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

CRIPTOGRAFIE ŞI SECURITATE

1. Date despre unitatea de curs

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/Departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studii	0613.3 Ingineria software				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opționalitate**	**Credite ECTS**
III (învățământ cu frecvență)	5	E-examen	**D** - Disciplină de domeniu profesional	**O** - unitate de curs obligatorie	4

2. Timpul total estimat

Total ore în planul de învățământ	**Din care**					
	Ore auditoriale		**Lucrul individual**			
	Curs	**Laborator**	**Seminar**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicații**
120	30	30	-	-	60	-

3. Precondiții de acces la unitatea de curs

Conform planului de învățământ	Cunoștințe fundamentale din matematica elementară și superioară, din teoria structurilor de date și a algoritmilor, abilități de programare imperativă
Conform competențelor	Competențe de programare imperativă (procedurală, OOP)

4. Condiții de desfășurare a procesului educațional

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector, PC/laptop și acces la internet. Nu vor fi tolerate întârzierile studenților, precum și convorbirile telefonice în timpul cursului
Laborator/Seminar	Studenții vor perfecta rapoarte conform condițiilor impuse de indicațiile metodice. Termenul de predare a lucrării de laborator – 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	CP 2. Proiectarea și dezvoltarea aplicațiilor CP 3. Integrarea componentelor CP 4. Furnizarea de servicii CP8. Ingineria sistemelor. Managementul problemelor
Competențe transversale	22T. Autonomie şi responsabilitate 23T. Interacţiune socială 24T. Dezvoltare personală şi profesională

6. Obiectivele unității de curs

Obiectivul general	Însușirea primitivelor criptografice și a sistemele criptografice comune, modurile lor de funcționare și interacțiune, precum și familiarizarea cu librăriile criptografice ale limbajelor de programare moderne pentru elaborarea aplicațiilor software cu asigurarea confidențialității, integrității, autenticității și a non-repudierii informației și a altor atribute de securitate adiacente, care sunt asigurate de criptografie.

Obiectivele specifice	Operarea cu concepte criptografice specifice (algoritm de criptare, criptare cu cheie privată, criptare cu cheie publică, funcție hash criptografică, semnătură digitală autentificarea mesajelor, etc.); alegerea primitivelor criptografice cele mai potrivite pentru asigurarea nivelului optim de securitate informațională în diverse contexte.

7. Conținutul unității de curs

Tematica cursului	**Numărul de ore învățământ cu frecvență**
T1. Introducere în securitatea informației	2
T2. Cifruri clasice	4
T3. Algoritmi de criptare fluidă	4
T4. Algoritmi de criptare de tip bloc	4
T5. Criptografia cu chei publice	4
T6. Funcții hash criptografice	2
T7. Coduri de autentificare a mesajului (MAC)	4
T.8. Scheme de semnătură digitală.	4
T9. Stabilirea cheilor criptografice.	2
Total ore de curs:	**30**
Tematica lucrărilor de laborator	**Numărul de ore învățământ cu frecvență**
LL1. Cifruri de substituție monoalfabetică și permutare	4
LL2. Criptanaliza cifrurilor de substituție monoalfabetică	2
LL3. Cifruri de substituție polialfabetică	2
LL4. Algoritmi de criptare fluidă	4
LL5. Algoritmi de criptare de tip bloc	6
LL6. Criptografia cu chei publice	4
LL7. Coduri de autentificare a mesajelor	4
LL8. Semnături digitale	4
Total lucrări de laborator/seminare:	**30**

Tematica lucrului individual	**Numărul de ore învățământ cu frecvență**
1. Incidentele de securitate conexe criptografiei.	8
2. Evoluția criptografiei clasice.	4
3. Cifruri fluide.	10
4. Cifruri bloc	10
5. Algoritmii de criptare cu cheie publică	10
6. Funcții hash criptografice	10
7. Funcții de autentificare a mesajelor	8
Total lucrul individual:	**60**

8. Referinţe bibliografice

Principale	1. Materialele didactice plasate pe pagina platformei ELSE: https://else.fcim.utm.md/course/view.php?id=1680 2. Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC; 2nd edition, 2014, 603 p. ISBN-10: 9781466570269. 3. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, Wiley, 2015, 784 p. ISBN-10: 1119096723. 4. Zgureanu A. *Fundamente ale criptografiei moderne*, Chișinău, ed. ASEM, 2023, 237 p. ISBN: 978-9975-147-81-1. 5. Венбо Мао. *Современная криптография. Теория и практика*. Вильямс, 2005. 768 с.
Suplimentare	1. Dan Boneh. Online Cryptography Course, Stanford University, https://crypto.stanford.edu/~dabo/courses/OnlineCrypto/. 2. Jaydip Sen. *Theory and Practice of Cryptography and Network Security Protocols and Technologies*. Edited by Jaydip Sen, Praxis Business School, 146 p, 2013. https://freecomputerbooks.com/Theory-and-Practice-of-Cryptography-and-Network-Security-Protocols-and-Technologies.html 3. Oded Goldreich. *The Foundations of Cryptographys*, Volume 1, Basic Tools. Pub: Cambridge University Press; 1 edition, 2007, 396 p. https://freecomputerbooks.com/Foundations-of-Cryptographys-Volume-1-Basic-Tools.html **Site-uri utile:** 1. *Cryptography*, University of Maryland, online course: https://www.classcentral.com/course/cryptography-1730; 2. *Cryptography I*, Stanford University, online course: https://www.classcentral.com/course/crypto-616 3. *Basic Cryptography and Programming with Crypto API*, University of Colorado System, online course: https://www.classcentral.com/course/basic-cryptography-and-crypto-api-9531; 4. Cărți despre securitatea informației cu liber acces: https://freecomputerbooks.com/compscspecialSecurityBooks.html 5. Cărți despre criptografie cu liber acces: http://www.freebookcentre.net/Security/Free-Cryptography-Books-Download.html

9. Utilizarea IA generativă

Permisiunea de utilizare	Utilizarea IA generative în cadrul temelor şi proiectelor este permisă, cu condiţia ca studenţii 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 şi ajustate de către student pentru a se asigura că acestea corespund cerinţelor academice. • Orice utilizare a IA generative trebuie să fie declarată în secţiunea 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 şi editat conţinutul după cum a fost necesar şi îşi asumă întreaga responsabilitate pentru conţinutul lucrării".
Restricţii de utilizare	Studenţii nu trebuie să considere IA generativă ca o sursă de încredere pentru informaţii, deoarece nu oferă referinţe clare sau surse documentate. • Nu este permisă citarea directă a conţinutului generat de IA în lucrările academice ca şi cum ar fi sursă primară. • Activităţile în care este interzis utilizarea IA generativă sunt specificare de profesor şi sunt de regulă evaluări intermediare şi finale sau care nu presupun activităţi de dezvoltare a competenţilor profesionale.

10. 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.				

11. Evaluare

Tip de evaluare	Criterii de evaluare	Metode de evaluare
Evaluarea periodică nr.1	Evaluarea abilităților teoretice și practice pentru temele T1-T3	Test grilă
Evaluarea periodică nr.2	Evaluarea abilităților teoretice și practice pentru temele T4-T8	Test grilă
Evaluarea curentă	Predarea la timp a lucrărilor individuale, activitatea curentă la lucrările de laborator	Evaluarea în baza îndeplinirii criteriilor de evaluare.
Lucrul individual	Dezvoltarea a două subiecte legate de temele 1-7 ale lucrului individual	Referat
Evaluarea finală	Punctajul acumulat conform baremului în urma rezolvării unui Test grilă/ unei sarcini de tip lucrare practică.	Test grilă ELSE care acoperă subiectele cu caracter teoretic ale cursului Criptografie/ sarcină practică la calculator.