

FIȘA DISCIPLINEI

Securitatea informației

Anul universitar 2022-2023

1. Date despre program

1.1	Instituția de învățământ superior	Universitatea din Pitești
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 informatinale
1.5	Ciclul de studii	Master
1.6	Programul de studii / Calificarea	Master Inginerie Electronica si Sisteme Inteligente (IESI)/ Proiectant inginer de sisteme si calculatoare (215214); Inginer sisteme de securitate (215222); Inginer de cercetare in automatica (215239)

2. Date despre disciplină

2. Date despre disciplina											
2.1	Denumirea disciplinei					Securitatea informației					
2.2	Titularul activităților de curs					Conf. dr. ing. Petre ANGHELESCU					
2.3	Titularul activităților de proiect					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	DAP

3. Timpul total estimat

3.1	Număr de ore pe săptămână	4	3.2	din care curs	2	3.3	proiect	2
3.4	Total ore din planul de inv.	56	3.5	din care curs	28	3.6	proiect	28
Distribuția 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								8
Pregătire seminarii/laboratoare, teme, referate, portofolii, eseuri								28
Tutoriat								-
Examinări								8
Alte activități								-
3.7	Total ore studiu individual	69						
3.8	Total ore pe semestru	125						
3.9	Număr de credite	5						

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Parcursarea disciplinelor de matematică (în special matematici speciale și algebra, capitolele referitoare la teoria numerelor), Criptografie si securitate informationala.
4.2	De competențe	-

5. Condiții (acolo unde este cazul)

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

6. Competențe specifice acumulate

Competențe profesionale	C1. Cunoașterea în profunzime a teoriilor și conceptelor pentru descrierea cantitativă si calitativă a sistemelor cu inteligență artificială. (2 puncte credit) C2. Utilizarea tehnicilor de modelare simulativă și proiectare asistată a circuitelor si sistemelor electronice de prelucrare inteligentă a informației, prin fuzionarea tehnologiei sistemelor programabile, reconfigurabile și analogice. (1 punct credit) C4. Aplicarea de metode specifice de implementare hardware și software a sistemelor cu inteligență artificială. (1 punct credit) C5. Utilizarea metodelor de analiză a cerințelor economice și de elaborare a specificațiilor tehnice pentru proiecte de cercetare-dezvoltare în domeniul sistemelor inteligente. (1 punct credit)
Competențe 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 moderne de securitate a informatiei, cu precădere a
-----	-----------------------------------	--

	securizării datelor prin criptare. 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	<p><i>Obiective cognitive</i> Insusirea conceptelor fundamentale din domeniul securitatii informatiei si intelegerea primitivelor si metodelor criptografice impreuna cu functionarea, avantajele si dezavantajele acestora.</p> <p><i>Obiective procedurale</i> Insusirea tehnicilor de baza pentru proiectarea, implementarea si analiza sistemelor de securitate a informatiei ce folosesc primitive criptografice.</p> <p><i>Obiective atitudinale</i> Dobândirea deprinderilor privind ordinea si lucrul in echipa in vederea realizării rapide de primitive de securitate a informatiei utilizate in aplicatiile proprii.</p>

8. Conținuturi

8.1. Curs		Metode de predare	Observații 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 Dezbatare Descriere și 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 Dezbatare Descriere și 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 Dezbatare Descriere și exemplificare	Tabla, Calculator, Videoproiector.
4.	Criptografia clasica – cifruri simetrice de substitutie -Timp alocat 2 ore	Prelegere Dezbatare Descriere și exemplificare	Tabla, Calculator, Videoproiector.
5.	Criptografia clasica – cifruri simetrice de transpozitie -Timp alocat 2 ore	Prelegere Dezbatare Descriere și exemplificare	Tabla, Calculator, Videoproiector.
6.	Criptografia cu chei simetrice de tip stream si generatoare de secvente aleatoare si pseudoaleatoare -Timp alocat 2 ore	Prelegere Dezbatare Descriere și 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 Dezbatare Descriere și 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 Dezbatare Descriere și exemplificare	Tabla, Calculator, Videoproiector.
9.	Sistemul de criptare AES (Advanced Encryption Standard) 1. Considerații generale, preliminarii matematice. 2. Descrierea sistemului criptografic. 3. Modalități de atac asupra AES. -Timp alocat 2 ore	Prelegere Dezbatare Studiu de caz	Tabla, Calculator, Videoproiector.
10.	Criptografia cu chei asimetrice – cifruri asimetrice si semnături digitale -Timp alocat 2 ore	Prelegere Dezbatare Studiu de caz	Tabla, Calculator, Videoproiector.
11.	Criptografie vizuala 1. Considerații generale. 2. Scheme criptografice. 3. Exemple. -Timp alocat 2 ore	Prelegere Dezbatare Descriere și exemplificare	Tabla, Calculator, Videoproiector.
12.	Sisteme criptografice bazate pe tehnici bioinspirate (1)	Prelegere	Tabla,

	<div>1. Considerații generale.</div> <div>2. Generatoare de secvente pseudoaleatoare bazate pe sisteme bioinspirate.</div> <div>3. Metode de testare a calității secvențelor pseudoaleatoare generate. Standardul NIST.</div> <div>-Timp alocat 2 ore</div>	Dezbateri Studiu de caz	Calculator, Videoproiector.
13.	<div>Sisteme criptografice bazate pe tehnici bioinspirate (2)</div> <div>1. Sisteme criptografice ce funcționează pe baza teoriei automatelor celulare.</div> <div>2. Exemple si analiza performante.</div> <div>-Timp alocat 4 ore</div>	Prelegere Dezbateri Studiu de caz	Tabla, Calculator, Videoproiector.
<div>Bibliografie</div> <div>1. Petre Angheliescu, "AUTOMATE CELULARE – fundamente și abordări practice cu aplicații în criptare", Editura Matrix ROM, ISBN 978-973-755-821-3, București, 2012 (disponibila la biblioteca si in laborator T215).</div> <div>2. William Stallings, „Cryptography and Network Security – Principles and Practice”, Prentice Hall, ISBN: 0-13-609704-9, 2011 (disponibila in laborator).</div> <div>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.</div> <div>4. Koc, C. K., "Cryptographic engineering", Springer Science + Business Media, LLC, ISBN: 978-0-387-71816-3, 2009.</div> <div>5. Menezes, A., Oorschot, P., Vanstone, S., "Handbook of applied cryptography", CRC Press, ISBN: 0-8493-8523-7, 1996.</div> <div>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).</div> <div>7. Petre Angheliescu, 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).</div> <div>8. Petre Angheliescu, 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/angheliescu.html.</div> <div>9. Stephen Wolfram, "A new kind of science", Wolfram Media Inc., ISBN: 1-57955-008-8, 2002 (disponibila in laborator T215).</div> <div>10. Petre Angheliescu, „Securitatea informatiei” – Note de curs, 2021.</div>			
8.2. Aplicații – Proiect		Metode de predare	Observații Resurse folosite
1.	<div>Definirea temelor de proiect – Tema de proiect poate fi selectata din urmatoarele directii ce urmeaza a fi particularizate ca urmare a discutiilor cu fiecare student in parte:</div> <div>1) securitate criptografica in aplicatii dezvoltate in limbaje high-level (de exemplu: .NET sau Java)</div> <div>2) securitate criptografica in sisteme embedded (e.g., implementari de functii criptografice in sisteme cu microcontrollere/FPGA). Se va tine cont de constrangerile impuse de sistemele embedded.</div> <div>3) securitate criptografica pe dispozitive mobile (e.g., smartphones cu SO Android/iOS/Windows Mobile, tablete, etc.)</div> <div>4) studii de caz (de exemplu: e-banking, etc.)</div> <div>5) securitate criptografica cu tehnici bazate pe teoria sistemelor bio-inspirate.</div> <div>6) alte teme din problematica cursului, de complexitate similara cu temele anterioare, propuse de studentii masteranzi.</div> <div>-Timp alocat 4 ore</div>	Coordonare activitati aplicative, Exerciții practice, Lucrul în grup, Prezentari de proiecte, Dezbaterea.	Materiale de instruire prezentate cu videoproiectorul, Calculator, Visual Studio .NET (C#, Visual C++), Android Studio si alte medii de simulare instalate pe fiecare stație de lucru
2.	<div>Analiza detaliata a cerintelor impuse prin tema de proiect si a scenariilor de functionare.</div> <div>-Timp alocat 4 ore</div>		
3.	<div>Proiectarea sistemelor criptografice propuse (definire arhitectura, stabilire prioritati critice pentru implementare).</div> <div>-Timp alocat 4 ore</div>		
4.	<div>Implementare (construire efectiva) a sistemelor propuse.</div> <div>-Timp alocat 10 ore</div>		
5.	<div>Testarea (asigurarea calitatii) sistemelor criptografice proiectate si implementate (testarea internă, testarea unitatilor, testarea intregii aplicatii/intregului sistem).</div> <div>-Timp alocat 4 ore</div>		
6.	<div>Prezentarea/sustinerea proiectului.</div> <div>-Timp alocat 2 ore</div>		
<div>Bibliografie</div> <div>1. Petre Angheliescu, "AUTOMATE CELULARE – fundamente și abordări practice cu aplicații în criptare", Editura Matrix ROM, ISBN 978-973-755-821-3, București, 2012 (disponibila la biblioteca si in laborator).</div> <div>2. William Stallings, „Cryptography and Network Security – Principles and Practice”, Prentice Hall, ISBN: 0-13-609704-9, 2011 (disponibila in laborator).</div> <div>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.</div> <div>4. Koc, C. K., "Cryptographic engineering", Springer Science + Business Media, LLC, ISBN: 978-0-387-71816-3, 2009.</div>			

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).

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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 naționale și internaționale de prestigiu de învățământ superior (UT din Cluj-Napoca – master Rețele de calculatoare și Sisteme distribuite, UP București, Academia Tehnică Militară București - Master Securitatea Tehnologiei Informației, MIT, NPTEL) – cursuri de securitatea informației sunt prezentate în 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 altă parte a avut întâlniri de lucru cu specialiști din producție și angajatori, inclusiv participarea la conferințe și workshop-uri din domeniu. În acest fel, disciplina respecta nivelul impus de rigorile academice și ofera în același timp abilitățile necesare pentru dezvoltarea de sisteme de securitate a informației stocate sau transmise în 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	Evaluare finală	Probă scrisă	50%
10.5 Proiect	Verificarea deprinderilor și abilităților practice dobândite de fiecare student.	Implicare în activități Realizare și prezentare proiect	10% 40%
10.6 Standard minim de performanță	Demonstrarea înțelegerii noțiunilor de bază, a principiilor și a metodelor uzuale din domeniul securității informației și abilitatea de a implementa corect, într-o aplicație proprie, primitive de securitate a informației. Admiterea proiectului (nota minimă 5) reprezintă o condiție de promovare a examenului.		

Data completării
12.09.2022

Titular de curs
Conf. dr. ing. Petre ANGHELESCU

Titular de proiect
Conf. dr. ing. Petre ANGHELESCU

Data avizării în departament
15.09.2022

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