Universitatea POLITEHNICA din Bucureşti
Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

FISA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea POLITEHNICA din Bucureşti
1.2 Facultatea	Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei
1.3 Departamentul	Departamentul de Electronică Aplicată şi Ingineria Informaţiei
1.4 Domeniul de studii	Calculatoare şi Tehnologia Informaţiei
1.5 Ciclul de studii	Licenţă
1.6 Programul de studii/Calificarea	Ingineria Informaţiei

2. Date despre disciplină

2.1 Denumirea disciplinei				Criptografie şi Protecţia Datelor			
2.2 Titularul activităţilor de curs				Prof. Dr. ing. Adriana VLAD			
2.3 Titularul activităţilor de seminar				S.l. Dr. ing. Mădălin FRUNZETE			
2.4 Anul de studiu	IV	2.5 Semestrul	II	2.6 Tipul de evaluare	Verificare	2.7 Regimul disciplinei	Obligatorie

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

3.1 Număr de ore pe săptămână din care	3	3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ din care	42	3.5 curs	28	3.6 seminar/laborator	14

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie și notițe	25
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	3
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	5
Tutoriat	0
Examinări	3
Alte activităţi	0

3.7 Total ore studiu individual	36
3.9 Total ore pe semestru	78
3. 10 Numărul de credite	3

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Teoria transmisiunii informaţiei,

	Matematici Speciale, Structuri de date și algoritmi.
4.2 de competenţe	Este complementar disciplinelor în care este vorba de prelucrarea informaţiei în reţele mari de calcul.

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	Nu este cazul
5.2 de desfăşurare a seminarului/laboratorului	Prezenţa obligatorie la laboratoare (conform regulamentului studiilor universitare de masterat în UPB).

6. Competenţe specifice acumulate

Competenţe profesionale	Stăpânirea fundamentelor teoretice care permit înţelegerea modului de funcţionare a unui criptosistem, precum şi cunoașterea celor mai importante metode și criptosisteme de interes practic. Dezvoltarea abilităţii de a proiecta noi sisteme de cifrare eficiente.
Competenţe transversale	Folosirea în practică a unui bagaj diversificat și complex de cunoștințe și noțiuni desprinse din disciplinele studiate in facultatea ETTI (teoria transmisiunii informației; procese aleatoare; programare; matematici speciale; rețele de calculatoare; prelucrări de imagini, etc.).

7. Obiectivele disciplinei (reieşind din grila de competenţe specifice acumulate)

7.1 Obiectivul genral al disciplinei	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).
7.2 Obiective specifice	Studenții sunt implicati in evaluarea teoretică și în diverse exerciții de proiectare/implementare/criptanaliză a unor algoritmi specifici criptografiei clasice şi cu chei publice.

8. Conţinut

8.1 Curs	Metode de predare	Observaţii
O privire de ansamblu asupra cursului: descriere, noțiuni de bază ale criptografiei convenţionale şi ale criptografiei cu chei publice.	Predarea se bazează pe expunerea fundamentelor teoretice în mod mixt, folosind atât tabla, cât și videoproiector (acoperind funcţia de comunicare şi demonstrativă). Materialele de curs sunt: notele şi	2 ore
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. • Spargerea cifrurilor. Redundanţa. Distanţa de unicitate. • Evaluarea sistemelor secrete practice: rezistenţa la		12 ore

atac criptanalitic, mărimea cheii, complexitatea cifrării/descifrării, propagarea erorilor, expandarea mesajului. • Combinaţii de cifruri. Funcţii criptografice de mixare. Difuzie şi confuzie. Exemple de cifruri clasice (construcţie, atac criptanalitic).	prezentările de curs, probleme si teme propuse (teoretice si cu rezolvare pe calculator), precum si diverse articole și extrase din bibliografia aferentă.	
Standarde de cifrare: **DES (Data Encryption Standard);** **AES (Advanced Encryption Standard)**		4 ore
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. • Sistemul RSA. • Sisteme de tip rucsac. Autentificarea în sistemele de comunicaţie. Semnătura secretă.		8 ore
Criptografie bazată pe sisteme haotice.		2 ore

Bibliografie

1. Adriana Vlad, *Note de Curs.*
2. C.E. Shannon, "*Communication Theory of Secrecy Systems*", Bell Systems Technical Journal, 28 (1949), 656-715.
3. W. Diffie and M. E. Hellman, *New directions in criptography*, IEEE Transactions on Information Theory, 22 (1976), 644-654.
4. I. Angheloiu, E. Györfi şi V. Patriciu, *Securitatea şi protecţia informaţiei în sistemele electronice de calcul*, Ed. Militară, Bucureşti, 1986.
5. Nicolae Constantinescu, *Criptografie*, Editura Academiei Romane, 2009
6. Douglas R. Stinson, *Cryptography: Theory and Practice*, Third Edition, Chapman and Hall/CRC - November 01, 2005
7. V. Patriciu, *Criptografia şi securitatea reţelelor de calculatoare cu aplicaţii în C şi Pascal*, Ed. Tehnică, Bucureşti, 1994.
8. 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.
9. 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.
10. Adriana Vlad, M. Mitrea, "*Cryptographic Mixing Transformations for Image Applications*", Proc. SPIE, Vol. **3405**, (1997), pp. 477-482.
11. Adriana Vlad, M. Mitrea *"Digital image – protection by means of cryptographic mixing transformations"* Proc. SPIE, Vol. **4430**, (2000), pp. 560-565.
12. 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.

8.2 Laborator	Metode de predare	Observaţii
Concepere şi implementare software a metodei de criptare şi evaluarea rezistenţei la atacuri criptanalitice. Se vor studia diverşi algoritmi din criptografia convenţională: metode de tip subtituţie, metode de tip transpoziţie, metode bazate pe funcţii criptografice de mixare, standardul american de criptare DES şi criptosisteme înrudite	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.	6 ore
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 ore
Verificare laborator		2 ore

Bibliografie

1. 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, Iaşi, pp. 151-155.
2. Adriana Vlad, A. Mitrea şi M. Mitrea, *Limba română scrisă ca sursă de informaţie*, Ed. Paideia, Bucureşti, 2003.
3. M.S. Baptista, "*Cryptography with chaos*" Physics Letters A, vol. 240 (1998) 50-54.
4. Adriana Vlad, A. Ilyas, A. Luca, "A closer view of running-key cipher on natural languages and its extension for new applications in cryptography", Proc. of the Romanian Academy, Series A, vol. 13, Number 2/2012, pp. 157–166.

9. Coroborarea conţinuturilor disciplinei cu asteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale si angajatori reprezentativi din domeniul aferent programului

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 in lume, aceste preocupări creează un spațiu, o platformă extinsă de lucru, conectând domenii și tehnici de lucru foarte diverse și relevând aspecte noi în beneficiul științei în general. În acest sens se înscriu manifestările științifice în domeniu, inclusiv cele două ediții ale conferinței "Romanian Cryptology Days", RCD 2011 si RCD 2013, care au creat un forum internațional de expunere /dezbatere de probleme și aplicații.

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 și protecția datelor reprezintă preocupări ale industriei electronice atât din punctul de vedere al dispozitivelor/sistemelor, cât și din prisma algoritmilor. Robustețea unui cifru este dependentă de puterea de calcul, iar acest curs le permite studenților adaptarea și inovarea spre noi algoritmi.

Se asigură absolvenţilor competenţe adecvate cu necesităţile calificărilor actuale si o pregătire ştiinţifică şi tehnică de calitate şi competitivă, care să le permită angajarea rapidă după absolvire, pregătirea fiind perfect încadrată 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.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală
10.4 Curs	- cunoaşterea noţiunilor teoretice fundamentale - cunoaşterea modului de aplicare a teoriei la probleme specifice	Două lucrări de verificare, de pondere 20% fiecare, în timpul semestrului, susţinute la date fixate la începutul cursului. O temă (lucru acasă) cu pondere de 30% care va fi sustinută într-o prezentare orală.	70%
10.5 Seminar/Laborator	- cunoaşterea modului de lucru al algoritmilor de cifrare studiați. - abilitatea de a implementa software un algoritm de criptare - înțelegerea principiului criptografiei cu cheie secretă și publică, evidențierea noțiunii de semnătură secretă.	Colocviu final de laborator, cuprinzând o componentă teoretică (un test grilă) şi o componentă practică (implementarea unui algoritm de criptare).	30%
10.6 Standard minim de performanţă			
- Realizarea unui algoritm de criptare cu cheie secretă, înțelegerea corespondenței unice între mesaj și criptogramă - Înțelegerea principiului criptografiei cu chei secrete și cu chei publice, evidențierea semnăturii digitale			

Data completării Semnătura titularului de curs Semnătura titularului de aplicaţii

..... Prof. Dr. ing. Adriana VLAD S.l. Dr. ing. Mădălin FRUNZETE

Data avizării în catedră Semnătura directorului de departament

..... Prof. Dr. Ing. S. Paşca