevilor.

Abilitățile de lucru în echipă vor fi exersate pentru a rezolva diferite sarcini de învățare.



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 - criptoconomie, 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 Vigenere 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 Javed 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	<ul style="list-style-type: none">• cunoașterea terminologiei folosite în criptologie.• utilizarea adecvată a notiuni din criptologie.• înțelegerea principiilor de bază ale algoritmilor în criptologie.• capacitatea de a construi și analiza cifruri mai complexe pornind de la algoritmii de bază.	Examen scris - implementări Matlab/Python și aspecte teoretice - assignment Moodle.	40
11.5 Seminar/laborator/proiect		Teme (assignments Moodle) și colocviu - implementări Matlab/Python și teorie.	60
11.6 Condiții de promovare			



Studentii trebuie să fie capabili să :

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

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 (SEİS)

Prin activități, elevii își dezvoltă abilitățile de a oferi soluții la probleme și de a propune idei de îmbunătățire a situației existente în domeniul comunicațiilor fără fir avansate.

Cursul are un conținut similar cu cursurile susținute de Institutul de Tehnologie din Massachusetts în Cambridge, Massachusetts.

Prin activități de laborator și curs, se realizează dezvoltarea abilităților de management ale masterului considerând situații practice cu care elevii se pot confrunta în viața reală pentru a-și spori contribuția la îmbunătățirea mediului socio-economic.

Data completării

Titular de curs

Titular(i) de aplicații

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