FIŞA DISCIPLINEI

Criptografie și securitate informațională

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	Calculatoare şi tehnologia informaţiei
1.5	Ciclul de studii	Licenţă
1.6	Programul de studii / Calificarea	Calculatoare/Inginer

2. Date despre disciplină

2.1	Denumirea disciplinei					***Criptografie şi securitate informațională***					
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	IV	2.5	Semestrul	I	2.6	Tipul de evaluare	E	2.7	Regimul disciplinei	S/A

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								26
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren								10
Pregătire seminarii/laboratoare, teme, referate, portofolii, eseuri								10
Tutoriat								2
Examinări								6
Alte activităţi								-

3.7	Total ore studiu individual	54
3.8	**Total ore pe semestru**	**96**
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), Bazele inteligenței artificiale.
4.2	De competenţe	**C1** Operarea cu fundamente stiintifice, ingineresti si ale informaticii

5. Condiţii (acolo unde este cazul)

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

6. Competenţe specifice acumulate

Competențe profesionale	**C5 Proiectarea, gestionarea ciclului de viata, integrarea si integritatea sistemelor hardware, software (4 puncte credit)** C5.1 Precizarea criteriilor relevante privind ciclul de viata, calitatea, securitatea si interactiunea sistemului de calcul cu mediul si cu operatorul uman (0,5 puncte credit) C5.2 Utilizarea unor cunostinte interdisciplinare pentru adaptarea sistemului informatic în raport cu cerintele domeniului de aplicatii (1 punct credit) C5.3 Utilizarea unor principii si metode de baza pentru asigurarea securitatii, sigurantei si usurintei în exploatare a sistemelor de calcul (0,5 puncte credit) C5.4 Utilizarea adecvata a standardelor de calitate, siguranta si securitate în prelucrarea informatiilor (1 punct credit) C5.5 Realizarea unui proiect incluzând identificarea si analiza problemei, proiectarea, dezvoltarea si demonstrând o întelegere a nevoii de calitate (1 punct 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 şi elemente de criptanaliză.
7.2 Obiectivele specifice	*Obiective cognitive* Insuşirea cunoştinţelor de bază privind domeniul securitatii prin criptografie (criptosistem simetric si asimetric, generatoare LFSR, criptanaliza). *Obiective procedurale* Insusirea tehnicilor de baza pentru proiectarea si implementarea sistemelor criptografice ce folosesc algoritmi simetrici, respectiv asimetrici, inclusiv elemente de criptanaliza. *Obiective atitudinale* Dobândirea deprinderilor privind ordinea si lucrul in echipa in vederea realizării rapide de aplicații criptografice utilizând limbajul C#.

8. Conţinuturi

8.1. Curs		Metode de predare	Observaţii Resurse folosite
1.	**Noțiuni de bază ale criptografiei (1)** 1. *Terminologie și concepte folosite în criptografie*: Criptologie, Criptografie, Criptanaliza, Criptosistem, Cifruri bloc, Cifruri stream, Criptare hardware, Criptare software. 2. *Servicii de securitate*: confidențialitate, autenticitate, integritate, nerepudiere, controlul accesului, disponibilitate. -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
2.	**Noțiuni de bază ale criptografiei (2)** 1. *Atacuri asupra securității sistemelor criptografice*: atacuri pasive și atacuri active – mod de operare, caracteristici. 2. *Taxonomia sistemelor criptografice*: Criptosisteme simetrice (cu cheie secretă), Criptosisteme asimetrice (cu cheie publică). -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
3.	**Sisteme mecanice de criptare** 1. *Masina Enigma* – mod de operare, caracteristici. 2. *Criptanaliza*. -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
4.	**Criptografie clasică (cu cheie secretă, simetrică) (1)** 1. Clasificarea metodelor de criptare simetrice (substituție, transpoziție, combinate). 2. Cifruri de substituție monoalfabetica (cifrul Caesar, cifrul Polybius). -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
5.	**Criptografie clasică (cu cheie secretă, simetrică) (2)** 1. Cifrul afin – cifru de substituție monoalfabetica. 2. Criptanaliza cifrurilor de substituție monoalfabetica. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
6.	**Criptografie clasică (cu cheie secretă, simetrică) (3)** 1. Cifruri de substituție omofonica. 2. Criptanaliza cifrurilor de substituție omofonica. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
7.	**Criptografie clasică (cu cheie secretă, simetrică) (4)** 1. Cifruri de substituție poligramica. 2. Criptanaliza cifrurilor de substituție poligramica. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
8.	**Criptografie clasică (cu cheie secretă, simetrică) (5)** 3. Cifruri de substituție polialfabetica. 4. Criptanaliza cifrurilor de substituție polialfabetica. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
9.	**Criptografie clasică (cu cheie secretă, simetrică) (6)** 1. Cifruri de permutare/transpozitie. 2. Criptanaliza cifrurilor de permutare/transpozitie. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
10.	**Criptografie clasică (cu cheie secretă, simetrică) (7)** 1. Cifrul ADFGVX. 2. Criptanaliza cifrurilor ce combina substitutia si transpozitia. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
11.	**Sistemul de criptare DES (Data Encryption Standard)** 1. Considerații generale. 2. Descrierea sistemului criptografic. 3. Modalități de atac asupra DES.	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.

	-Timp alocat **2 ore**		
12.	**Criptografie asimetrică (cu cheie publică)** 1. Considerații generale. 2. Funcții neinversabile. 3. Securitatea sistemelor de criptare cu cheie publică. 4. Comparație între criptarea simetrică și cea asimetrică. -Timp alocat **2 ore**	Prelegere Dezbatere Descriere şi exemplificare	Tabla, Calculator, Videoproiector.
13.	**Sistemul de criptare RSA (Rivest-Shamir Adleman)** 1. Considerații generale. 2. Descrierea sistemului criptografic RSA. 3. Exemplu. 4. Generalizarea sistemului de criptare RSA. -Timp alocat **2 ore**	Prelegere Dezbatere Studiu de caz	Tabla, Calculator, Videoproiector.
14.	**Generatoare de secvențe pseudoaleatoare.** 1. Rolul numerelor aleatoare/pseudo-aleatoare in criptografie 2. Generatoare bazate pe LFSR. 3. Metode de testare a calității secvențelor pseudoaleatoare generate. Standardul NIST. -Timp alocat **2 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).
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).
10. Petre Anghelescu, *Criptografie si securitate informationala* – Note de curs, format letric si electronic, 2017.

8.2. Aplicaţii – Laborator		Metode de predare	Observaţii Resurse folosite
1.	Implementarea și analiza cifrurilor de criptare simetrice monoalfabetice (cifrul Caesar, cifrul Polybius, cifrul Afin). -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 cifrurilor de criptare simetrice polialfabetice (cifrul Vigenere, cifrul Playfair). -Timp alocat **4 ore**	Studiul de caz Exerciţiul Lucrul în grup Dezbaterea	
3.	Implementarea algoritmilor de criptare bazati pe transpozitii. Implementarea generatoarelor de secvențe pseudoaleatoare (LFSR) utilizate la construirea algoritmilor criptografici. Utilizarea testelor statistice NIST pentru analiza calității secvențelor generate. -Timp alocat **4 ore**	Studiul de caz Exerciţiul Lucrul în grup Dezbaterea	
4.	Proba practica. Verificarea deprinderilor şi abilităţilor practice dobândite de fiecare student. -Timp alocat **2 ore**	Exerciţiul	

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, *Criptografie si securitate informationala* – Note de laborator, format electronic, 2017.

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 Cluj,

UP Bucuresti, MIT, NPTEL), 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 aplicatii criptografice in vederea securizarii informatiilor 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	Tema de casa	Referat si susținere tema	20%
	Evaluare pe parcurs	Test scris la jumătatea semestrului	20%
	Evaluare finală	Probă scrisă	50%
10.5 Laborator	Verificarea deprinderilor şi abilităţilor practice dobândite de fiecare student.	Probă practică	10%
10.6 Standard minim de performanţă	* Se are în vedere rezolvarea cerinţelor de la lucrările de laborator şi nota minimă 5 la proba practică. * 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 prezinte un generator de numere pseudoaleatoare, să stăpânească metodele de realizare și evaluare a unui algoritm criptografic).		

Data completării
17.09.2018

Titular de curs
Conf. dr. ing. Petre ANGHELESCU

Titular de laborator
Conf. dr. ing. Petre ANGHELESCU

Data avizării în departament
21.09.2018

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