MD-2045, CHIŞINĂU, STR. Studenţilor 9/7, TEL: 022 509-908, www.utm.md

TEHNICI ŞI METODE DE CRIPTANALIZĂ

1. Date despre unitatea de curs/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de master, ciclul II				
Programul de studii	Ingineria Software				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
I	2	E	F – unitate de curs de specialitate	A - unitate de curs opțională	5

2. Timpul total estimat

Total ore în planul de învăţământ	**Din care**				
	Ore auditoriale		**Lucrul individual**		
	Curs	**Laborator/seminar**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicaţii**
150	20	20		60	50

3. Precondiţii de acces la unitatea de curs/modul

Conform planului de învăţământ	Pentru a atinge obiectivele cursului masteranzii trebuie să posede abilități de analiză și testare a soluțiilor de criptare. Aceste competenţe sunt formate de următoarele unităţile de curs: Analiza și proiectarea algoritmilor, Bazele securității informaționale, Matematica superioară, Metode criptografice de protecție a informației
Conform competenţelor	Explicarea soluțiilor inginerești prin utilizarea tehnicilor, conceptelor și principiilor din științele exacte și aplicative

4. Condiţii de desfăşurare a procesului educaţional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector şi calculator. Nu vor fi tolerate întârzierile, precum şi convorbirile telefonice în timpul cursului.
Laborator/seminar	Se vor utiliza diverse tehnici și metode de criptanaliză conform condiţiilor impuse. Termenul de predare a lucrării – o săptămână după finalizarea acesteia. Pentru predarea cu întârziere a lucrării aceasta se depunctează cu 1pct./săptămână de întârziere.

5. Competenţe specifice acumulate

Competenţe profesionale	**C1 Operarea cu concepte și metode științifice în domeniul Criptanalizei** C1.1 Identificarea și definirea conceptelor, teoriilor și metodelor privind criptanaliza C1.2 Explicarea soluțiilor de securitate prin utilizarea tehnicilor, conceptelor și principiilor științifice privind criptanaliza C1.3 Rezolvarea problemelor privind tehnicile și metodele de criptanaliză C1.4 Alegerea criteriilor și metodelor pentru analiza sistemelor de criptare C1.5 Modelarea unor probleme tip de criptanaliză folosind metodele de cerectare științifică **C3 Modelarea sistemelor complexe de securitate și implementarea lor prin sisteme informatice** C3.1 Identificarea și definirea conceptelor, procedeelor și metodelor de criptanaliză C3.2 Explicarea tehnologiilor potrivite pentru realizarea criptanalizei C3.3 Utilizarea tehnologiilor moderne în definirea metodelor de criptanaliză C3.4 Utilizarea de criterii și metode determinate de tehnologii pentru evaluarea criptanalizei C3.5 Dezvoltarea algoritmilor de criptanaliză utilizând tehnologii și sisteme moderne de criptare

6. Obiectivele unităţii de curs/modulului

Obiectivul general	Însușirea conceptelor, metodelor și tehnicilor de criptanaliză
Obiectivele specifice	Prezentarea aspectelor teoretice şi practice ale tehnicilor și metodelor de criptanaliză. Dezvoltarea capacităţii de analiză, comparare și de descriere a elementelor de criptanaliză.

7. Conţinutul unităţii de curs/modulului

Tematica activităţilor didactice	Numărul de ore învăţământ cu frecvenţă
Tematica cursului	
T.1. Abordarea teoretică şi practică a tehnicilor și metodelor utilizate în proiectarea algoritmilor şi protocoalelor criptografice	2
T.2. Abordarea teoretică şi practică a tehnicilor și metodelor de spargere/evaluare ale algoritmilor şi protocoalelor criptografice	2
T.3. Algoritmii asimetrici - securitate bazată pe dificultatea computaţională a rezolvării problemelor matematice din teoria numerelor	2
T.4. Algoritmii simetrici - securitate estimată prin raportarea la metodele de căutare exhaustiva. Tehnicile criptografice moderne utilizate în protecţia diverselor sisteme industrial de tip SCADA	2
T.5. Enigma. Enigma Cipher Machine. Enigma Keyspace. Rotors. Enigma Attack	2
T.6. RC4 as Used in WEP. RC4 Algorithm. RC4 Cryptanalytic Attack. Prevenirea atacurilor în RC4	2
T.7. Linear and Differential Cryptanalysis. Quick Review of DES. Overview of Differential Cryptanalysis. Overview of Linear Cryptanalysis. Tiny DES. Differential Cryptanalysis of TDES. Linear Cryptanalysis of TDES. Implications Block Cipher Design	4
T.8. Lattice Reduction and the Knapsack	2
T.9. RSA Timing Attacks. A Simple Timing Attack. Kocher's Timing Attack	2
Total ore de curs:	**20**
Tematica lucrărilor de laborator/seminarelor	
L.1. Enigma Attack	4
L.2. RC4 Cryptanalytic Attack	4
L.3. Differential Cryptanalysis of TDES. Linear Cryptanalysis of TDES.	4
L.4. Lattice Reduction and the Knapsack	4
L.5. RSA Timing Attacks. Kocher's Timing Attack	4
Total lucrări de laborator/seminare:	**20**
Tematica lucrului individual	
Studierea materialului teoretic	20
Studierea tematicilor de realizare a lucrărilor practice	20
Realizarea prezentărilor electronice de aprofundare a cunoștințelor	20
Total lucru individual:	**60**
Pregătire aplicații	
Enigma Attack; RC4 Cryptanalytic Attack	20
Differential Cryptanalysis of TDES. Linear Cryptanalysis of TDES	10
Lattice Reduction and the Knapsack; RSA Timing Attacks. Kocher's Timing Attack	20
Total pregătire aplicații:	**50**

8. Referinţe bibliografice

Principale	1. Mark Stamp, *Information security. Principles and Practice,* Second Edition, SanJose State University, AJOHN WILEY&SONS, USA, 2011. - 608 p. 2. A.Calder, S.Watkins, *A Manager's Guide to Data Security and ISO 27001/ISO27002*, 4th Edition, Kogan Page, 2008. 3. Constantin Popescu, *Introducere in Criptografie*, http://webhost.uoradea.ro/cpopescu/ 4. С. И. Макаренко, *Информационная безопасность,* Ставрополь СФ МГГУ им. М. А. Шолохова, 2009. 5. С. А. Нестеров, *Информационная безопасность и защита информации*, Санкт-Петербург, Издательство Политехнического университета, 2009.
Suplimentare	1. OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July2002.* www.oecd.org 2. Luminița Scripcariu, Ion Bogdan etc., *Securitatea rețelelor de comunicații*, Casa de editură Venus, Iași, 2008. - 193 p.

9. Evaluare

Nota semestrială				Evaluarea finală
Evaluarea periodică		Evaluarea curentă	Lucrul individual	
Nr.1	Nr.2			
15%	15%	15%	15%	40%
Standard minim de performanţă				
Prezenţa şi activitatea la prelegeri şi lucrări practice; Obţinerea notei minime de „5” la fiecare dintre atestări şi lucrări practice; Demonstrarea în lucrarea de examinare finală a cunoaşterii condiţiilor de aplicare a procedeelor de modelare constructivă.				
Evaluarea periodică nr.1: Test				
Evaluarea periodică nr.2: Test				
Evaluarea curentă: Lucrări practice				
Lucrul individual: Prezentări electronice				
Evaluarea finală: Test				