FIŞA DISCIPLINEI

Securitatea informației în conducerea proceselor

Anul universitar 2023-2023

1. Date despre program

1.1	Instituţia de învăţământ superior	Universitatea din Piteşti
1.2	Facultatea	Electronica, Comunicatii si Calculatoare
1.3	Departamentul	Electronica, Calculatoare si Inginerie Electrica
1.4	Domeniul de studii	Inginerie electronica,telecomunicatii si tehnologii informationale
1.5	Ciclul de studii	Master
1.6	Programul de studii / Calificarea	Master sisteme electronice pentru conducerea proceselor industriale (SECPI)/ Inginer de cercetare în electronica aplicată (215224); Asistent de cercetare în electronica aplicată (215225)

2. Date despre disciplină

2.1	Denumirea disciplinei					***Securitatea informației în conducerea proceselor***					
2.2	Titularul activităţilor de curs					Conf. dr. ing. Petre ANGHELESCU					
2.3	Titularul activităţilor de laborator					Conf. dr. ing. Petre ANGHELESCU					
2.4	Anul de studii	II	2.5	Semestrul	I	2.6	Tipul de evaluare	E	2.7	Regimul disciplinei	DSI/O/AI

3. Timpul total estimat

3.1	Număr de ore pe saptămână	3	3.2	din care curs	2	3.3	laborator	1
3.4	Total ore din planul de inv.	42	3.5	din care curs	28	3.6	laborator	14

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	6
Pregătire seminarii/laboratoare, teme, referate, portofolii, eseuri	24
Tutoriat	-
Examinări	8
Alte activităţi	-

3.7	Total ore studiu individual	58
3.8	**Total ore pe semestru**	**100**
3.9	**Număr de credite**	**4**

4. Precondiţii (acolo unde este cazul)

4.1	De curriculum	Parcurgerea disciplinelor de matematică (in special matematici speciale și algebra, capitolele referitoare la teoria numerelor).
4.2	De competenţe	**-**

5. Condiţii (acolo unde este cazul)

5.1	De desfăşurare a cursului	Sală cu o capacitate de minim 30 locuri dotată cu tabla, videoproiector și ecran de proiecție.
5.2	De desfăşurare a laboratorului	Calculatoare (minim 15), Internet, Mediul de programare Visual Studio .NET (Visual C++, C#) – de exemplu laborator T215.

6. Competenţe specifice acumulate

Competenţe profesionale	**C4.** Integrarea contextuală a sistemelor electronice de complexitate ridicată pentru conducerea proceselor industriale în timp real în conexiune cu tehnologiile de proces. **(4 puncte credit)**
Competenţe transversale	

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Prin acest curs ne propunem insusirea de catre studentii masteranzi a cunostintelor fundamentale si a tehnicilor avansate de securitate a informatiei. Cursul acopera metode computationale, tehnici bioinspirate, algoritmi, arhitecturi combinate software-hardware pentru securitatea informatiei destinate sistemelor informatice utilizate in retelele de

	telecomunicatii.
7.2 Obiectivele specifice	*Obiective cognitive* Insusirea conceptelor fundamentale din domeniul securitatii informatiei si intelegerea primitivelor si metodelor criptografice impreuna cu functionarea, avantajele si dezavantajele acestora. *Obiective procedurale* Insusirea tehnicilor de baza pentru proiectarea, implementarea si analiza sistemelor de securitate a informatiei ce folosesc primitive criptografice. *Obiective atitudinale* Dobândirea deprinderilor privind ordinea si lucrul in echipa in vederea realizării rapide de primitive de securitate a informatiei utilizate in aplicatiile proprii.

8. Conţinuturi

8.1. Curs		Metode de predare	Observaţii Resurse folosite
1.	**Introducere in securitatea informatiei (1)** 1. *Terminologie si concepte fundamentale* 2. *Aspecte sociale, etice si legislative ale securitatii informatiei.* 3. *Fundamente matematice si computationale.* -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
2.	**Introducere in securitatea informatiei (2)** 1. *Riscuri, amenintari si vulnerabilitati la adresa securitatii informatiei* 2. *Servicii si mecanisme de securitate* -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
3.	**Deziderate in sistemele criptografice contemporane** 1. *Criterii de evaluare a sistemele criptografice* 2. *Taxonomia sistemelor criptografice* 3. Sisteme criptografice – moduri de lucru -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
4.	**Criptografia clasica – cifruri simetrice de substitutie** -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
5.	**Criptografia clasica – cifruri simetrice de transpozitie** -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
6.	**Criptografia cu chei simetrice de tip stream si generatoare de numere aleatoare si pseudoaleatoare** -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
7.	**Criptografia cu chei simetrice de tip bloc si modurile de operare a cifrurilor de tip bloc** -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
8.	**Sistemele de criptare DES (Data Encryption Standard) si 3DES** 1. Considerații generale. 2. Descrierea sistemelor criptografice DES și 3DES. 3. Modalități de atac asupra DES & 3DES. -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
9.	**Sistemul de criptare AES (Advanced Encryption Standard)** 1. Considerații generale. 2. Descrierea sistemului criptografic. 3. Modalități de atac asupra AES. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
10.	**Criptografia cu chei asimetrice – cifruri asimetrice si semnaturi digitale** -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
11.	**Criptografie vizuala** 1. *Consideratii generale*. 2. *Scheme criptografice*. 3. *Exemple.* -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
12.	**Sisteme criptografice bazate pe tehnici bioinspirate (1)** 1. Considerații generale. 2. Generatoare de secvente pseudoaleatoare bazate pe	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.

	sisteme bioinspirate. 3. Metode de testare a calității secvențelor pseudoaleatoare generate. Standardul NIST. -Timp alocat **2 ore**		
13.	**Sisteme criptografice bazate pe tehnici bioinspirate (2)** 1. Sisteme criptografice ce funcționează pe baza teoriei automatelor celulare. 2. Exemple si analiza performante. -Timp alocat **4 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.

Bibliografie

1. Petre Anghelescu, "*AUTOMATE CELULARE – fundamente şi abordări practice cu aplicaţii în criptare*", Editura Matrix ROM, ISBN 978-973-755-821-3, Bucureşti, 2012 (disponibila la biblioteca si in laborator T215).
2. William Stallings, „*Cryptography and Network Security – Principles and Practice*", Prentice Hall, ISBN: 0-13-609704-9, 2011 (disponibila in laborator).
3. Rodriguez-Henriquez, F., Saqib, N. A., Diaz-Perez, A., Koc, C. K., "*Cryptographic algorithms on reconfigurable hardware*", Springer Science + Business Media, LLC, ISBN 0-387-33883-7, 2006.
4. Koc, C. K., "Cryptographic engineering", Springer Science + Business Media, LLC, ISBN: 978-0-387-71816-3, 2009.
5. Menezes, A., Oorschot, P., Vanstone, S., "Handbook of applied cryptography", CRC Press, ISBN: 0-8493-8523-7, 1996.
6. C. Shannon. Communication Theory of Secrecy Systems. Bell Sys. Tech. J. 28, pp. 656–715, 1949. (netlab.cs.ucla.edu/wiki/files/shannon1949.pdf).
7. Petre Anghelescu, Teza de doctorat: „Proiectarea si analiza automatelor celulare pentru prelucrarea informatiei", Conducător de doctorat – prof. univ. dr. ing. Emil Sofron, Pitesti, Decembrie 2007 (disponibila in laborator).
8. Petre Anghelescu, Matthew Szudzik "Exploring Hybrid Cellular Automata (HCA) for Cryptographic Applications", A New Kind of Science Summer School, Boston, SUA, 26.06.2011 – 17.07.2011, http://www.wolframscience.com/summerschool/2011/participants/anghelescu.html.
9. Stephen Wolfram, "*A new kind of science*", Wolfram Media Inc., ISBN: 1-57955-008-8, 2002 (disponibila in laborator T215).
10. Petre Anghelescu, „*Securitatea informatiei în conducerea proceselor"* – Note de curs, 2021.

8.2. Aplicaţii – Laborator		Metode de predare	Observaţii Resurse folosite
1.	Implementarea și analiza algoritmilor criptografici clasici - **cifruri simetrice de substitutie monoalfabetică**. -Timp alocat **4 ore**	Studiul de caz Exerciţiul Lucrul în grup Dezbaterea	Calculator, Visual Studio .NET (C#, Visual C++) instalat pe fiecare staţie de lucru
2.	Implementarea și analiza algoritmilor criptografici clasici - **cifruri simetrice de substitutie polialfabetică**. -Timp alocat **4 ore**	Studiul de caz Exerciţiul Lucrul în grup Dezbaterea	
3.	Implementarea și analiza algoritmilor criptografici clasici - **cifruri simetrice de transpozitie**. -Timp alocat **4 ore**	Studiul de caz Exerciţiul Lucrul în grup Dezbaterea	
4.	Implementarea și analiza algoritmilor de criptare ce **îmbină substituția** cu **transpoziția.** -Timp alocat **2 ore**	Studiul de caz Exerciţiul Lucrul în grup Dezbaterea	

Bibliografie

1. Petre Anghelescu, "*AUTOMATE CELULARE – fundamente şi abordări practice cu aplicaţii în criptare*", Editura Matrix ROM, ISBN 978-973-755-821-3, Bucureşti, 2012 (disponibila la biblioteca si in laborator).
2. William Stallings, „*Cryptography and Network Security – Principles and Practice*", Prentice Hall, ISBN: 0-13-609704-9, 2011 (disponibila in laborator).
3. Rodriguez-Henriquez, F., Saqib, N. A., Diaz-Perez, A., Koc, C. K., "*Cryptographic algorithms on reconfigurable hardware*", Springer Science + Business Media, LLC, ISBN 0-387-33883-7, 2006.
4. Koc, C. K., "Cryptographic engineering", Springer Science + Business Media, LLC, ISBN: 978-0-387-71816-3, 2009.
5. Menezes, A., Oorschot, P., Vanstone, S., "Handbook of applied cryptography", CRC Press, ISBN: 0-8493-8523-7, 1996.
6. Stephen Wolfram, "*A new kind of science*", Wolfram Media Inc., ISBN: 1-57955-008-8, 2002 (disponibila in laborator).
7. Petre Anghelescu, *Securitatea informației în conducerea proceselor* – Note de laborator, format electronic, 2021.

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori din domeniul aferent programului

Atat pentru elaborarea tematicii, cât și pentru alegerea metodelor de predare/învățare, titularul disciplinei a analizat pe de o parte oferta academică a unor instituții nationale si internationale de prestigiu de învățământ superior (UT din Cluj-Napoca – master Retele de calculatoare si Sisteme distribuite, UP Bucuresti, Academia Tehnica Militara Bucuresti - Master Securitatea Tehnologiei Informatiei, MIT, NPTEL) – cursuri de securitatea informatiei sunt prezentate in cadrul multor alte programe de master din acest domeniu (CSci 6331 Cryptography – The George Washington University – Washington DC, USA – Master of Science in Cybersecurity, Cryptography (252-0407-00L) – ETH Zurich – Elveția – Information Security Master), iar pe de alta parte a avut intalniri de lucru cu specialisti din productie si angajatori, inclusiv participarea la conferinte si workshop-uri din domeniu. In acest fel, disciplina respecta nivelul impus de rigorile academice și ofera în același timp abilităţile necesare pentru dezvoltarea de sisteme de securitate a informatiei stocate sau transmise in rețelele de comunicații.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Implicare in activitati	Initiative si teme	10%
	Evaluare finală	Probă scrisă	50%
10.5 Laborator	Verificarea deprinderilor şi abilităţilor practice dobândite de fiecare student.	Evaluare periodica privind rezolvarea studiilor de caz	40%
10.6 Standard minim de performanţă	Demonstrarea intelegerii notiunilor de baza, a principiilor si a metodelor uzuale din domeniul securitatii informatiei si abilitatea de a implementa corect, intr-o aplicatie proprie, primitive de securitate a informatiei. Finalizarea cu succes a laboratorului (nota minima 5) reprezinta o conditie de promovare a examenului.		

Data completării
15.09.2021

Titular de curs
Conf. dr. ing. Petre ANGHELESCU

Titular de laborator
Conf. dr. ing. Petre ANGHELESCU

Data avizării în departament
27.09.2021

Director de departament
Prof. univ. dr. ing. Gheorghe SERBAN