FIŞA DISCIPLINEI[1]

1. Date despre program

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

2. Date despre disciplină

2.1 Denumirea disciplinei			**Securitatea Informației**				
2.2 Titularul activităţilor de curs			Ș.l.dr.ing. Bogdan GROZA				
2.3 Titularul activităţilor de seminar			Asist. dr. ing. Mihaela Marcella CRIȘAN-VIDA				
2.4 Anul de studiu	2	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 (SI)	2	3.3 seminar/laborator (AA)	2
3.4 Total ore din planul de învăţământ	56	din care:3.5 curs	28	3.6 seminar/laborator	28
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					21
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					10
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					5
Tutoriat					9
Examinări					3
Alte activităţi					

3.7 Total ore studiu individual	48
3.8 Total ore pe semestru	104
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	• Nu este cazul
4.2 de competenţe	• Cunoștințe de programare și matematică

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	• Sală medie, Materiale suport: laptop, proiector, tablă.
5.2 de desfăşurare a seminarului/laboratorului	• Laborator cu 17-25 calculatoare – Mediu de programare pentru aplicații

6. Competenţe specifice acumulate

Competenţe profesionale[4]	• Utilizarea de cunoştinţe de matematică, fizică, tehnica măsurării, grafică tehnică, inginerie mecanică, chimică, electrică şi electronică în ingineria sistemelor. • 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;

[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

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	• Operarea cu noțiuni specifice securității informației și criptografiei în sisteme informatice de uz comun si industriale
7.2 Obiectivele specifice	• Consolidarea cunostintelor de securitate în software si hardware (de ex. Programare Java, .NET, retele de calculatoare) • Dezvoltarea de aplicatii practice care includ elemente de securitate și criptografie

8. Conţinuturi

8.1 Curs	Număr de ore	Metode de predare
Cap. 1. Introducere. Context Istoric. Obiective de securitate. Tipuri de adversari si de atacuri.	2	Prelegere susţinută de prezentări PPT, conversaţii, explicaţii, exemplificări
Cap. 2. Functii Criptografice. Cap. 2.1. Functii 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. Functii Asimetrice. Functii de criptarea cu cheie publica si semnaturi digitale (RSA, Diffie-Hellman-Merkle, ElGamal, DSA, ECC).	14	
Cap. 3. Protocoale Criptografice.Protocoale de autentificare. Autentificarea informatiei, autentificarea entitatilor si schimburi autentificate de cheie secreta. Principii constructive: password based authentication, one-time passwords, challenge-response, zero-knowledge	6	
Cap. 4. Functii criptografice in .NET si Java	6	

Bibliografie

[1] Bogdan Groza, Introducere in criptografie: functii criptografice, fundamente matematice și computaționale, 200 pagini, ISBN 978-973-625-564-9, 2007.
[3] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 816 pages, ISBN 0849385237 , 1996.
[4] Bruce Schneier, Applied Cryptography, John Wiley & Sons, 784 pages, ISBN 0471117099 , 1996.
[5] Wenbo Mao, Modern Cryptography:Theory and Practice, 648 p., ISBN13:9780130669438, ISBN10: 0-13-066943-1, Prentice Hall, 2003.
[6] Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley, 640 p., ISBN 0-471-38922-6, 2001.
[7] Matt Bishop, Computer Security: Art and Science, 1136 p., Addison-Wesley Professional, ISBN-10: 0201440997, ISBN-13: 978-0201440997, 2002.
[8] Peter Thorsteinson, G. Gnana Arun Ganesh, .NET Security and Cryptography, 496 pages, Prentice Hall (August 28, 2003), ISBN-10: 013100851X, ISBN-13: 978-0131008519
[9] Brian A. LaMacchia, Sebastian Lange, Matthew Lyons, Rudi Martin, Kevin T. Price, .NET Framework Security, Addison Wesley, 2002, ISBN : 0-672-32184-X, 816 p.
[10] François Koeune, and François-Xavier Standaert. A Tutorial on Physical Security and Side-Channel Attacks, Foundations of Security Analysis and Design III : FOSAD 2004/2005, Volume 3655 of Lecture Notes in Computer Science, pages 78-108, November 2006
[11] 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.
[12] 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 Seminar/laborator	Număr de ore	Metode de predare
1. Realizarea unor programe implementate in Java în mediul de programare Eclipse sau în C# în mediul de programare Visual Studio .NET folosind funcții criptografice - funcții simetrice	10	Discutii ce au la baza progresul studentului in rezolvarea temei
2. Evaluarea programelor	2	
3. Realizarea unor programe implementate in Java în mediul de programare Eclipse sau în C# în mediul de programare Visual Studio .NET folosind funcții criptografice – funcții asimetrice	10	
4. Evaluarea programelor	2	
5. Recuperări	4	

Bibliografie
[1] Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley, 640 p., ISBN 0-471-38922-6, 2001.
[2] Peter Thorsteinson, G. Gnana Arun Ganesh, .NET Security and Cryptography, 496 pages, Prentice Hall (August 28, 2003), ISBN-10: 013100851X, ISBN-13: 978-0131008519
[3] Brian A. LaMacchia, Sebastian Lange, Matthew Lyons, Rudi Martin, Kevin T. Price, .NET Framework Security, Addison Wesley, 2002, ISBN : 0-672-32184-X, 816 p.

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

- Securitatea Informatiei devine o preocupare constanta pentru dezvoltatorii software in toate sectoarele industriale automotive, telecomunicatii, etc. Continutul disciplinei aduce exemple de probleme de securitate si solutii ale acestora aplicabile in toate aceste sectoare.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Corectitudinea raspunsurilor	Examen scris	100%
10.5 Seminar /laborator		Prezentarea programelor realizate de student si adresarea de intrebari specifice temei	100%
10.6 Standard minim de performanţă (volumul de cunoştinţe minim necesar pentru promovarea disciplinei şi modul în care se verifică stăpânirea lui)			
• Cunoasterea modului de functionare a algoritmilor prezentati in curs si capacitatea de a ii utiliza corect pentru dezvoltarea de solutii practice			

11. Compatibilitate internaţională

- University of Bristol http://www.cs.bris.ac.uk/Teaching/unitglance.jsp?unit=COMS30002

Data completării	Semnătura titularului de curs	Semnătura titularilor de seminar
05.02.2015	s.l.dr.ing. Bogdan Groza	Asist. dr. ing. Mihaela Marcella CRIȘAN-VIDA
	…….....	…….....

Data avizării în departament	Semnătura directorului de departament
15.02.2015	Prof. dr. ing. Ioan SILEA
	…….……