



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



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	Electronică Aplicată și Ingineria Informației
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclu de studii	Licență
1.6 Specializarea	Ingineria Informației

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)		Criptografie și protecția datelor Cryptography and Data Protection					
2.2 Titularul activităților de curs		Conf, Dr. Ing. Madalin Frunzete					
2.3 Titularul activităților de seminar / laborator		S.I./Lect. Dr. Alexandru DINU					
2.4 Anul de studiu	4	2.5 Semestrul	II	2.6. Tipul de evaluare	V	2.7 Regimul disciplinei	Op
2.8 Tipul disciplinei	S	2.9 Codul disciplinei	04.S.08.A.116	2.10 Tipul de notare	Nota		

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

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2.00	3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	42.00	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					30
Tutorat					2
Examinări					1
Alte activități (dacă există):					0
3.7 Total ore studiu individual	33.00				
3.8 Total ore pe semestru	75				
3.9 Numărul de credite	3				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Teoria transmisiunii informației; Matematici Speciale; Structuri de date si algoritmi.
4.2 de rezultate ale învățării	Este complementar disciplinelor în care este vorba de prelucrarea informației în rețele mari de calcul.

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

5.1 Curs	Nu e cazul
----------	------------



5.2 Seminar/ Laborator/Proiect	Prezența obligatorie la laboratoare (conform regulamentului studiilor universitare de masterat în UPB).
-----------------------------------	---

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.)*

Cursul face o prezentare de ansamblu a sistemelor secrete clasice și cu chei publice urmărind: (1) stăpânirea de către student a teoriei și a tehnicilor de protecție a informației, a metodelor de proiectare, realizare și evaluare a unui algoritm criptografic; (2) utilizarea metodelor criptografice în alte domenii (codarea imaginilor, algoritmi complecși) sau cu alte scopuri (modelarea limbajului natural, evidențierea și evaluarea entropiei și redundanței din surse naturale, generarea de numere pseudoaleatoare, etc).

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	- Utilizarea elementelor fundamentale referitoare la dispozitivele, circuitele și instrumentația electronică. - Aplicarea, în situații tipice, a metodelor de bază de prelucrare a semnalelor electrice și neelectrice; implementarea unor proceduri de complexitate medie pe procesoarele de semnal. - Înțelegerea și utilizarea conceptelor fundamentale din domeniul comunicațiilor și transmisiunii informației. - Aplicarea cunoștințelor, conceptelor și metodelor fundamentale privitoare la arhitectura sistemelor de calcul, microcontrolere, limbaje și tehnici de programare. - Proiectarea și utilizarea sistemelor de calcul și a rețelelor de calculatoare. - Dezvoltarea sistemelor software complexe: sisteme de baze de date, sisteme paralele și distribuite, sisteme multimedia, interfețe om-mașină. - Prelucrarea avansată a informației: recunoașterea formelor, analiza și prelucrarea imaginilor și a semnalului vocal, inteligența computațională.
Transversale (generale)	- Utilizarea elementelor fundamentale referitoare la dispozitivele, circuitele și instrumentația electronică. - Aplicarea, în situații tipice, a metodelor de bază de prelucrare a semnalelor electrice și neelectrice; implementarea unor proceduri de complexitate medie pe procesoarele de semnal. - Înțelegerea și utilizarea conceptelor fundamentale din domeniul comunicațiilor și transmisiunii informației. - Aplicarea cunoștințelor, conceptelor și metodelor fundamentale privitoare la arhitectura sistemelor de calcul, microcontrolere, limbaje și tehnici de programare. - Proiectarea și utilizarea sistemelor de calcul și a rețelelor de calculatoare. - Dezvoltarea sistemelor software complexe: sisteme de baze de date, sisteme paralele și distribuite, sisteme multimedia, interfețe om-mașină. - Prelucrarea avansată a informației: recunoașterea formelor, analiza și prelucrarea imaginilor și a semnalului vocal, inteligența computațională.



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	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. Să explice fundamentele teoretice care permit înțelegerea modului de funcționare a unui criptosistem. Să prezinte cele mai importante metode și criptosisteme de interes practic. Să dezvolte abilități de a proiecta noi sisteme de cifrare eficiente. Sunt considerați algoritmi specifici criptografiei clasice și cu chei publice, cu scop ilustrativ (activitatea de laborator), dar și pentru exerciții de proiectare (teme de casă).
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). • Selectează și grupează informații relevante pentru domeniul criptografiei și al protecției datelor • Rezolvă aplicații practice. • Formulează concluzii la experimentele realizate. • Argumentează soluțiile identificate/modurile de rezolvare. • Stăpânește teoria și tehnicile de protecție a informației, metodele de proiectare, realizare și evaluare a unui algoritm criptografic; • Utilizează metodele criptografice în alte domenii (codarea imaginilor, algoritmi complecși) sau cu alte scopuri (modelarea limbajului natural, evidențierea și evaluarea entropiei și redundanței din surse naturale, generarea de numere pseudoaleatoare, etc).
Responsabilitate și autonomie	Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale. • Selectează surse bibliografice potrivite și le analizează. • Respectă principiile de etică academică, citând corect sursele bibliografice utilizate. • Demonstrează receptivitate pentru contexte noi de învățare. • Manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice • Demonstrează autonomie în organizarea situației/contextului de învățare sau a problemei de rezolvat • Promovează/contribuie prin soluții noi, aferente domeniului de specialitate pentru a îmbunătăți calitatea vieții sociale • Conștientizează valoarea contribuției sale în domeniul ingineriei la identificarea de soluții viabile/sustenabile care să rezolve probleme din viața socială și economică (responsabilitate socială). • Aplică principii de etică/deontologie profesională în analiza impactului tehnologic al soluțiilor propuse în domeniul de specialitate asupra mediului înconjurător.



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

Curs:

Predarea se bazează pe expunerea fundamentelor teoretice în mod mixt, folosind atât tabla, cât și videoproiector (acoperind funcția de comunicare și demonstrativă). Materialele de curs sunt: notele și prezentările de curs, probleme și teme propuse (teoretice și cu rezolvare pe calculator), precum și diverse articole și extrase din bibliografia aferentă.

Laborator:

Predarea se bazează pe folosirea videoproiectorului (acoperind funcția de comunicare și demonstrativă); metoda de comunicare orală utilizată este metoda problematizării. Studenții simulează, implementează, testează și evaluează independent probleme de criptografie cu chei secrete/publice prin utilizarea continuă a calculatorului și a mediului software. Materialele didactice sunt platformele de laborator

10. Conținuturi

CURS		
Capitolul	Conținutul	Nr. ore
1	1 O privire de ansamblu asupra cursului: descriere, noțiuni de baza ale criptografiei convenționale și ale criptografiei cu chei publice. 2 Principiile criptografiei în lumina teoriei sistemelor secrete a lui C.E. SHANNON. Cantitatea de secret. Sistem secret perfect, sistem secret cu soluție unică, sistem secret ideal.	6
2	3 Spargerea cifrurilor. Redundanța. Distanța de unicitate. 2 4 Evaluarea sistemelor secrete practice: rezistența la atac criptanalitic, mărimea cheii, complexitatea cifrării/descifrării, propagarea erorilor, expandarea mesajului. 2 5 Combinații de cifruri. Funcții criptografice de mixare. Difuzie și confuzie. 2	6



3	6 Exemple de cifruri clasice (construcție, atac criptanalitic). 2 7 Standarde de cifrare: DES (Data Encryption Standard) 2 8 Standarde de cifrare: AES (Advanced Encryption Standard) 2 9 Criptografia cu chei publice. Contribuțiile lui Hellman. Fundamente matematice în criptografia cu chei publice. Complexitate computațională. Sisteme cu distribuire publică a cheilor și sisteme secrete publice. Autentificarea în sistemele de comunicație. Semnătura secretă. 8 10 Criptografia bazată pe sisteme haotice. 2	16
Total:		28

Bibliografie:

- Adriana Vlad, *Note de Curs* - <https://curs.upb.ro/2021/course/view.php?id=9179>
- C.E. Shannon, "Communication Theory of Secrecy Systems", Bell Systems Technical Journal, 28 (1949), 656-715.
- W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, 22 (1976), 644-654.
- I. Angheloiu, E. Gyorfi și V. Patriciu, *Securitatea și protecția informației în sistemele electronice de calcul*, Ed. Militară, București, 1986.
- Nicolae Constantinescu, *Criptografie*, Editura Academiei Romane, 2009
- Douglas R. Stinson, *Cryptography: Theory and Practice*, Third Edition, Chapman and Hall/CRC - November 01, 2005
- V. Patriciu, *Criptografia și securitatea rețelelor de calculatoare cu aplicații în C și Pascal*, Ed. Tehnică, București, 1994.
- Adriana Vlad, M. Mitrea, "A Study of Confusion Involved by Shannon's Mixing Transformations", Buletinul Științific al Universității "Politehnica" din București, Seria C, Vol. 57-58, Nr. 1-4, (1995-1996), pp. 55-64.
- Adriana Vlad, M. Mitrea, "Image Enciphering by Means of Cryptographic Mixing Transformations", Buletinul științific al Universității "Politehnica" din Timișoara, Tom 43(57), Fasc. 2, (1998), pp. 185-190.
- Adriana Vlad, M. Mitrea, "Cryptographic Mixing Transformations for Image Applications", Proc. SPIE, Vol. 3405, (1997), pp. 477-482.
- Adriana Vlad, M. Mitrea "Digital image – protection by means of cryptographic mixing transformations" Proc. SPIE, Vol. 4430, (2000), pp. 560-565.
- Adriana Vlad, A. Luca, O. Hodea, R. Tataru, "Generating chaotic secure sequences using tent map and a running-key approach", Proc. of the Romanian Academy, Series A, vol.14, Special Issue-CRYPTOLOGY SCIENCE, pp.265-302, 2013.
- Roxana Dragomir, Adriana Vlad. "Statistical testing of the initializing stage of a block cipher, as part of the security assessment." Scientific Bulletin of University POLITEHNICA of Bucharest, Series A, Vol. 79, Iss. 2, 2017, Applied Mathematics and Physics
- Aurel Andrei, Marilena Stanculescu, *Criptografie vs. criptanaliză*, Editura Printech, Bucuresti, 2014



Nr. crt.	Conținutul	Nr. ore
1	1. Concepere și implementare software a metodei de criptare și evaluarea rezistenței la atacuri criptanalitice. Se vor studia diverși algoritmi din criptografia convențională: metode de tip substituție, metode de tip transpoziție, metode bazate pe funcții criptografice de mixare, standardul american de criptare DES și criptosisteme înrudite 6 2. Implementare software și analiza unor algoritmi din criptografia cu chei publice: - metode bazate pe problema rucsacului - metoda RSA (Rivest Shamir Adleman) - funcția Hash; semnătura secretă 6 3. Verificare laborator 2	14
	Total:	14

Bibliografie:

- <https://curs.upb.ro/2025/>
- M. Mitrea, Adriana Vlad, A. Branea, "The m-gram Substitution in the Cryptographic Mixing Transformation Applied to Images", in Proc. Intl. Symp. on Signal, Circuits & Systems - SCS'99, July 1999, Iași, pp. 151-155.
- Adriana Vlad, A. Mitrea și M. Mitrea, *Limba română scrisă ca sursă de informație*, Ed. Paideia, București, 2003.
- M.S. Baptista, "Cryptography with chaos" Physics Letters A, vol. 240 (1998) 50-54.
- Adriana Vlad, A. Ilyas, A. Luca, "A closer view of running-key cipher on natural languages and its extension
or new applications in cryptography", Proc. of the Romanian Academy, Series A, vol. 13, Number 2/2012, pp. 57-166.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	10.4 Curs Cunoașterea /intelegerea noțiunilor teoretice fundamentale	Două lucrări de verificare, de pondere 20% fiecare, în timpul semestrului, susținute la date fixate la începutul cursului 40%	40%
	Cunoașterea / intelegerea modului de aplicare a teoriei la probleme specifice	Mini teste la curs si/sau o temă (lucru acasă) cu pondere de 30% care va fi susținută într-o prezentare orală	30%



11.5 Seminar/laborator/proiect	Cunoașterea modului de lucru al algoritmilor de criptare studiați Abilitatea de a implementa software un algoritm de criptare Întelegerea principiului criptografiei cu cheie secretă și publică, evidențierea noțiunii de semnătură secretă.	Colocviu de laborator	30%
11.6 Condiții de promovare			
Obținerea a 50% din punctajul total. Obținerea a 50% din punctajul aferent laboratorului			

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)

Criptografia a fost și este un domeniu interdisciplinar, de mare interes și foarte actual, urmărind asigurarea confidențialității și a protecției informației. Indirect, dar în același timp foarte important pentru cercetarea științifică în lume, aceste preocupări creează un spațiu, o platformă extinsă de lucru, conectând domenii și tehnici de lucru foarte diverse și relevand aspecte noi în beneficiul științei în general. În acest sens se înscriu manifestările științifice în domeniu, inclusiv cele cinci ediții ale conferinței “Romanian Cryptology Days”, RCD 2011, RCD 2013, RCD 2015, RCD 2017, RCD 2019 care au creat un forum internațional de expunere /dezbateri de probleme și aplicații.

Programa cursului răspunde concret acestor cerințe actuale de dezvoltare, subscrise economiei europene a serviciilor din domeniul Calculatoare și Tehnologia Informației (CTI). În contextul progresului tehnologic actual, criptografia și protecția datelor reprezintă preocupări ale industriei electronice atât din punctul de vedere al dispozitivelor/sistemelor, cât și din prisma algoritmilor. Robustetea unui cifru este dependentă de puterea de calcul, iar acest curs le permite studenților adaptarea și inovarea spre noi algoritmi.

Se asigură absolvenților competențe adecvate cu necesitățile calificărilor actuale și o pregătire științifică și tehnică de calitate și competitivă, care să le permită angajarea rapidă după absolvire, pregătirea fiind perfect încadrată în politica Universității Politehnice din București atât din punctul de vedere al conținutului și structurii, cât și din punctul de vedere al aptitudinilor și deschiderii internaționale oferite studenților.

Data completării

Titular de curs

Titular(i) de aplicații

25.09.2025

Conf.dr.ing. Madalin FRUNZETE

S.I./Lect. Dr. Alexandru DINU



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



Data avizării în departament

Director de departament

Data aprobării în Consiliul Facultății Decan

26.09.2025

Prof. Dr. Mihnea Udrea