R40 Anexa 1

FIŞA DISCIPLINEI
(licenţă)

1. **Date despre program**

Instituţia de învăţământ superior	**Universitatea „Ştefan cel Mare” Suceava**
Facultatea	**Inginerie Electrică şi Ştiinţa Calculatoarelor**
Departamentul	**Calculatoare**
Domeniul de studii	**Calculatoare și tehnologia informației**
Ciclul de studii	**Licență**
Programul de studii	**Calculatoare**

2. **Date despre disciplină**

Denumirea disciplinei	CRIPTOGRAFIE ȘI SECURITATE INFORMAȚIONALĂ					
Titularul activităţilor de curs	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ					
Titularul activităţilor aplicative	ș.l. dr. inf. Adina-Luminița BĂRÎLĂ					
Anul de studiu	IV	Semestrul	8	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DF - fundamentală, DD - în domeniu, DS - de specialitate, DC – complementară					DS
	Categoria de opţionalitate a disciplinei: DI - impusă, DO - opţională, DF - facultativă					DI

3. **Timpul total estimat** (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3,5	Curs	2	Seminar	-	Laborator	1,5	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	49	Curs	28	Seminar	-	Laborator	21	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	18
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	20
II d) Tutoriat	
III Examinări	3
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	48
Total ore pe semestru (Ib+II+III+IV)	100
Numărul de credite	4

4. **Precondiţii** (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. **Condiţii** (acolo unde este cazul)

Desfăşurare a cursului		• laptop, videoproiector, tablă, note de curs
Desfăşurare aplicaţii	Seminar	• -
	Laborator	• calculatoare, software specializat, laptop, videoproiector, tablă, suport electronic pentru aplicații
	Proiect	• -

6. **Competenţe specifice acumulate**

Competenţe profesionale	C1. Operarea cu fundamente ştiinţifice, ingineresti şi ale informaticii C2. Proiectarea componentelor hardware, software şi de comunicaţii C3. Soluţionarea problemelor folosind instrumentele ştiinţei şi ingineriei calculatoarelor
Competenţe transversale	CT1. Comportarea onorabilă, responsabilă, etică, în spiritul legii, pentru a asigura reputaţia profesiei CT3. Demonstrarea spiritului de iniţiativă şi acţiune pentru actualizarea cunoştinţelor profesionale,

	economice şi de cultură organizaţională

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

Obiectivul general al disciplinei	• Însuşirea cunoştinţelor teoretice fundamentale referitoare la algoritmi de criptare cu cheie pecifi şi publică
	•

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Introducere în criptografie 1.1. Istoric 1.2. Terminologie 1.3. Criptografia modernă. Cerinţe. 1.4. Algoritmi de criptare clasici	4	expunerea, prelegerea participativă, conversaţia, demonstraţia, exemplificare, studiu de caz	
2. Importanţa cheilor 2.1. Criptografia cu cheie pecifi. Descriere. Exemple. 2.2. Criptografia cu cheie publică. Descriere. Exemple.	2		
3. Criptarea prin transpoziţie 3.1. Exemple. Metode de criptanaliză. Creşterea securităţii 3.2. Algoritmul ADFGVX	2		
4. Criptarea prin substituţie 4.1. Exemple. Metode de criptanaliză. 4.2. Algoritmul PlayFair 4.3. cu cheie publica	2		
5. Tabela lui Vigenere 5.1. Metode de criptanaliză în cazul algoritmului Vigenere	2		
6. Algoritmul “Homophonic” 6.1. Metode de criptanaliză în cazul algoritmului “Homophonic” 6.2. Exemplu de criptanaliza din “The Gold-Bug” de Edgar Allan Poe.	2		
7. Algoritmul de criptare RSA 7.1. Elemente de Matematică 7.2. Prezentarea algoritmului 7.3. Exemple de criptare / decriptare.	2		
8. Maşina Enigma 8.1. Istoric 8.2. Prezentare pecifi 8.3. Detalii tehnice 8.4. Exemple de criptare / decriptare 8.5. Stabilirea cheilor şi a modului de funcţionare 8.6. Complexitatea maşinii Enigma 8.7. Slăbiciunile maşinii Enigma. Concluzii	2		
9. Algoritmul DES (Data Encryption Standard) 9.1. Istoric 9.2. Introducere în DES 9.3. DES, descriere în detaliu a criptării 9.4. DES, descriere în detaliu a decriptării 9.5. Moduri de aplicare ale algoritmului DES. Triple DES	2		
10. Algoritmi de criptare ce folosesc funcţii de dispersie 10.1. Securitatea algoritmilor de criptare ce se bazează pe funcţii de dispersie 10.2. Algoritmul MD5. Istoric. Descriere in detaliu. Exemple. 10.3. Algoritmul SHA-1. Descriere in detaliu. Exemple.	2		
11. Protocoale de stabilire a cheilor 11.1. Stabilirea si transportul cheilor in cazul criptarii cu cheie pecifi	2		

11.2. Stabilirea si transportul cheilor in cazul criptarii 11.3. Analiza protocoalelor de stabilire a cheilor			
12. Tehnici de management al cheilor 12.1. Introducere si pecifi de baza 12.2. Tehnici de distribuţie a cheilor private 12.3. Tehnici de distribuţie a cheilor publice 12.4. Concluzii	2		
13. Algoritmul AES (Advanced Encryption Standard) 13.1. Motivaţia unui nou standard 13.2. Cerinţe iniţiale 13.3. Candidaţii (MARS, RC6, Rijndael, Serpent, Twofish) 13.4. Evaluare finală a candidaţilor. Consideraţii 13.5. Descrierea algoritmului AES (Rijndael). Diagrame 2D, 3D 13.6. Implementarea algoritmului AES	2		

Bibliografie

1. Applied Cryptography, Bruce Schneier; John Wiley & Sons, ISBN 0-471-11709-9
2. Cryptography: Theory and Practice (4th Edition), Douglas R. Stinson, Maura Paterson; Chapman and Hall/CRC Press, ISBN 978-1-1381-9701-5, 2018
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

Protectia si securitatea informatiilor, Dumitru Oprea, Polirom, 2003

Bibliografie minimală

1. Applied Cryptography, Bruce Schneier; John Wiley & Sons, ISBN 0-471-11709-9
2. Cryptography: Theory and Practice (4th Edition), Douglas R. Stinson, Maura Paterson; Chapman and Hall/CRC Press, ISBN 978-1-1381-9701-5, 2018
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

Aplicaţii (laborator)	Nr. ore	Metode de predare	Observaţii
1. Prezentarea aplicaţiei ce trebuie realizată în cadrul laboratorului	1.5	expunere, lucrări practice, exerciţiu, dezbatere	
2. Implementarea algoritmului “Reverse Chiper”. Implementarea algoritmului lui Cezar	1.5		
3. Implementarea algoritmului ADFGVX	1.5		
4. Implementarea algoritmului PlayFair	1.5		
5. Implementarea algoritmului Vigenere	1.5		
6. Implementarea Algoritmului “Homophonic”	1.5		
7. Implementarea criptării RSA	1.5		
8. Implementarea decriptării RSA	1.5		
9. Implementarea criptării /decriptării Enigma	1.5		
10. Implementarea criptării/decriptării DES	1.5		
11. Implementarea Triple DES pecifi	1.5		
12. Implementarea algoritmului MD5	1.5		
13. Implementarea algoritmului SHA-	1.5		
14. Implementarea algoritmului AES	1.5		

Bibliografie

1. Applied Cryptography, Bruce Schneier; John Wiley & Sons, ISBN 0-471-11709-9.
2. Cryptography: Theory and Practice (4th Edition), Douglas R. Stinson, Maura Paterson; Chapman and Hall/CRC Press, ISBN 978-1-1381-9701-5, 2018
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

Bibliografie minimală

1. Applied Cryptography, Bruce Schneier; John Wiley & Sons, ISBN 0-471-11709-9.
2. Cryptography: Theory and Practice (4th Edition), Douglas R. Stinson, Maura Paterson; Chapman and Hall/CRC Press, ISBN 978-1-1381-9701-5, 2018
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.

9. **Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori 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	-cunoașterea terminologiei utilizate -însușirea algoritmilor de criptare fundamentali -abilitatea de rezolvare a unor probleme pecific domeniului	Evaluare sumativă prin probă teoretică	50%
Seminar	-		

Laborator	-însușirea algoritmilor specifici domeniului -capacitatea de implementare a algoritmilor specifici domeniului - abilitatea de rezolvare a unor probleme pecific domeniului	Probă practică	50%
Proiect			
Standard minim de performanţă			
- 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;			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie
26.09.2022		

Data avizării în departament	Semnătura directorului de departament
29.09.2022	

Data aprobării în consiliul facultăţii	Semnătura decanului
30.09.2022	