

FIȘA DISCIPLINEI

Criptografie și securitate informațională

Anul universitar 2021-2022

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	Calculatoare și tehnologia informației
1.5	Ciclul de studii	Licență
1.6	Programul de studii / Calificarea	Calculatoare/Inginer de sistem în informatică (251203), Programator de sistem informatic (251204), Inginer de sistem software (251205)

2. Date despre disciplină

2. Date despre disciplina											
2.1	Denumirea disciplinei					Criptografie și securitate informațională					
2.2	Titularul activităților de curs					Conf. dr. ing. Petre ANGHELESCU					
2.3	Titularul activităților de laborator					Conf. dr. ing. Petre ANGHELESCU					
2.4	Anul de studii	IV	2.5	Semestrul	II	2.6	Tipul de evaluare	E	2.7	Regimul disciplinei	S/O

3. Timpul total estimat

3.1	Număr de ore pe săptămână	4	3.2	din care curs	2	3.3	laborator	2
3.4	Total ore din planul de inv.	56	3.5	din care curs	28	3.6	laborator	28
Distribuția fondului de timp								ore
Studiul după manual, suport de curs, bibliografie și notițe								18
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren								10
Pregătire seminarii/laboratoare, teme, referate, portofolii, eseuri								10
Tutoriat								2
Examinări								4
Alte activități								-
3.7	Total ore studiu individual	44						
3.8	Total ore pe semestru	100						
3.9	Număr de credite	4						

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Parcursirea disciplinelor de matematică (in special matematici speciale și algebra, capitolele referitoare la teoria numerelor).
4.2	De competențe	C1 Operarea cu fundamente stiintifice, ingineresti si ale informaticii

5. Condiții (acolo unde este cazul)

5.1	De desfășurare a cursului	Sală cu o capacitate de minim 100 locuri dotată cu două table, videoproector și ecran de proiecție.
5.2	De desfășurare a laboratorului	Laboratorul disciplinei (sala T 215), Calculatoare (minim 15), Internet, Mediul de programare Visual Studio .NET (Visual C++, C#).

6. Competențe specifice acumulate

Competențe profesionale	C5 Proiectarea, gestionarea ciclului de viata, integrarea si integritatea sistemelor hardware, software (4 puncte credit)
Competențe transversale	

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Familiarizarea studentilor cu notiunile si elementele de baza ale criptografiei si securitatii informatiei. Insusirea cunostintelor referitoare la probleme din teoria numerelor care stau la baza sistemelor criptografice, algoritmi de criptare si decriptare conventionali, algoritmi de criptare si decriptare cu cheie publica, generatoare de secvente pseudo-aleatoare. In cadrul cursului sunt prezentate tehnici de criptare/decriptare și elemente de criptanaliză.
---------------------------------------	--

7.2 Obiectivele specifice	<p><i>Obiective cognitive</i> Insușirea cunoștințelor de bază privind domeniul securității prin criptografie (criptosistem simetric și asimetric, elemente de criptanaliza).</p> <p><i>Obiective procedurale</i> Insușirea tehnicilor de bază pentru proiectarea și implementarea sistemelor criptografice ce folosesc algoritmi simetrici, respectiv asimetrici, inclusiv elemente de criptanaliza.</p> <p><i>Obiective atitudinale</i> Dobândirea deprinderilor privind ordinea și lucrul în echipă în vederea realizării rapide de aplicații criptografice utilizând limbajul C#.</p>
---------------------------	--

8. Conținuturi

8.1. Curs		Metode de predare	Observații Resurse folosite
1.	<p>Noțiuni de bază ale criptografiei (1)</p> <ol style="list-style-type: none"> <i>Terminologie și concepte folosite în criptografie:</i> Criptologie, Criptografie, Criptanaliza, Criptosistem, Cifruri bloc, Cifruri stream, Criptare hardware, Criptare software. <i>Servicii de securitate:</i> confidențialitate, integritate, disponibilitate, autenticitate, nerepudiare. <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Descriere și exemplificare Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
2.	<p>Noțiuni de bază ale criptografiei (2)</p> <ol style="list-style-type: none"> <i>Atacuri asupra securității sistemelor criptografice:</i> atacuri pasive și atacuri active – mod de operare, caracteristici. <i>Mecanisme de securitate.</i> <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Descriere și exemplificare Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
3.	<p>Sisteme criptografice</p> <ol style="list-style-type: none"> <i>Criterii de clasificare a sistemelor criptografice.</i> <i>Sisteme mecanice de criptare</i> – mașina Enigma. <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Descriere și exemplificare Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
4.	<p>Criptografie clasică (cu cheie secretă, simetrică) (1)</p> <ol style="list-style-type: none"> Clasificarea metodelor de criptare simetrice (substituție, transpoziție, combinate). Cifruri de substituție monoalfabetică (fundamente matematice, cifrul aditiv, cifrul multiplicativ). Exemple. <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
5.	<p>Criptografie clasică (cu cheie secretă, simetrică) (2)</p> <ol style="list-style-type: none"> Cifrul afin – fundamente matematice, criptare/decriptare. Criptanaliza cifrurilor de substituție monoalfabetică. Exemple. <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
6.	<p>Criptografie clasică (cu cheie secretă, simetrică) (3)</p> <ol style="list-style-type: none"> Cifruri de substituție omofonica. Criptanaliza cifrurilor de substituție omofonica. <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
7.	<p>Criptografie clasică (cu cheie secretă, simetrică) (4)</p> <ol style="list-style-type: none"> Cifruri de substituție poligramică – fundamente matematice, criptare/decriptare. Criptanaliza cifrurilor de substituție poligramică. <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
8.	<p>Criptografie clasică (cu cheie secretă, simetrică) (5)</p> <ol style="list-style-type: none"> Cifruri de substituție polialfabetică. Criptanaliza cifrurilor de substituție polialfabetică. <p>-Timp alocat 2 ore</p>	<p>Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.</p>	<p>Tabla, Calculator, Videoproiector.</p>
9.	<p>Criptografie clasică (cu cheie secretă, simetrică) (6)</p> <ol style="list-style-type: none"> Algoritmul HILL. 	<p>Prelegere Dezbateri</p>	<p>Tabla, Calculator, Videoproiector.</p>

	2. Criptanaliza algoritmului. 3. Exemple. -Timp alocat 2 ore	Studiu de caz Discuții pe o platformă online.	
10.	Criptografie clasică (cu cheie secretă, simetrică) (7) 4. Algoritmul Vigenere. 5. Criptanaliza algoritmului. 6. Exemple. -Timp alocat 2 ore	Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.	Tabla, Calculator, Videoproiector.
11.	Criptografie clasică (cu cheie secretă, simetrică) (6) 1. Cifruri de permutare/transpozitie. 2. Criptanaliza cifrurilor de permutare/transpozitie. 3. Exemple. -Timp alocat 2 ore	Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.	Tabla, Calculator, Videoproiector.
12.	Criptografie clasică (cu cheie secretă, simetrică) (7) 1. Cifrul Rail Fence – criptare/decriptare. 2. Criptanaliza. 3. Exemple. -Timp alocat 2 ore	Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.	Tabla, Calculator, Videoproiector.
13.	Criptografie clasică (cu cheie secretă, simetrică) (7) 4. Cifrul ADFGVX – criptare/decriptare. 5. Criptanaliza. 6. Exemple. -Timp alocat 2 ore	Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.	Tabla, Calculator, Videoproiector.
14.	Sistemul de criptare DES & 3DES 1. Considerații generale. 2. Descrierea sistemului criptografic DES. 3. Descrierea sistemului criptografic 3DES. -Timp alocat 2 ore	Prelegere Dezbateri Studiu de caz Discuții pe o platformă online.	Tabla, Calculator, Videoproiector.
Bibliografie 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). 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 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). 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 . 9. Stephen Wolfram, "A new kind of science", Wolfram Media Inc., ISBN: 1-57955-008-8, 2002 (disponibila in laborator). 10. Petre Angheliescu, <i>Criptografie si securitate informationala</i> – Note de curs, 2021.			
8.2. Aplicații – Laborator		Metode de predare	Observații Resurse folosite
1.	Exemplificarea unor aplicatii specifice. Implementarea și analiza cifrurilor de criptare simetrice monoalfabetice (cifrul aditiv – varianta funcțională 1 in care parola este reprezentată de numere + metode de criptanaliza). -Timp alocat 4 ore	Studiu de caz Exercițiul Lucrul în grup Dezbateri Discuții pe o platformă online.	Calculator, Visual Studio .NET (C#, Visual C++) instalat pe fiecare stație de lucru
2.	Exemplificarea unor aplicatii specifice. Implementarea și analiza cifrurilor de criptare simetrice monoalfabetice (cifrul aditiv – varianta funcțională 2 în care parola este reprezentată prin șiruri de caractere + metode de criptanaliza). -Timp alocat 4 ore	Studiu de caz Exercițiul Lucrul în grup Dezbateri Discuții pe o platformă online.	
3.	Implementarea și analiza cifrurilor de criptare simetrice monoalfabetice (cifrul Afin). -Timp alocat 4 ore	Studiu de caz Exercițiul Lucrul în grup	

		Dezbateră Discuții pe o platformă online.	
4.	Implementarea și analiza cifrurilor de criptare simetrice monoalfabetice - cifrul Polybius. -Timp alocat 4 ore	Studiul de caz Exercițiul Lucrul în grup Dezbateră Discuții pe o platformă online.	
5.	Implementarea și analiza cifrurilor de criptare simetrice poligramice – cifrul Playfair. -Timp alocat 4 ore	Studiul de caz Exercițiul Lucrul în grup Dezbateră Discuții pe o platformă online.	
6.	Implementarea algoritmilor de criptare bazati pe substitutie poligramica (cifrul Hill). -Timp alocat 4 ore	Studiul de caz Exercițiul Lucrul în grup Dezbateră Discuții pe o platformă online.	
7.	Implementarea algoritmilor de criptare bazati pe permutare/transpozitii (cifrul cu transpunere în coloane + cifrul Rail fence). -Timp alocat 4 ore	Studiul de caz Exercițiul Lucrul în grup Dezbateră Discuții pe o platformă online.	
Bibliografie <ol style="list-style-type: none"> 1. Petre Anghelescu, "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). 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, <i>Criptografie si securitate informationala</i> – Note de laborator, format electronic, 2021. 			

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 Cluj, UP București, MIT, NPTEL), iar pe de alta 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 aplicații criptografice în vederea securizării informațiilor stocate sau transmise în rețelele de telecomunicații.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Implicare în activități	Inițiative și teme	10%
	Test de verificare	Test scris la jumătatea semestrului	20%
	Evaluare finală	Probă scrisă	50%
10.5 Laborator	Verificarea deprinderilor și abilităților practice dobândite de fiecare student.	Probă practică	20%
10.6 Standard minim de performanță	<p>* Se are în vedere rezolvarea cerințelor de la lucrările de laborator și nota minimă 5 la proba practică.</p> <p>* Set de cunoștințe minimale pentru promovarea examenului final: (sa cunoasca terminologia si taxonomia sistemelor criptografice, sa descrie tipurile de atacuri criptografice, sa descrie serviciile de securitate, să descrie un sistem de criptare simetric, să descrie un sistem de criptare asimetric, să stăpânească metodele de implementare și evaluare a unui algoritm criptografic).</p>		

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