Universitatea Ştefan cel Mare Suceava

PROGRAMA ANALITICĂ / FIŞA DISCIPLINEI

1. **Date despre program**

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

2. **Date despre disciplină**

Denumirea disciplinei	CRIPTOGRAFIE ŞI SECURITATE INFORMAŢIONALA					
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	IV	Semestrul	8	Tipul de evaluare	Examen	
Regimul disciplinei	Categoria formativă a disciplinei DF - fundamentală, DD - în domeniu, DS - de specialitate, DC - complementară					DS
	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	5	Curs	3	Seminar		Laborator	1.5	Proiect	
I b) Totalul de ore pe semestru din planul de învăţământ	63	Curs	42	Seminar		Laborator	21	Proiect	

II Distribuţia fondului de timp pe semestru:	ore
II a)Studiul după manual, suport de curs, bibliografie şi notiţe	14
II b)Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	14
II c)Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	14
II d)Tutoriat	14
III Examinări	14
IV Alte activităţi:	14

Total ore studiu individual II (a+b+c+d)	56
Total ore pe semestru (I+II+III+IV)	133
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 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 privată şi publică.
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
Conţinutul ştiinţific al cursului **1. Introducere în criptografie.** **3h** • Istoric • Terminologie • Criptografia modernă. Cerinţe. • Algoritmi de criptare clasici	6	Videoproiector, tablă	
2. Importanţa cheilor. **3h** • Criptografia cu cheie privată. Descriere. Exemple. • Criptografia cu cheie publică. Descriere. Exemple.	3		
3. Criptarea prin transpoziţie. **3h** • Exemple. Metode de criptanaliză. Creşterea securităţii • Algoritmul ADFGVX	3		
4. Criptarea prin substituţie. **3h** • Exemple. Metode de criptanaliză. • Algoritmul PlayFair.	3		
5. Tabela lui Vigenere. **2h** • Metode de criptanaliză în cazul algoritmului Vigenere.	3		
6. Algoritmul "Homophonic". **3h** • Metode de criptanaliză în cazul algoritmului "Homophonic". • Exemplu de criptanaliza din "The Gold-Bug" de Edgar Allan Poe.	3		
7. Algoritmul de criptare RSA **4h** • Elemente de Matematică. • Prezentarea algoritmului. • Exemple de criptare / decriptare.	3		
8. Maşina Enigma **6h** • Istoric • Prezentare generală. • Detalii tehnice.	3		

• Exemple de criptare / decriptare. • Stabilirea cheilor şi a modului de funcţionare. • Complexitatea maşinii Enigma. • Slăbiciunile maşinii Enigma. Concluzii. **9. Algoritmul DES (Data Encryption Standard) 3h** • Istoric • Introducere în DES. • DES, descriere în detaliu a criptării. • DES, descriere în detaliu a decriptării. • Moduri de aplicare ale algoritmului DES. Triple DES. **10. Algoritmi de criptare ce folosesc funcţii de dispersie. 3h** • Securitatea algoritmilor de criptare ce se bazează pe funcţii de dispersie. • Algoritmul MD5. Istoric. Descriere in detaliu. Exemple. • Algoritmul SHA-1. Descriere in detaliu. Exemple. **11. Protocoale de stabilire a cheilor. 3h** • Stabilirea si transportul cheilor in cazul criptarii cu cheie privata. • Stabilirea si transportul cheilor in cazul criptarii cu cheie publica. • Analiza protocoalelor de stabilire a cheilor. **12. Tehnici de management al cheilor. 3h** • Introducere si concepte de baza. • Tehnici de distribuţie a cheilor private. • Tehnici de distribuţie a cheilor publice. • Concluzii. **13. Algoritmul AES (Advanced Encryption Standard) 3h** • Motivaţia unui nou standard. • Cerinţe iniţiale. • Candidaţii (MARS, RC6, Rijndael, Serpent, Twofish). • Evaluare finală a candidaţilor. Consideraţii. • Descrierea algoritmului AES (Rijndael). Diagrame 2D, 3D. • Implementarea algoritmului AES.	3 3 3 3 3		

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
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, 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.
Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone; CRC Press, ISBN 0-8493-8523-7.

Aplicaţii (Seminar/laborator/proiect)	Nr. ore	Metode de predare	Observaţii
1. Prezentarea aplicaţiei ce trebuie realizată în cadrul laboratorului.	1.5	Îndrumar laborator	
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 clasic.	1.5		
12. Implementarea algoritmului MD5.	1.5		
13. Implementarea algoritmului SHA-1.	1.5		
14. Implementarea algoritmului AES.	1.5		

Bibliografie

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

Bibliografie minimală

4. Applied Cryptography, Bruce Schneier; John Wiley & Sons, ISBN 0-471-11709-9.
5. Cryptography: Theory and Practice, Douglas R. Stinson; CRC Press, ISBN 0-8493-8521-0.
6. Information Warfare and Security, Dorothy E. Denning; ACM Press & Addison Wesley, ISBN 0-201-43303-6.
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 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	**Corectitudinea criptării/decriptării algoritmilor**	**Teme la curs**	**50%**
Seminar			
Laborator	**Implementarea criptării/decriptării algoritmilor**	**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