FIŞA DISCIPLINEI[1]

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Politehnica Timişoara
1.2 Facultatea[2] / Departamentul[3]	Automatică şi Calculatoare / Automatică şi Informatică Aplicată
1.3 Catedra	-
1.4 Domeniul de studii	Automatică și Informatică Aplicată
1.5 Ciclul de studii	Licenţă
1.6 Programul de studii / Calificarea	Ingineria Sistemelor / inginer

2. Date despre disciplină

2.1 Denumirea disciplinei			**Securitatea informației**				
2.2 Titularul activităţilor de curs			Conf. dr. Ing. Bogdan Groza				
2.3 Titularul activităţilor de seminar			dr. Ing. Horaţiu Gurban				
2.4 Anul de studiu	3	2.5 Semestrul	2	2.6 Tipul de evaluare	E	2.7 Regimul disciplinei	Obligatorie

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

3.1 Număr de ore pe săptămână	4	din care:3.2 curs	2	3.3 laborator/proiect	2
3.4 Total ore din planul de învăţământ	65	din care:3.5 curs	28	3.6 laborator/proiect	28
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					3
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					3
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					3
Tutoriat					7
Examinări					3
Alte activităţi					

3.7 Total ore studiu individual	9
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	• Nu este cazul
4.2 de competenţe	• Cunoştinţe de matematică, algoritmi şi programare la nivelul anului I

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	• Sală mare, Materiale suport: laptop, proiector, tablă.
5.2 de desfăşurare a seminarului/laboratorului	• Laborator cu 15-20 calculatoare – mediile de programare C, C# şi Java, sistem de operare Windows şi Unix, tablă

6. Competenţe specifice acumulate

Competenţe profesionale[4]	• Operarea cu concepte fundamentale din ştiinţa calculatoarelor, tehnologia informaţiei si comunicatiilor

[1] Formularul corespunde Fişei Disciplinei promovată prin OMECTS 5703/18.12.2011 (Anexa3);

[2] Se înscrie numele facultăţii care gestionează programul de studiu căruia îi aparţine disciplina;

[3] Se înscrie numele departamentului căruia i-a fost încredinţată susţinerea disciplinei şi de care aparţine titularul cursului;

	• Proiectarea, implementarea, testarea, utilizarea şi mentenanţa sistemelor cu echipamente de uz general şi dedicat, inclusiv reţele de calculatoare, pentru aplicaţii de automatică şi informatică aplicată.
Competenţe transversale	• Aplicarea, în contextul respectării legislaţiei, a drepturilor de proprietate intelectuala (inclusiv transfer tehnologic), a metodologiei de certificare a produselor, a principiilor, normelor şi valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă şi responsabilă. • Identificarea rolurilor şi responsabilităţilor într-o echipă plurispecializată luarea deciziilor si atribuirea de sarcini, cu aplicarea de tehnici de relaţionare şi muncă eficientă în cadrul echipei

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	• Dobândirea noţiunilor de bază pentru securizarea sistemelor şi criptografiei
7.2 Obiectivele specifice	• Însuşirea de către studenţi a tehnicilor moderne de din domeniul criptografiei, a designului şi analzei algoritmilor contemporani, • Însuşirea de către studenţi a tehnicilor moderne cu privire la securitatea sistemelor de calcul, a reţelelor şi tranzacţiilor Internet

8. Conţinuturi

8.1 Curs	Număr de ore	Metode de predare
Cap. 1. Introducere. Context istoric. Obiective de securitate. Tipuri de adversari şi de atacuri.	2	Prelegere susţinută de prezentări PPT, conversaţii, explicaţii, exemplificări
Cap. 2. Funcţii Criptografice. Cap. 2.1. Funcţii Simetrice. Functii fara cheie: generatoare de numere pseudo-aleatoare si functii hash (MD5, SHA1, SHA2, SHA3). Functii cu cheie simetrica: coduri MAC (NMAC, HMAC) si criptari simetrice (DES, 3DES, AES). Cap. 2.2. Funcţii Asimetrice. Funcţii de criptare cu cheie publică şi semnătură digitală (RSA, Diffie-Hellman-Merkle, ElGamal, DSA, ECC).	8	
Cap. 3. Fundamente matematice şi probleme computaţionale. Elemente de teoria informaţiei. Elemente de teoria probabilităţii. Elemente de teoria numerelor: Grupul Zn*, Teoremele lui Euler şi Fermat. Calculul operatiilor aritmetice în precizie arbitrară. Problema factorizării şi a logaritmului discret. Generarea numerelor prime. Curbe Eliptice.	4	
Cap. 4. Protocoale Criptografice. Cap. 4.1. Protocoale de autentificare. Autentificarea informaţiei, autentificarea entităţilor si schimburi autentificate de cheie secretă. Principii constructive: password based authentication, one-time passwords, challenge-response, zero-knowledge. Cap. 4.2. Protocoale de autentificare în sisteme de operare şi sisteme bancare (ATM, NTLM, MS-CHAP, ISO TPMA). Cap. 4.3. Protocoale de autentificare în reţele de calculatoare (EKE, STS, IPSec, SSL/TLS, SSH, Kerkeros).	6	
Cap. 5. Securitate wireless. Cap. 5.1. Securitate wireless in retele home-enterprise (WEP, WPA, WPA2). Cap. 5.2. Securitate in reţele de senzori (familia de protocoale TESLA).	4	
Cap. 6. Securitate software şi securitate hardware. Cap. 6.1. Funcţii criptografice în .NET si Java. Cap. 6.2. Securitate folosind smart-carduri, standardul PKCS11.	2	
Cap. 7. Securitate în sisteme automotive. Cap. 7.1. Distributia sigură a softwareului, imobilizatorul electronic, tahograful digital.	2	

Bibliografie

[1] Bogdan Groza, Introducere in criptografie, 200 pagini, ISBN 978-973-625-564-9, 2012, disponibil on-line la http://www.aut.upt.ro/~bgroza/Books/IntroCripto.pdf.
[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 816 pages, ISBN 0849385237 , 1996.
[3] Bruce Schneier, Applied Cryptography, John Wiley & Sons, 784 pages, ISBN 0471117099 , 1996.
[4] Wenbo Mao, Modern Cryptography:Theory and Practice, 648 p., ISBN13: 9780130669438, ISBN10: 0-13-066943-1, Prentice Hall, 2003.
[5] Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley, 640 p., ISBN 0-471-

[4] Aspectul competenţelor profesionale va fi tratat cf. Metodologiei OMECTS 5703/18.12.2011. Se vor prelua competenţele care sunt precizate în Registrul Naţional al Calificărilor din Învăţământul Superior RNCIS (http://www.rncis.ro/portal/page?_pageid=117,70218&_dad=portal&_schema=PORTAL) pentru domeniul de studiu de la pct. 1.4, programul de studii de la pct. 1.6 din această fişă şi materia în cauză

38922-6, 2001.
[6] Kerstin Lemke , Christof Paar, Marko Wolf et al., Embedded Security in Cars: Securing Current and Future Automotive IT Applications, 273 pages, Springer; 1 edition (December 7, 2005), ISBN-10: 3540283846, ISBN-13: 978-3540283843.
[7] Donggang Liu, Peng Ning, Security for Wireless Sensor Networks, 212 pages, Springer; 1 edition (November 9, 2006), ISBN-10: 0387327231, ISBN-13: 978-0387327235

8.2 Laborator/proiect	Număr de ore	Metode de predare
1. Analiza autentificării în sistemul de operare Unix, atacuri asupra autentificării bazate pe parole	2	Expunere temă, discuţii, întrebări, rezolvare pe calculator a 1-2 probleme.
2. Implementări ale funcţiilor criptografice cu cheie simetrică DES, 3DES, AES în mediul .NET (sau alternativ Java)	2	
3. Implementări ale unor funcţii fără cheie MD5, SHA1, SHA2 în mediul .NET (sau alternativ Java)	2	
4. Analiza matematică a unor funcţii şi probleme din criptografia cu cheie publică. Operaţii cu întregi în precizie arbitrară.	2	
5. Implementări ale funcţiilor criptografice cu cheie publică RSA, ElGamal, Diffie-Hellman în mediul .NET (sau alternativ Java)	2	
6. Atacuri asupra securiăţii reţelelor wireless conform standardului 802.11.	2	
7. Implementări ale unor funcţii criptografice în sisteme embedded.	2	
8. Proiectarea si implementarea intr-unul din limbajele cunoscute (de preferința C++, C# sau Java) a unei aplicaţii software ce are la bază cel puţin un algoritm modern de criptare destinat unor sisteme precizate prin tema de proiectare, e.g., securitatea unei aplicaţii client-server prin socket TCP, autentificarea la accesul de la distanţă a unei baze de date, autentificarea într-un sistem mobil bazat pe Android, etc.	12	
8. Recuperări	2	

Bibliografie

[1] Bogdan Groza, Introducere in criptografie, fundamente matematice şi computaţionale, 200 pagini, ISBN 978-973-625-564-9, 20011.
[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 816 pages, ISBN 0849385237 , 1996.
[3] Bruce Schneier, Applied Cryptography, John Wiley & Sons, 784 pages, ISBN 0471117099 , 1996.
[4] Wenbo Mao, Modern Cryptography:Theory and Practice, 648 p., ISBN13: 9780130669438, ISBN10: 0-13-066943-1, Prentice Hall, 2003.
[5] Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley, 640 p., ISBN 0-471-38922-6, 2001.

9. Corelarea conţinutului disciplinei cu cerinţele specialiştilor din domeniu şi cu aşteptările angajatorilor reprezentativi

- Cunoştinţele de securizare a informației sunt importante pentru toate componentele (software sau hardware) din domeniile IT&C.
- Majoritatea angajatorilor reprezentativi din domeniul aferent programului solicită cunoştinţe specifice securizării informației.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Rezolvarea unui subiect conținând problematici teoretice si aplicative	Examinare scrisă	66 %
10.5 Laborator/proiect	Rezolvarea problemelor corespunzătore lucrărilor de laborator	Prezentarea rezolvărilor, răspunsuri la întrebări	9 %
	Teme de casă	Prezentarea rezolvărilor, răspunsuri la întrebări	8 %
	Test laborator	Examinare scrisă	16 %
10.6 Standard minim de performanţă (volumul de cunoştinţe minim necesar pentru promovarea disciplinei şi modul în care se verifică stăpânirea lui)			
• Efectuarea tuturor aplicaţiilor practice de laborator si a temelor de laborator si realizarea a 50% răspunsuri corecte la partea scrisă (corespunzătoare cursului)			

11. Compatibilitate internaţională

- Stanford University http://crypto.stanford.edu/cs155/
- University of California - Berkeley http://inst.eecs.berkeley.edu/~cs161/fa08/

- Massachusetts Institute of Technology http://courses.csail.mit.edu/6.857/2013/

Data completării	Semnătura titularului de curs	Semnătura titularilor de laborator/proiect
	Conf. dr. Ing. Bogdan Groza	dr. Ing. Horaţiu Gurban
	…….……....	…….…….....

Data avizării în departament

Semnătura directorului de departament

Prof. dr. Ing. Ioan SILEA

……..……..……