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/lucrări practice	1,5	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	49	Curs	28	Seminar	-	Laborator/lucrări practice	21	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	20
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	18
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, suporturi electronice pentru unitatea de curs
Desfăşurare aplicaţii	Seminar	• -
	Laborator/lucrări practice	• 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	CT1. Comportarea onorabilă, responsabilă, etică, în spiritul legii, pentru a asigura reputaţia profesiei

transversale	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 conceptelor fundamentale ale criptografiei moderne și familiarizarea cu metodele utilizate pentru securizarea sistemelor informatice

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Introducere în criptografie 1.1. Istoric 1.2. Terminologie 1.3. Criptografia modernă - cerinţe	2	expunerea, prelegerea participativă, conversaţia, demonstraţia, exemplificare, studiu de caz	
2. Algoritmi de criptare clasici 2.1. Cifruri de substituție 2.1.1. Cifruri monoalfabetice: Cezar, afin, Polybios 2.1.2. Cifruri polialfabetice: Playfair, Vigenère 2.1.3. Metode de criptanaliză 2.2. Cifruri cu tramspoziție	4		
3. Sisteme mecanice de criptare 3.1. sistemul Skitala 3.2. criptograful lui Alberti 3.3. cilindrul Jefferson	2		
4. Mașini de criptare: maşina Enigma 4.1. Istoric 4.2. Prezentare generală 4.3. Detalii tehnice 4.4. Exemple de criptare / decriptare 4.5. Stabilirea cheilor şi a modului de funcţionare 4.6. Complexitatea maşinii Enigma 4.7. Slăbiciunile maşinii Enigma. Concluzii	2		
5. Importanţa cheilor 5.1. Criptografia cu cheie privată. Descriere. Exemple. 5.2. Criptografia cu cheie publică. Descriere. Exemple.	2		
6. Algoritmi simetrici de criptare 6.1. Cifruri bloc. Rețeaua Feistel 6.2. Algoritmul DES (Data Encryption Standard) 6.2.1. Istoric 6.2.2. Introducere în DES 6.2.3. DES, descriere în detaliu a criptării 6.2.4. DES, descriere în detaliu a decriptării 6.2.5. Controverse 6.2.6. Variante ale DES (Triple DES, DES-X)	2		
7. Algoritmul AES (Advanced Encryption Standard) 7.1. Motivaţia unui nou standard 7.2. Cerinţe iniţiale 7.3. Candidaţii (MARS, RC6, Rijndael, Serpent, Twofish) 7.4. Evaluare finală a candidaţilor. Consideraţii 7.5. Preliminarii matematice – câmpuri Galois 7.6. Descrierea algoritmului AES (Rijndael) 7.7. Implementarea algoritmului AES	2		
8. Algoritmul de criptare RSA 8.1. Elemente de Matematică 8.2. Prezentarea algoritmului 8.3. Exemple de criptare / decriptare	2		
9. Algoritmi de criptare ce folosesc funcţii de dispersie 9.1. Securitatea algoritmilor de criptare ce se bazează pe funcții de dispersie 9.2. Algoritmul MD5. Istoric. Descriere in detaliu.	2		

Exemple. 9.3. Algoritmul SHA-1. Descriere in detaliu. Exemple			
10. Semnături digitale	2		
11. Atacuri criptografice	2		
12. Securizarea codului/aplicațiilor	2		
13. Securitatea bazelor de date	2		

Bibliografie

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, *Criptografie și securitatea informației. Aplicații*, Editura Matrixrom, ISBN 9789737556752, 2011
3. Dumitru Oprea, *Protecția și securitatea informațiilor,* Editura Polirom, ISBN 978-973-46-0927-7, 2007
4. Michael Welschenbach, *Cryptography in C and C++*, Second Edition, Apress, ISBN 1-59059-502-5**,** 2005
5. Douglas R. Stinson, Maura B. Paterson, *Cryptography: Theory and Practice (4th Edition)*, CRC Press, ISBN 978-1-1381-9701-5, 2018
6. Rolf Oppliger, *Cryptography 101: From theory to practice*, Artech House, ISBN 13: 978-1-63081-846-3, 2021
7. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 20th Anniversary Edition, Wiley, ISBN: 978-1-1 19-09672-6, 2015
8. Marcelo Sampaio de Alencar, *Cryptography and Network Security*, River Publishers, ISBN 978-87-7022-406-2 , 2022
9. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

Bibliografie minimală

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

Aplicaţii (Seminar / laborator / lucrări practice / proiect)	Nr. ore	Metode de predare	Observaţii
1. Prezentarea normelor de protecţia şi igiena muncii. Implementarea cifrului lui Cezar	2	expunere, lucrări practice, exerciţiu, dezbatere	
2. Implementarea cifrului PlayFair	2		
3. Implementarea cifrului Vigenere	2		
4. Implementarea cifrului cu transpoziție	2		
5. Implementarea algoritmului DES	2		
6. Implementarea algoritmului AES	2		
7. Implementarea criptării RSA	2		
8. Implementarea decriptării RSA	2		
9. Semnături digitale	2		
10. Securitatea bazelor de date	3		

Bibliografie

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. David Naccache, Emil Simio, Adela Mihăiță, Ruxandra-Florentina Olimid, Andrei-George Oprina, *Criptografie și securitatea informației. Aplicații*, Editura Matrixrom, ISBN 9789737556752, 2011
3. Dumitru Oprea, *Protecția și securitatea informațiilor,* Editura Polirom, ISBN 978-973-46-0927-7, 2007
4. Michael Welschenbach, *Cryptography in C and C++*, Second Edition, Apress, ISBN 1-59059-502-5**,** 2005
5. Douglas R. Stinson, Maura B. Paterson, *Cryptography: Theory and Practice (4th Edition)*, CRC Press, ISBN 978-1-1381-9701-5, 2018
6. Rolf Oppliger, *Cryptography 101: From theory to practice*, Artech House, ISBN 13: 978-1-63081-846-3, 2021
7. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 20th Anniversary Edition, Wiley, ISBN: 978-1-1 19-09672-6, 2015
8. Marcelo Sampaio de Alencar, *Cryptography and Network Security*, River Publishers, ISBN 978-87-7022-406-2 , 2022
9. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

Bibliografie minimală

1. Adrian Atanasiu, *Securitatea informației, vol1:Criptografie*, Editura InfoData, ISBN 978-973-1803-16-6, 2007
2. Adina Bărîlă - suporturi electronice pentru curs puse la dispoziția studenților pe Google Classroom

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

Conținutul cursului si al laboratorului este în concordanță cu așteptările reprezentanților comunității epistemice și angajatorilor reprezentativi din domeniul calculatoarelor și tehnologiei informației. De

asemeni, conținutul cursului și al laboratorului se regăsește în curricula disciplinelor similare de la universități din țară sau străinătate, cum ar fi:

- Universitatea din București/FMI – Securitatea sistemelor informatice https://cursuri.fmi.unibuc.ro/api/uploads/86c717d5-c7a6-4a60-bfad-35da223ac873.pdf
- Universitatea Politehnică Timișoara/FAC – Securitatea informației https://ac.upt.ro/specializari/informatica/
- Stanford University - CS255: Introduction to Cryptography http://crypto.stanford.edu/~dabo/cs255
- University of Illinois - CS/ECE 407: Cryptography https://courses.grainger.illinois.edu/CS407/fa2023/
- University of California, Berkeley - CS 261 Computer Security https://people.eecs.berkeley.edu/~daw/teaching/cs261-s21/
- University of Toledo - EECS 4980 - Cryptography course https://www.utoledo.edu/engineering/electrical-engineering-computer-science/current-students/syllabi/eecs-4980-inside-cryptography.html
- Texas A&M University - CSCI5323:001, Cryptography/Secure Communication https://apps.tamusa.edu/course-information/syllabi/Fall2023/Cryptography-Secure-Comm-CSCI-5323-001.pdf

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 specifice domeniului	evaluare finală: probă scrisă urmată de verificarea orală a gradului de îndeplinire a cerințelor în lucrarea scrisă	50%
Seminar	-		
Laborator	-însușirea algoritmilor specifici domeniului -capacitatea de implementare a algoritmilor specifici domeniului - abilitatea de rezolvare a unor probleme specifice domeniului	probă practică	50%
Proiect			
Standard minim de performanţă			
Curs: - însușirea noțiunilor fundamentale și utilizarea terminologiei - capacitatea de a descrie din punct de vedere logic, sub forma de prezentare libera, a cel puțin 3 algoritmi de criptare Laborator: - capacitatea de a implementa un algoritm clasic de criptare			

Data completării	Semnătura titularului de curs	Semnătura cadrului didactic coordonator
23.09.2024		

Data avizării	Semnătura responsabilului de program
24.09.2024	

Data avizării în departament	Semnătura directorului de departament
25.09.2024	

Data aprobării în consiliul facultăţii	Semnătura decanului
27.09.2024	