MD-2068, CHIŞINĂU, STR. STUDENŢILOR, 9/7, TEL: 022 50-99-63, www.utm.md

CRIPTOGRAFIE APLICATĂ

1. Date despre disciplină/modul

Facultatea	Calculatoare, Informatică şi Microelectronică				
Departamentul	Inginerie Software şi Automatică				
Ciclul de studii	Ciclul II, Studii superioare de master				
Programul de studii	Ingineria software				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
Anul I *(învăţământ cu frecvenţă)*	II	E	F – uniate de curs fundamentală	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învățământ		**Din care**				
		Ore auditoriale		**Lucrul individual**		
		Curs	**Practice**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicații**
Învățământ cu frecvență	**150**	20	20	-	60	50

3. Precondiții de acces la disciplină/modul

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

4. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector şi calculator. Nu vor fi tolerate întârzierile, precum și convorbirile telefonice în timpul cursului.
Practice	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. Competențe specifice acumulate

Competențe 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
Competențe transversale	**CT3.** Demonstrarea spiritului de inițiativă și acțiune pentru actualizarea propriilor cunoștințe profesionale, economice și de cultură organizațională.

6. Obiectivele disciplinei/modulului

Obiectivul general	Dezvoltarea competențelor teoretice și practice necesare pentru înțelegerea, proiectarea, evaluarea și aplicarea algoritmilor și protocoalelor criptografice moderne utilizate în securitatea informației și protecția datelor.
Obiectivele specifice	• Înțelegerea metodelor criptografice și clasificarea algoritmilor • Proiectarea algoritmilor criptografici siguri și eficienți • Identificarea vulnerabilităților prin tehnici de criptanaliză • Implementarea metodelor criptografice în aplicații practice • Utilizarea protocoalelor criptografice moderne pentru protecția comunicațiilor • Prevenirea atacurilor criptanalitice prin măsuri adecvate • Redactarea și interpretarea rapoartelor tehnice privind metodele criptografice

7. Conținutul disciplinei/modulului

Tematica activităților didactice	**Numărul de ore învățământ cu frecvență**
Tematica cursurilor	
T1. Abordarea teoretică şi practică a tehnicilor și metodelor utilizate în proiectarea algoritmilor şi protocoalelor criptografice	**2**
T2. Abordarea teoretică şi practică a tehnicilor și metodelor de spargere/evaluare ale algoritmilor şi protocoalelor criptografice	**2**
T3. Algoritmii asimetrici - securitate bazată pe dificultatea computaţională a rezolvării problemelor matematice din teoria numerelor	**2**
T4. Algoritmii simetrici - securitate estimată prin raportarea la metodele de căutare exhaustiva. Tehnicile criptografice moderne utilizate în protecţia diverselor sisteme industrial de tip SCADA	**2**
T5. Enigma. Enigma Cipher Machine. Enigma Keyspace. Rotors. Enigma Attack	**2**
T6. RC4 as Used in WEP. RC4 Algorithm. RC4 Cryptanalytic Attack. Prevenirea atacurilor în RC4	**2**
T7. 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**
T8. Lattice Reduction and the Knapsack	**2**
T9. RSA Timing Attacks. A Simple Timing Attack. Kocher's Timing Attack	**2**
Total curs:	**20**
Tematica lucrărilor practice	
LP1. Enigma Attack	**4**
LP2. RC4 Cryptanalytic Attack	**4**
LP3. Differential Cryptanalysis of TDES. Linear Cryptanalysis of TDES.	**4**
LP4. Lattice Reduction and the Knapsack	**4**
LP5. RSA Timing Attacks. Kocher's Timing Attack	**4**
Total lucrări practice:	**20**

8. Referințe 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. Utilizarea IA generativă

Permisiunea de utilizare	Utilizarea IA generative în cadrul temelor și proiectelor este permisă, cu condiția ca studenții să respecte următoarele reguli: • IA generativă poate fi utilizată pentru generarea de idei, structuri de text sau cod, dar toate materialele generate trebuie să fie revizuite și ajustate de către student pentru a se asigura că acestea corespund cerințelor academice. • Orice utilizare a IA generative trebuie să fie declarată în secțiunea de apendice a fiecărei lucrări, folosind fraza: "În timpul pregătirii acestei lucrări, autorul a utilizat [NUME INSTRUMENT / SERVICIU] în scopul [MOTIV]. După utilizarea acestui instrument/serviciu, autorul a revizuit și editat conținutul după cum a fost necesar și își asumă întreaga responsabilitate pentru conținutul lucrării."
Restricții de utilizare	Studenții nu trebuie să considere IA generativă ca o sursă de încredere pentru informații, deoarece nu oferă referințe clare sau surse documentate. • Nu este permisă citarea directă a conținutului generat de IA în lucrările academice ca și cum ar fi sursă primară. • Activitățile în care este interzis utilizarea IA generativă sunt specificare de profesor și sunt de regulă evaluări intermediare și finale sau care nu presupun activități de dezvoltare a competenților profesionale.

10. Evaluare

Periodică		**Curentă**	**Studiu individual**	**Proiect/teză**	**Examen**
EP 1	**EP 2**				
Învăţământ cu frecvenţă					
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.					

11. Criterii de evaluare

Activitate	**Componente evaluare**	**Metodă de evaluare, criterii de evaluare**	**Pondere în nota finală a activității**	**Ponderea în evaluarea disciplinei**
Evaluare periodică I	Conținut teoretic Teme 1-4	Test electronic pe platforma else.fcim.utm.md	100%	**15%**
Evaluare periodică II	Conținut teoretic Teme 5-9	Test electronic pe platforma else.fcim.utm.md	100%	**15%**
Evaluare curentă	Participare, lucrări practice, rapoarte	Participarea la activități, calitatea și acuratețea realizării lucrărilor practice, pregătirea și susținerea rapoartelor	100%	**15%**
Studiul individual	Prezentarea unui articol științific	Prezentare orală/discurs la tema articolului în fața colegilor; evaluarea coerenței, clarității și documentării	100%	**15%**
Evaluarea finală	Conținut teoretic și practic	Test electronic pe platforma else.fcim.utm.md	100%	**40%**