Ministerul Educaţiei al Republicii Moldova
Universitatea de Stat „Alecu Russo” din Bălți
Facultatea de Științe Reale, Economice și ale Mediului
Catedra de matematică și informatică

CURRICULUM

la unitatea de curs

„CRIPTOGRAFIE”

Ciclul I, studii superioare de licență
Codul şi denumirea domeniului general de studiu: 44 Științe exacte
Codul şi denumirea specialităţii: 444.1 Informatica
Forma de învăţământ: cu frecvenţă la zi

Autor:
lect.univ., Adela GOREA

Bălți, 2017

Discutat şi aprobat la şedinţa Catedrei de matematică și informatică

Procesul-verbal nr.____ din _____

Şeful Catedrei de matematică și informatică

_____ conf. univ., dr. Eugeniu PLOHOTNIUC

Discutat şi aprobat la şedinţa Consiliului Facultăţii de Ştiinţe Reale, Economice şi ale Mediului,

Procesul-verbal nr. ____ din _____

Decanul Facultăţii de Ştiinţe Reale, Economice şi ale Mediului

_____ conf. univ., dr. Ina CIOBANU

I. Informații de identificare a unității de curs

Facultatea: Științe Reale, Economice și ale Mediului

Catedra: Matematică și informatică

Domeniul general de studiu: 44 Științe exacte

Domeniul de formare profesională la ciclul I: 444 Informatica

Denumirea specialității: 444.1 Informatica

Denumirea unității de curs: Criptografie

Administrarea unității de curs:

Codul unității de curs	Credite ECTS	Total ore	Repartizarea orelor				Forma de evaluare	Limba de predare
			Prel.	Sem.	Lab.	Lucrul ind.		
S.05.A.140	5	150	30	0	45	75	Examen	Rom/rus

Anul de studiu și semestrul în care se studiază: Anul III, semestrul 5.

Statutul: la liberă alegere

Localizarea sălilor: curs – aula 141, laboratoare – aula 158, 141a, 150.

I. Informații referitoare la cadrul didactic

Adela Gorea, lector universitar, absolventa Universităţii de Stat „A. Russo” din Bălți, specialitatea „Informatică”. A efectuat studiile de master la specializarea „Tehnologii informaționale și comunicaționale în învățământ”.

E-mail:adelaosadta@gmail.com

Orele de consultaţii – marți: 14.00 -15.30. Consultaţiile se oferă atât în regim „faţă-în-faţă”, cât şi prin utilizarea poştei electronice, Skype. Numele în Skype – adela_gorea

II. Integrarea unității de curs în programul de studii

Cursul „Criptografie” este un curs de specializare care se bazează pe studiu asupra algoritmilor matematici fundamentali utilizați în criptografie. Disciplina dată, prin aria sa aplicativă, aparţine domeniului de asigurarea securităţii, siguranţei şi uşurinţei în exploatare şi pune la dispoziţie cunoştinţele necesare analizei, proiectării, testării şi implementării sistemelor de criptare şi securizare a transferului de date între diferite entităţi informaţionale.

Studierea unităţii de curs „Criptografie” se sprijină pe cunoştinţele, capacităţile şi competenţele dezvoltate în cadrul disciplinei „Matematica I, II”, „Programarea Structurată”, „Baze de date”, „Structuri discrete”, „Rețele de calculatoare”, studiată la ciclul I. Finalităţile şi conţinutul unităţii de curs sunt corelate cu finalităţile şi conţinuturile unităţilor de curs menționate mai sus.

Cursul este destinat studenţilor de la specialitatea „Informatica (științe exacte)” studii superioare de licență a Facultăţii de Ştiinţe Reale, Economice și ale Mediului. Este o disciplină la libera alegere pentru viitorii specialiști în informatică.

Prin conţinutul său şi activităţile de învăţare a studenţilor, cursul „Criptografie” contribuie la dezvoltarea mai multor competenţe generice, necesare profesorului de informatică:

- capacitatea de analiză şi sinteză;
- deprinderi de gestiune a informaţiei (extragerea şi analiza informaţiei din diverse surse);
- capacitatea de a lucra în echipă;
- ataşamentul la valorile etice;
- capacitatea de a aplica cunoştinţele în practică;
- capacitatea de a genera idei noi;
- capacitatea de a lucra independent.

III. Competenţe prealabile:

1. Utilizarea eficientă a resurselor sistemelor de calcul, de operare și ale Internetului.
2. Dezvoltarea de componente pentru produse software, folosind structuri de date, algoritmi, tehnici și limbaje de programare evoluate.

IV. Competențele formate/dezvoltate în cadrul unității de curs

În cadrul studierii disciplinei la studenți vor fi dezvoltate următoarele competențe:

CP1. Operarea cu fundamentele științifice ale informaticii și matematicii și utilizarea acestor noțiuni în comunicarea profesională.

CP2. Elaborarea modelelor pentru descrierea fenomenelor și proceselor reale.

CP3. Proiectarea, elaborarea și analiza algoritmilor pentru rezolvarea problemelor.

CP4. Programarea, dezvoltarea și mentenanța aplicațiilor informatice în limbaje de nivel înalt .

CP5. Integrarea tehnologiilor informaţionale in diferite domenii ale economiei naţionale.

CP6. Prelucrarea datelor, analiza și interpretarea lor.

CT1. Aplicarea regulilor de muncă riguroasă și eficientă, manifestarea unei atitudini responsabile față de domeniul profesional, pentru valorificarea optimă și creativă a propriului potențial în situații specifice, cu respectarea principiilor și a normelor de etică profesională.

V. Finalităţile unității de curs

La finalizarea studierii disciplinei și realizarea sarcinilor de învățare studentul va fi capabil:

La finalizarea studierii cursului studentul va fi capabil:

- să prezinte noțiuni teoretice și practice ale criptografiei;
- să-și formeze și dezvolte gândirea pe baza noțiunilor matematice, criptografice învățate;
- să elaboreze algoritmi legați de criptografia clasică, algoritmilor legați de sistemele criptografice cu cheie privată, respectiv prezentarea securității acestor sisteme;
- să prezinte noțiunile matematice legate de sistemele criptografice cu cheie publică;
- să implementeze algoritmii învățați într-un limbaj de programare ca de exemplu: C++, #C, Java.

VI. Conținuturi

Conținuturi

Nr. d/o	Subiectele predate	Nr.de ore
1.	Istoria Criptografiei. Elemente fundamentale.	2
2.	Criptosisteme. Semnături Digitale.	2
3.	Atacuri de securitate. Servicii de securitate. Mecanisme de securitate. Definiția criptografiei.	2
4.	Probleme din teoria numerelor. Problema logaritmilor discreţi. Problema de reprezentare.	2
5.	Problema Diffie-Hellman. Factorizarea numerelor întregi mari. Problema logaritmului discret pe o curbă eliptică.	2
6.	Criptografia convenţională. Cifruri substituţie. Cifrul lui Cezar. Modelul unui criptosistem convenţional.	2
7.	**Evaluare curentă**.	2
8.	Tipuri de atacuri.	2
9.	Cifruri monoalfabetice. Cifruri polialfabetice. Cifrul Vigenere. Cifrul transpoziție. Cifrul DES.	2
10.	Cifrul triple DEA. Cifrul IDEA. Cifrul Blowfish. Cifrul RC5. Moduri de cifrare	2
11.	Criptografia cu chei publice. Criptarea cu chei publice. Semnătura digitala. Funcții greu inversabile. Criptosistemul RSA.	2
12.	Criptosistemul ElGamal. Algoritmul Diffie-Hellman. Criptografia bazata pe curbe eliptice. Recomandări pentru alegerea cheilor RSA	2
13.	Curbe eliptice peste câmpuri finite. Operaţia de adunare pe o curbă eliptică. Criptosistemul ElGamal bazat pe curbe eliptice. Problema logaritmilor discreţi pe o curbă eliptică. Funcţii hash. Comparaţie între funcţiile hash.	2
14.	Semnături digitale. Schema de semnătură RSA. Schemamail.ru de semnătură ElGamal. Schema de semnătură DSA.	2
15.	**Evaluare finală.**	2
Total		**30**

Temetica lecțiilor de laborator

Nr. d/o	Tematica	Nr. de ore
1.	Sistemul de cifrare Cezar.	2
2.	Metoda substituției.	2
3.	Sistemul de cifrare Playfair .	2
4.	Sistemul de cifrare Hill.	2
5.	Sisteme de cifrare polialfabetice.	2
6.	Metoda transpoziției.	2

7.	Sisteme mixte.	2
8.	Generatoare pseudoaleatoare. Calcule în corpuri Galois. Algoritmul RIJNDAEL - Standardul AES.	2
9.	**Sarcini individuale nr. 1**	2
10.	Criptanaliza cifrurilor bloc.	2
11.	Sistemul de cifrare Merkle-Hellman.	2
12.	Sistemul de cifrare RSA	2
13.	Sistemul de cifrare ElGamal	2
14.	Aritmetica pe curbe eliptice	2
15.	Sistemul de cifrare ElGamal bazat pe curbe eliptice	2
16.	Sistemul de cifrare Menezes-Vanstone	2
17.	Semnătura ElGamal	2
18.	Semnătura DSA.	2
19.	Protocolul Diffie-Hellman de stabilire a cheilor	2
20.	Sistemul Shafir de partajare a secretelor. Principii criptografice. Atacuri in mediul de implementare.	2
21.	**Sarcini individuale nr. 2**	2
22.	***Susținerea proiectului Testarea aplicațiilor.***	3
Total		**45**

VII. Activități individuale

Proiectul va presupune elaborarea unei aplicații de criptare a datelor care rezolvă o problemă din viața reală. Aplicația va conține și o descriere a problemei soluționate și a modului în care a fost rezolvată. Codul aplicației va avea comentarii explicative. Descrierea aplicației va fi prezentate într-un raport editat într-un document Word pe 3-4 pagini format A4, font #12, 1.5 intervale. Activitatea va fi evaluată atât de către colegi cât şi de către titularul disciplinei într-o şedinţă aparte.

Criterii de evaluare:

- Corectitudinea rezolvării problemei prin elaborarea aplicației;
- Relevanța și valoarea comentariilor;
- Exactitate (logică, ortografică) a raportului prezentat;

Termenul limită (deadline) de prezentare a sarcinii – perechea a 22-a (lucrare de laborator)

VIII. Principiile de lucru în cadrul unității de curs

1. O parte din sarcinile de învăţare vor fi propuse pentru realizare în grupe mici prin cooperare. Deşi activitatea de învăţare va fi una colectivă, notele pentru realizarea sarcinilor vor fi individuale. Prezentarea sarcinilor realizate va fi însoțită de o evaluare reciproca a membrilor subgrupului pentru a identifica aportul fiecărui membru în rezultatul final.
2. Calendarul cursului (termenii-limită de prezentare a sarcinilor propuse spre rezolvare, momentele de evaluare etc.) este corelat cu calendarele la alte discipline din semestru. De aceea prezentarea sarcinilor după termenul-limită indicat în calendar nu este salutată, iar studenţii care amână frecvent prezentarea sarcinilor îşi formează o imagine nefavorabilă.
3. Nu este salutată întârzierea la ore.
4. Este salutată poziția activă a studentului, care studiază din propria iniţiativă noi conținuturi, propune soluții, formulează întrebări în cadrul prelegerilor şi a orelor practice.
5. În cadrul disciplinei o atenție sporită va fi oferită respectării principiilor *etice*. Prezentarea unor soluții a sarcinilor, preluate de la colegi sau din alte surse, preluarea informaţiilor din diverse surse, fără a face trimitere la sursă, va fi considerată *plagiat* şi va fi sancționată prin note de „1” .

Evaluarea

Cunoştinţele, capacităţile şi competenţele studenţilor vor fi evaluate:

1. La prelegeri (**PR**):
   1.1.Lucrare de control scrisă: perechea a 7-a (**LC1**).
   1.2.Lucrare de control scrisă: perechea a 15-a (**LC2**).
2. În cadrul lecţiilor de laborator (**LLab**):
   2.1.Sarcini individuale nr. 1: perechea a 9-a (**SI1**)
   2.2.Sarcini individuale nr. 2: perechea a 21-a (**SI2**)
   2.3.Proiect: perechea a 22-a (**Pro**)
3. La examenul final, conform orarului întocmit de decanat (**Ex**).

Nota finală la disciplina „*Reţele media sociale*” se calculează conform formulelor:

N_evaluarea_curentă=1/2x**PR**+1/2x**LLab**

N_finală=0,6x*N_evaluarea_curentă*+ 0,4x*N_examen*,

Unde **PR**=(**LC1+LC2)**/2 și **LLab**=(**SI1**+**SI2+Pro**)/3

Examenul final se susţine scris, care va include un test complex cu diferite tipuri de item.

Pentru a fi admis la examen, este obligator ca ambele note (**PR** și **LLab**) să fie pozitive.

Recuperarea notelor și susținerea repetată a examenului are loc în datele stabilite de orarul întocmit de decanat de susținere a restanțelor.

Baremul

de convertire a punctajului în note

pentru examenul de evaluare a cunoştinţelor la disciplina

„*Criptografie*”

(în baza REGULAMENTULUI

cu privire la evaluarea rezultatelor academice ale studenţilor în Universitatea de Stat „Alecu Russo” din Bălţi)

Procentajul	**Nota**
100 – 91	10
90 – 81	9
80 – 71	8
70 – 66	7
65 – 61	6
60 – 51	5
50 – 41	4
40 – 31	3
30 – 16	2
15 – 0	1

Resursele informaţionale la disciplină

A. Literatura de bază

1. Popescu, Introducere în criptografie, Editura Universitatii din Oradea, Oradea, 2001;
2. Schneier, Applied Cryptography, JohnWiley &Sons, SUA, 1996;

B. Literatura suplimentară

1. Handbook of Applied Cryptography: Alfred Menezes, Paul van Oorschot, Scott Vanstone, CRC Press, ISBN 0-8493-8523-7, 1996;
2. Nicolae Constantinescu, *Criptografie*, Editura Academiei Romane, 2009;
3. Douglas R. Stinson, *Cryptography: Theory and Practice*, Third Edition, Chapman and Hall/CRC - November 01, 2005;
4. Understanding Cryptography: A Textbook for Students and Practitioners, Paar, Pelzl
5. Curiac – Algoritmi de criptare pentru securizarea datelor, Ed. Politehnica, 2005
6. N. Constantinescu – Criptografie, Ed. Academiei Române, 2009.