Universitatea POLITEHNICA din Bucureşti
Facultatea de Ştiinţe Aplicate

FISA DISCIPLINEI
METODE STATISTICE AVANSATE PENTRU MODELAREA SISTEMELOR HAOTICE CU APLICATII ÎN CRIPTOLOGIE (M.S.A.M.S.H.A.C)

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea POLITEHNICA din Bucureşti
1.2 Facultatea	Facultatea de Ştiinţe Aplicate
1.3 Departamentul	Departamentul de Metode şi Modele Matematice
1.4 Domeniul de studii	Ştiinţe Ingineresti Aplicate
1.5 Ciclul de studii	MASTER
1.6 Programul de studii/Calificarea	TCSI/Specialist SIG/IT COD.COR 252901

2. Date despre disciplină

2.1 Denumirea disciplinei				Metode statistice avansate pentru modelarea sistemelor haotice cu aplicații în criptologie (M.S.A.M.S.H.A.C.)			
2.2 Titularul activităţilor de curs				lector dr. Raluca Purnichescu-Purtan			
2.3 Titularul activităţilor de seminar				lector dr. Raluca Purnichescu-Purtan			
2.4 Anul de studiu	I	2.5 Semestrul	I	2.6 Tipul de evaluare	Verificare pe parcurs	2.7 Regimul disciplinei	Obligatoriu

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână din care	3	3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ din care	42	3.5 curs	28	3.6 seminar/laborator	14
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					5
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					10
Tutoriat					0
Examinări					3
Alte activităţi					0

3.7 Total ore studiu individual	62
3.9 Total ore pe semestru	104
3. 10 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de competenţe	Nu este cazul

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	Nu este cazul
5.2 de desfăşurare a laboratorului	Nu este cazul

6. Competenţe specifice acumulate

Competenţe profesionale	- Dezvoltarea capacităţii de a folosi în domeniul cercetării informatice cunoştinţe de matematică modernă; - Dezvoltarea abilităţilor de folosire a sistemelor de operare UNIX şi LINUX; - Dezvoltarea capacităţii de a proiecta şi administra reţele de calculatoare; - Dezvoltarea capacităţii de a proteja serverele de atacurile informatice si de a asigura un trafic informaţional securizat; - Dezvoltarea capacităţii de lucru în echipă; - Dezvoltarea capacităţii de cercetare ştiinţifică; - În urma asimilării cunoştinţelor teoretice interdisciplinare (elemente de teoria informației, procese aleatoare, criptografie și statistică), prin propriile analize şi simulări, masteranzii își vor dezvolta capacitatea de analiză și sinteză necesară soluționării problemelor specifice criptologiei. - Asimilarea cunoştinţelor privind comportamentul statistic al sistemelor haotice va contribui la o mai bună percepere și utilizare interdisciplinară a situaţiilor determinism/haos, dependenţă/independenţă statistică, precum şi la testarea şi dezvoltarea de generatoare de date *i.i.d* (independente şi identic distribuite) cu multiple aplicaţii în criptologie.
Competenţe transversale	- Inţelegerea importanţei dobândirii și folosirii noțiunilor interdisciplinare necesare dezvoltarii profesionale; - Inţelegerea necesităţii de respectare a normelor de etică profesională şi de conduită morală.

7. Obiectivele disciplinei (reieşind din grila de competenţe specifice acumulate)

7.1 Obiectivul general al disciplinei	Aplicarea în criptologie a elementelor de teoria informației, procese aleatoare, criptografie și statistică.
4.2 Obiective specifice	**1. Cunoştinţe teoretice - Cunoaştere şi înţelegere:** Prezentarea tehnicilor şi metodelor statistice şi algoritmice utilizate în determinarea aleatorismului pentru secvențe scurte și în varianta ”next bit”. Cunoaşterea principiilor şi metodelor de aplicare a teoriei sistemelor dinamice haotice în compresie, criptare şi modulare. **2. Deprinderi dobândite - Explicare şi interpretare:** Formarea deprinderilor necesare testării, implementării şi evaluării testelor de aleatorism. Identificarea problemelor specifice algoritmizării teoriei sistemelor dinamice pentru compresie, criptare și modulare. **3. Abilităţi dobândite - Instrumental-aplicative:** Utilizarea instrumentelor de analiză şi testare a mecanismelor pentru determinarea aleatorismului. Implementarea algoritmilor specifici sistemelor dinamice haotice în diverse soluţii pentru compresie, criptare și modulare. **4. Atitudinale:** Capacitatea de lucru în echipă pentru rezolvarea unor probleme practice. Responsabilitate şi corectitudine în activităţile desfăşurate.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii

1. *Variabile aleatoare, caracteristici numerice ale variabilelor aleatoare. Repartiții clasice.* ➢ Definiții, clasificare, funcția și densitatea de probabilitate, funcția de repartiție; ➢ Media, dispersia, abaterea standard, covarianța, coeficientul de corelație. ➢ Repartiția Bernoulli, binomială, Poisson, uniformă (discretă și continuă), exponențială, normală, chi-pătrat, Student.	Predarea se realizează prin prelegere, observație, descoperire inductivă și deductivă, problematizare și algoritmizare. Materialele de curs folosite sunt videoproiectorul, notele și prezentările de curs, cursuri publicate in edituri de specialitate, on line și cu acces la bibliotecă precum și pe platforma educațională a UPB.	2 ore
2. *Elemente de statistică inferențială – Intervale de încredere, ipoteze statistice, teste parametrice și neparametrice.* ➢ Noțiunea de cuantilă, nivel de semnificație, interval de încredere; ➢ Teste parametrice (z, t, chi-pătrat); ➢ Teste neparametrice (testul de concordanță chi-pătrat, testul de concordanță Smirnov-Kolmogorov)		4 ore
3. Tehnici Monte Carlo. ➢ Metode de transformare; ➢ Teorema de transformare integrală; ➢ Generarea de eșantioane aleatoare și pseudo-aleatoare din distribuții cunoscute		2 ore
4. *Analiza statistico-informațională. Teste statistice pentru determinarea aleatorismului pentru secvențe scurte și în varianta "next bit"* ➢ Teste de frecvență (simplu și bloc); ➢ Testul serial; ➢ Testul succesiunilor; ➢ Testul rangului; ➢ Testul "random walk"; ➢ Testul de primalitate; ➢ Testul polinoamelor ireductibile		8 ore
5. *Senzitivitatea testelor de aleatorism* ➢ Teste invariante; ➢ Teste independente statistic; ➢ Teste cu efecte minimale asupra rezultatului		2 ore
6. *Corelații și autocorelații. Teste specifice*		2 ore
7. *Entropie. Teste specifice*		2 ore
8. *Aplicații ale sistemelor dinamice haotice în compresie, criptare și modulare*		6 ore

Bibliografie

1. R. Purnichescu-Purtan, *Probabilităţi şi Statistică – teorie, exerciţii, aplicaţii Matlab.* Editura Printech, 2015, ISBN 978-606-23-0522-2 .
2. E. Simion, V. Preda şi A. Popescu, *Criptanaliza. Rezultate şi Tehnici Matematice*, Ed. Univ. Buc., ISBN 973575975-6, 2004.
3. L. Kocarev, *Chaos-based cryptography: a brief overview*, IEEE Circuits and Systems Magazine ,Vol 1, Issue: 3, pp.6-21, 2001, DOI: 10.1109/7384.963463
4. G. Makris , I. Antoniou, *Cryptography with Chaos*, Proceedings, 5th Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens Greece
5. L.Kocarev, S. Lian (Eds), *Chaos-Based Cryptography*. *Theory, Algorithms and Applications*, Studies in Computational Intelligence 354, pp.1-25, Springer, 2011
6. National Institute of Standards and Technologies, SP 800-22, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, 2010.
7. M.G. Parker (Ed), *Cryptography and Coding*, Proceedings, 12th IMA International Conference Cryptography and Coding 2009, Cirencester, UK, Springer, 2009, ISSN 0302-9743

8.2. Laborator	Metode de predare	Observaţii
1. Determinarea caracteristicilor numerice ale variabilelor aleatoare din repartiții clasice	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării, utilizate frontal. Materialele didactice sunt postate pe platforma educaţională a UPB.	1 oră
2. Algoritmi pentru testele statistice (parametrice si neparametrice)		2 ore
3. Generarea de eșantioane aleatoare și pseudo-aleatoare din distribuții cunoscute (aplicarea tehnicilor Monte-Carlo)		1 oră
4. Teste statistice pentru determinarea aleatorismului pentru secvențe scurte și în varianta ”next bit”		4 ore
5. Teste de senzitivitate		1 oră
6. Teste de corelație și autocorelație		1 oră
7. Teste de entropie		1 oră
8. Algoritmi pentru compresie, criptare și modulare folosind sisteme dinamice haotice		3 ore

Bibliografie

1. R. Purnichescu-Purtan, *Probabilităţi şi Statistică – teorie, exerciţii, aplicaţii Matlab.* Editura Printech, 2015, ISBN 978-606-23-0522-2 .
2. E. Simion, V. Preda şi A. Popescu, *Criptanaliza. Rezultate şi Tehnici Matematice*, Ed. Univ. Buc., ISBN 973575975-6, 2004.
3. National Institute of Standards and Technologies, SP 800-22, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, 2010.
4. L.Kocarev, S. Lian (Eds), *Chaos-Based Cryptography*. *Theory, Algorithms and Applications*, Studies in Computational Intelligence 354, pp.1-25, Springer, 2011

9. Coroborarea conţinuturilor disciplinei cu asteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale si angajatori reprezentativi din domeniul aferent programului

Testarea statistică este o parte a unei evaluări de securitate. Testarea statistică reprezintă o parte importantă a unei evaluări de securitate, o etapă obligatorie atât în procesul de dezvoltare cât şi în cel de evaluare a unei primitive criptografice.

În criptografie, utilizarea şirurilor de numere aleatoare şi pseudoaleatoare este indispensabilă pentru a lua o decizie rapidă în ceea ce priveşte aleatorismul unei secvenţe.

Cursul are ca obiectiv dobândirea competențelor necesare conceperii, implementării și evaluării testelor de aleatorism precum și a folosirii proprietăților sistemelor haotice în compresie, criptare și modulare.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală
10.4 Curs	-cunoaşterea noţiunilor teoretice fundamentale; - cunoaşterea modului de aplicare a teoriei la probleme specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice.	Notare în timpul semestrului, teme de casă.	66%
10.5 Laborator	- cunoasterea aplicarii, pe exemple concrete a elementelor teoretice exemplificate in cadrul cursului.	Notare în timpul semestrului, teme de casă.	33%
10.6 Standard minim de performanţă			
Cunoaşterea noţiunilor teoretice de bază prezentate la curs şi rezolvarea unor probleme tip.			

Data completării **01.09.2018**

Semnătura titularului de curs
lector dr. Raluca Purnichescu-Purtan

Semnătura titularului de aplicaţii
lector dr. Raluca Purnichescu-Purtan

Data avizării în departament
.....

Semnătura sefului de department
prof. dr. Mircea Olteanu

Responsabil program master
lector dr. Emil Simion