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	**Electronică Aplicată şi Ingineria Informaţiei**
1.4 Domeniul de studii	Calculatoare şi Tehnologia Informaţiei
1.5 Ciclul de studii	Licenţă
1.6 Specializarea	Ingineria Informaţiei

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Criptografie şi protecţia datelor			
2.2 Titularul activităţilor de curs				Conf. Dr. Ing. Madalin Frunzete			
2.3 Titularul activităţilor de seminar / laborator				As. 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.017		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	2.00	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	42.00	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					33
Tutorat					0
Examinări					3
Alte activităţi (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. Precondiţii (acolo unde este cazul)

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

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

5.1 Curs	Nu este cazul

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

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.)*

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

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	- Utilizarea elementelor fundamentale referitoare la dispozitivele, circuitele şi instrumentaţia electronică. - Aplicarea, în situaţii tipice, a metodelor de bază de prelucrare a semnalelor electrice şi neelectrice; implementarea unor proceduri de complexitate medie pe procesoarele de semnal. - Înţelegerea şi utilizarea conceptelor fundamentale din domeniul comunicaţiilor şi transmisiunii informaţiei. - Aplicarea cunoştinţelor, conceptelor şi metodelor fundamentale privitoare la arhitectura sistemelor de calcul, microcontrolere, limbaje şi tehnici de programare. - Proiectarea şi utilizarea sistemelor de calcul şi a reţelelor de calculatoare. - Dezvoltarea sistemelor software complexe: sisteme de baze de date, sisteme paralele şi distribuite, sisteme multimedia, interfeţe om-maşină. - Prelucrarea avansată a informaţiei: recunoaşterea formelor, analiza şi prelucrarea imaginilor şi a semnalului vocal, inteligenţa computaţională.
Transversale (generale)	- Capacitatea de a comunica cu structurile ierarhice superioare și cu echipa aflată în subordine. - Capacitatea de a funcționa ca lider al unei echipe care poate fi formată din persoane cu specializări și nivele de calificare diferite. - Capacitatea de a identifica și aplica cele mai potrivite și relevante strategii de management ale echipei aflate în subordine. - Capacitatea de a lua decizii în vederea rezolvării problemelor curente sau imprevizibile, care apar în procesul de exploatare a sistemelor de calcul. - Capacitatea de a asigura planificarea și managementul proiectelor din domeniul ingineriei informației. - Capacitatea de a se informa și documenta permanent pentru dezvoltarea personală și profesională prin citirea literaturii de specialitate. - Capacitatea de a comunica și de a prezenta conținut tehnic atât în limba română, cât și în limba engleză. - Flexibilitate în utilizarea de noi sisteme și tehnologii în cadrul unei echipe în care membrii împreună ating un obiectiv bine definit, asumând în același timp roluri sau sarcini diferite.

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.* Să explice fundamentele teoretice care permit înţelegerea modului de funcţionare a unui criptosistem. Să prezinte cele mai importante metode şi criptosisteme de interes practic. Să dezvolte abilităţi de a proiecta noi sisteme de cifrare eficiente. Sunt consideraţi algoritmi specifici criptografiei clasice şi cu chei publice, cu scop ilustrativ (activitatea de laborator), dar şi pentru exerciţii de proiectare (teme de casă).
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).* • Selectează şi grupează informaţii relevante pentru domeniul criptografiei şi al protecţiei datelor • Rezolvă aplicaţii practice. • Formulează concluzii la experimentele realizate. • Argumentează soluţiile identificate/modurile de rezolvare. • Stăpâneşte teoria şi tehnicile de protecţie a informaţiei, metodele de proiectare, realizare şi evaluare a unui algoritm criptografic; • Utilizează metodele criptografice în alte domenii (codarea imaginilor, algoritmi complecşi) sau cu alte scopuri (modelarea limbajului natural, evidenţierea şi evaluarea entropiei şi redundanţei din surse naturale, generarea de numere pseudoaleatoare, etc).
Responsabilitate şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi aptitudinile sale.* • Selectează surse bibliografice potrivite şi le analizează. • Respectă principiile de etică academică, citând corect sursele bibliografice utilizate. • Demonstrează receptivitate pentru contexte noi de învăţare. • Manifestă colaborare cu ceilalţi colegi şi cadre didactice în desfăşurarea activităţilor didactice • Demonstrează autonomie în organizarea situaţiei/contextului de învăţare sau a problemei de rezolvat • Promovează/contribuie prin soluţii noi, aferente domeniului de specialitate pentru a îmbunătăţi calitatea vieţii sociale • Conştientizează valoarea contribuţiei sale în domeniul ingineriei la identificarea de soluţii viabile/sustenabile care să rezolve probleme din viaţa socială şi economică (responsabilitate socială). • Aplică principii de etică/deontologie profesională în analiza impactului tehnologic al soluţiilor 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 rămâneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)*

Curs:

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

Laborator:

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

10. Conţinuturi

CURS		
Capitolul	**Conţinutul**	**Nr. ore**
1	O privire de ansamblu asupra cursului: descriere, notiuni de baza ale criptografiei convenţionale şi ale criptografiei cu chei publice.	2
2	Principiile criptografiei în lumina teoriei sistemelor secrete a lui C.E. SHANNON. Cantitatea de secret. Sistem secret perfect, sistem secret cu soluţie unică, sistem secret ideal.	4
3	Spargerea cifrurilor. Redundanţa. Distanţa de unicitate.	2
4	Evaluarea sistemelor secrete practice: rezistenţa la atac criptanalitic, mărimea cheii, complexitatea cifrării/descifrării, propagarea erorilor, expandarea mesajului.	2
5	Combinaţii de cifruri. Funcţii criptografice de mixare. Difuzie şi confuzie.	2
6	Exemple de cifruri clasice (construcţie, 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. Contribuţiile lui Hellman. Fundamente matematice în criptografia cu chei publice. Complexitate computaţională. Sisteme cu distribuire publică a cheilor şi sisteme secrete publice. Autentificarea în sistemele de comunicaţie. Semnătura secretă.	2
10	Criptografia bazată pe sisteme haotice.	2
	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 criptography*, IEEE Transactions on Information Theory, 22 (1976), 644-654.
. I. Angheloiu, E. Gyorfi şi V. Patriciu, *Securitatea şi protecţia informaţiei in sistemele electronice de calcul*, Ed. Militară, Bucureşti, 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 şi securitatea reţelelor de calculatoare cu aplicaţii in C şi Pascal*, Ed. Tehnică, Bucureşti, 1994.
. Adriana Vlad, M. Mitrea, "*A Study of Confusion Involved by Shannon's Mixing Transformations*", Buletinul Ştiinţific al Universităţii "Politehnica" din Bucureşti, 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 ştiinţific al Universităţii "Politehnica" din Timişoara, Tom **43**(**57**), Fasc. **2**, (1998), pp. 185-190.
0. Adriana Vlad, M. Mitrea, "*Cryptographic Mixing Transformations for Image Applications*", Proc. SPIE, Vol. **3405**, (1997), pp. 477-482.
1. Adriana Vlad, M. Mitrea "*Digital image – protection by means of cryptographic mixing transformations*" Proc. SPIE, Vol. **4430**, (2000), pp. 560-565.
2. 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.
3. 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
4. Aurel Andrei, Marilena Stanculescu, Criptografie vs. criptanaliză, Editura Printech, Bucuresti, 2014

LABORATOR

Nr. crt.	Conţinutul	Nr. ore
1	Concepere şi implementare software a metodei de criptare şi evaluarea rezistenţei la atacuri criptanalitice.	6
2	Implementare software şi analiza unor algoritmi din criptografia cu chei publice: - metode bazate pe problema rucsacului - metoda RSA (Rivest Shamir Adleman) - funcţia Hash; semnătura secretă	6
3	Verificare laborator	2
	Total:	14

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 criptography*, IEEE Transactions on Information Theory, 22 (1976), 644-654.
. I. Angheloiu, E. Gyorfi şi V. Patriciu, *Securitatea şi protecţia informaţiei in sistemele electronice de calcul*, Ed. Militară, Bucureşti, 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 şi securitatea reţelelor de calculatoare cu aplicaţii in C şi Pascal*, Ed. Tehnică, Bucureşti, 1994.
. Adriana Vlad, M. Mitrea, "*A Study of Confusion Involved by Shannon's Mixing Transformations*", Buletinul Ştiinţific al Universităţii "Politehnica" din Bucureşti, 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 ştiinţific al Universităţii "Politehnica" din Timişoara, Tom **43**(**57**), Fasc. **2**, (1998), pp. 185-190.
0. Adriana Vlad, M. Mitrea, "*Cryptographic Mixing Transformations for Image Applications*", Proc. SPIE, Vol. **3405**, (1997), pp. 477-482.
1. Adriana Vlad, M. Mitrea "*Digital image – protection by means of cryptographic mixing transformations*" Proc. SPIE, Vol. **4430**, (2000), pp. 560-565.
2. 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.
3. 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
4. Aurel Andrei, Marilena Stanculescu, Criptografie vs. criptanaliză, Editura Printech, Bucuresti, 2014

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	Cunoaşterea /intelegerea noţiunilor teoretice fundamentale	Două lucrări de verificare, de pondere 20% fiecare, în timpul semestrului, susţinute la date fixate la începutul cursului	40%
	Cunoaşterea / intelegerea modului de aplicare a teoriei la probleme specifice	O temă (lucru acasă) cu pondere de 30% care va fi sustinută într-o prezentare orală	30%

11.5 Seminar/laborator/proiect	Cunoaşterea modului de lucru al algoritmilor de criptare studiati Abilitatea de a implementa software un algoritm de criptare Întelegerea principiului criptografiei cu cheie secretă şi publică, evidenţierea noţiunii de semnatură secretă.	Colocviu final de laborator, cuprinzând o componentă teoretică (un test grilă) şi o componentă practică (implementarea unui algoritm de criptare)	30%
11.6 Condiţii de promovare			
Obţinerea a 50% din punctajul total. Obţinerea a 50% din punctajul aferent activităţii pe parcursul semestrului. Obţinerea a 50% din punctajul aferent laboratorului			

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)

Criptografia a fost şi este un domeniu interdisciplinar, de mare interes şi foarte actual, urmarind asigurarea confidentialitaţii şi a protecţiei informaţiei. Indirect, dar în acelaşi timp foarte important pentru cercetarea ştiinţifică in lume, aceste preocupări creează un spaţiu, o platformă extinsă de lucru, conectând domenii şi tehnici de lucru foarte diverse şi relevand aspecte noi in beneficiul stiintei in general. In acest sens se inscriu manifestările ştiinţifice în domeniu, inclusiv cele cinci ediţii ale conferinţei “Romanian Cryptology Days”, RCD 2011, RCD 2013, RCD 2015, RCD 2017, RCD 2019 care au creat un forum internaţional de expunere /dezbatere de probleme şi aplicaţii.

Programa cursului răspunde concret acestor cerinţe actuale de dezvoltare, subscrise economiei europene a serviciilor din domeniul Calculatoare şi Tehnologia Informaţiei (CTI). În contextul progresului tehnologic actual, criptografia si protectia datelor reprezinta preocupari ale industriei electronice atât din punctual de vedere al dispozitivelor/sistemelor, cât şi din prisma algoritmilor. Robusteţea unui cifru este dependentă de puterea de calcul, iar acest curs le permite studenţilor adaptarea şi inovarea spre noi algoritmi.

Se asigură absolvenţilor competenţe adecvate cu necesităţile calificărilor actuale si o pregătire ştiinţifică şi tehnică de calitate şi competitiva, care să le permită angajarea rapidă după absolvire, pregatirea fiind perfect încadrata în politica Universităţii Politehnica din Bucureşti atât din punctul de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite studenţilor.

Data completării	Titular de curs	Titular(i) de aplicaţii
09.09.2022	Conf. Dr. Ing. Madalin Frunzete	As. Dr. Alexandru DINU

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

S.L. Dr. Ing, Cosmin Danisor

Data avizării în departament	Director de departament
16.10.2024	Conf. Dr. Bogdan Cristian FLOREA

Data aprobării în Consiliul Facultății	Decan
01.11.2024	Prof. Dr. Mihnea Udrea