Universitatea
Ştefan cel Mare
Suceava

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	**Universitatea „Ştefan cel Mare" Suceava**
Facultatea	**Inginerie Electrică şi Ştiinţa Calculatoarelor**
Departamentul	**Departamentul de Calculatoare**
Domeniul de studii	**Calculatoare si tehnologia informatiei**
Ciclul de studii	**Masterat**
Programul de studii/calificarea	**Stiinta si Ingineria Calculatoarelor**

2. Date despre disciplină

Denumirea disciplinei	SECURITATEA AVANSATA A SISTEMELOR INFORMATICE					
Titularul activităţilor de curs	s.l. dr. ing. Marius-Cristian CERLINCĂ					
Titularul activităţilor de seminar	s.l. dr. ing. Marius-Cristian CERLINCĂ					
Anul de studiu	I	Semestrul	1	Tipul de evaluare	Examen	
Regimul disciplinei	Categoria formativă a disciplinei DSI – Discipline de sinteză; DAP – Discipline de aprofundare					DAP
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DA - opţională (la alegere), DL - facultativă (liber aleasă)					DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore, pe săptămână	2	Curs	1	Seminar		Laborator	1	Proiect	
I.b) Totalul de ore (pe semestru) din planul de învăţământ	28	Curs	14	Seminar		Laborator	14	Proiect	

II. Distribuţia fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie şi notiţe	25
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	25
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	25
II.d) Tutoriat	20
III. Examinări	2
IV. Alte activităţi:	0

Total ore studiu individual II (a+b+c+d)	95
Total ore pe semestru (I+II+III+IV)	125
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	• sala curs, proiector, tabla, calculatoare
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	C1. Operarea cu concepte şi metode ştiinţifice avansate din calculatoare şi tehnologia informaţiei C5. Auditarea sistemelor şi serviciilor informatice
Competenţe transversale	CT1. Comportarea onorabilă, responsabilă, etică, în spiritul legii, pentru a asigura reputaţia profesiei

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	- Însuşirea cunoştinţelor teoretice fundamentale referitoare la algoritmi avansati de criptare precum si elemente de criptanaliza.

Obiective specifice	- Înţelegerea principiilor de proiectare şi analiză a unor protocoale de comunicaţie sigure.
	- Dezvoltarea deprinderilor de cercetare interdisciplinară.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Introducere in criptografie si criptanaliza. 2. Prezentarea principalelor tipuri de criptare: simetrica/asimetrica cu exemple de algoritmi istorici/moderni. 3. Functii de dispersie. 4. Elemente de criptanaliza.	2 4 4 4	Videoproiector, tablă	

Bibliografie

1. Applied Cryptography, Bruce Schneier; John Wiley & Sons, ISBN 0-471-11709-9.
2. Cryptography: Theory and Practice, Douglas R. Stinson; CRC Press, ISBN 0-8493-8521-0.
3. Information Warfare and Security, Dorothy E. Denning; ACM Press & Addison Wesley, ISBN 0-201-43303-6.
4. Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone; CRC Press, ISBN 0-8493-8523-7.
5. Cryptography in C and C++, Second Edition, Bruce Schneier, Apress, 2005
6. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Bruce Schneier, Wiley, 2005
7. Modern Cryptography: Theory and Practice, Wenbo Mao, Prentice Hall PTR, 2003
8. Introduction to Cryptography, Hans Delfs, Helmut Knebl, Springer, 2002
9. Handbook of Applied Cryptography, Alfred Menezes, CRC, 1996
10. Foundations of Cryptography, Oded Goldreich, Cambridge University Press, 2004
11. Introduction to Cryptography with Coding Theory, Wade Trappe, Lawrence C. Washington, Prentice Hall, 2002
12. Contemporary Cryptography, Rolf Oppliger, Artech House Publishers, 2005
13. Practical Cryptography, Bruce Schneier, Niels Ferguson, John Wiley & Sons Inc
14. Hiding in Plain Sight, John Wiley & Sons Inc
15. Malicious Cryptography, Moti Yung, Adam Young, John Wiley & Sons Inc
16. Protectia si securitatea informatiilor, Dumitru Oprea, Polirom, 2003

Aplicaţii (Seminar/laborator/proiect)	Nr. ore	Metode de predare	Observaţii
1. Prezentarea aplicatiei care trebuie realizata in cadrul laboratorului. 2. Implementarea unei aplicatii care foloseste metoda fortei brute/cautarea exhaustiva a cheii. 3. Implementarea unei aplicatii de criptanaliza care se bazeaza pe metoda histogramei : • analiza unui fisier criptat din punctul de vedere al frecventei de aparitie a „caracterelor” • crearea de fisiere cu frecventa de aparitie a literelor in diferite limbi de circulatie: engleza, spaniola, franceza, etc • crearea unor grafice cu histogramel folosind fisierele generate • identificarea limbii folosite intr-un text criptat folosind histogramele/fisierele generate • decriptarea textului criptat (atat cat este posibil) folosind statisticile generate	2 4 8	Indrumar laborator	

Bibliografie

17. Applied Cryptography, Bruce Schneier; John Wiley & Sons, ISBN 0-471-11709-9.
18. Cryptography: Theory and Practice, Douglas R. Stinson; CRC Press, ISBN 0-8493-8521-0.
19. Information Warfare and Security, Dorothy E. Denning; ACM Press & Addison Wesley, ISBN 0-201-43303-6.
20. Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A.

Vanstone; CRC Press, ISBN 0-8493-8523-7.
21. Cryptography in C and C++, Second Edition, Bruce Schneier, Apress, 2005
22. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Bruce Schneier, Wiley, 2005
23. Modern Cryptography: Theory and Practice, Wenbo Mao, Prentice Hall PTR, 2003
24. Introduction to Cryptography, Hans Delfs, Helmut Knebl, Springer, 2002
25. Handbook of Applied Cryptography, Alfred Menezes, CRC, 1996
26. Foundations of Cryptography, Oded Goldreich, Cambridge University Press, 2004
27. Introduction to Cryptography with Coding Theory, Wade Trappe, Lawrence C. Washington, Prentice Hall, 2002
28. Contemporary Cryptography, Rolf Oppliger, Artech House Publishers, 2005
29. Practical Cryptography, Bruce Schneier, Niels Ferguson, John Wiley & Sons Inc
30. Hiding in Plain Sight, John Wiley & Sons Inc
31. Malicious Cryptography, Moti Yung, Adam Young, John Wiley & Sons Inc
32. Protectia si securitatea informatiilor, Dumitru Oprea, Polirom, 2003

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

- **Cursuri asemanatoare din comunitatea academica si industrie:**

CS255: Introduction to Cryptography
http://crypto.stanford.edu/~dabo/cs255/
Applied Cryptography
https://www.udacity.com/course/cs387
Cryptography and Cryptanalysis
http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-875-cryptography-and-cryptanalysis-spring-2005/
Cryptographer and Entrepreneur
http://saweis.net/crypto.html
Applied Cryptography
http://courses.engr.illinois.edu/cs598man/fa2009/
CSE 107 Introduction to Modern Cryptography
http://cseweb.ucsd.edu/users/mihir/cse107/
CSE 207 Modern Cryptography
http://cseweb.ucsd.edu/~mihir/cse207/
An introduction to cryptography
https://www.ice.cam.ac.uk/component/courses/?view=course&cid=3779
650.445: PRACTICAL CRYPTOGRAPHIC SYSTEMS
http://spar.isi.jhu.edu/~mgreen/650.445/650.445__Main.html
CS 276 Cryptography
http://www.cs.berkeley.edu/~daw/teaching/cs276-s06/

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	**Cunoaşterea şi comunicarea într-o formă lizibilă a conţinutului cursului**	**Teme curs**	**50%**
Seminar			
Laborator	**Implementarea corectă a diverselor interfeţe/controlere/microprocesoare**	**Teste**	**50%**
Proiect			
Standard minim de performanţă			

Standarde minime pentru nota 5:
- capacitatea de a descrie din punct de vedere logic, sub forma de prezentare libera, a unei probleme;
- cunoaşterea a cel puţin 4 algoritmi de criptare;

Standarde minime pentru nota 10:
- capacitatea de a comunica corect si coerent pe teme de specialitate
- capacitate de sinteză, abordare logică a problemelor propuse spre rezolvare
- capacitatea de a elimina orice eroare de sintaxa din cadrul unui program realizat

- capacitatea de a identifica sursele erorilor de logica in cadrul programului - capacitatea de a obtine solutii acceptabile acolo unde este depasit de complexitatea problemei - interes pentru abordarea bibliografiei suplimentare - activitate buna în cadrul orelor de laborator - rezolvarea integrală a subiectelor de examen

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie

Data avizării în departament	Semnătura directorului de departament

Data aprobării în Consiliul academic	Semnătura decanului