МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Факультет математики та інформатики

Кафедра алгебри та геометрії

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КРИПТОЛОГІЯ ТА ЕЛЕМЕНТИ ЗАХИСТУ ІНФОРМАЦІЇ

Освітня програма: Математика

Спеціальність: 111 Математика

Галузь знань: 11 Математика та статистика

Затверджено на засіданні кафедри
Протокол № 7 від 29 березня 2022 р.

м. Івано-Франківськ – 2022 рік

ЗМІСТ

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

Назва дисципліни	Криптологія та елементи захисту інформації
Викладач(-і)	Мазуренко Н.І.
Контактний телефон	(0342)596016
E-mail	nataliia.mazurenko@pnu.edu.ua
Формат дисципліни	Лекції та практичні заняття
Обсяг дисципліни	6 кредитів
Консультації	Вівторок, 15^{00}

2. АНОТАЦІЯ ДО КУРСУ

Криптологія охоплює криптографію – науку про збереження таємниці тексту, та криптоаналіз – науку про проникнення у таємницю захищеного тексту. Із появою ідеології відкритого ключа криптографічна практика почала використовувати фундаментальні результати теорії чисел і одночасно стала джерелом нових глибоких математичних задач. Як наслідок, на сьогоднішній день криптологія перетворилась на математичну дисципліну з класичною структурою: означення – теорема – доведення.

Гармонійне поєднання в цьому курсі математичного аспекту криптології з прикладним (захист інформації) робить його однаково привабливим як для теоретиків, так і для практиків.

3. МЕТА ТА ЦІЛІ КУРСУ

Курс забезпечує набуття знань з математичних основ криптографічного захисту інформації. Його метою є виклад базових принципів побудови математичного обгрунтування криптографічних систем, а ціллю – навчити студента реалізовувати базову версію шифрування з відкритим чи симетричним ключами, знаходити обернений елемент у кільці лишків, дискретний логарифм, тестувати простоту числа.

4. КОМПЕТЕНТНОСТІ

- Здатність до абстрактного мислення, аналізу та синтезу, до застосування теорії у практичних ситуаціях;

- Здатність до пошуку та інтерпретації інформації, засвоєння нових знань, генерування та викладу ідей, зокрема, з застосуванням інформаційних технологій;
- Здатність працювати як автономно, так і у складі наукового, зокрема, інтернаціонального, колективу фахівців з усвідомленням відповідальності за результати роботи;
- Здатність вести дослідницьку діяльність, включаючи оцінку актуальності дослідження, аналіз проблем, вибір способу й методів дослідження, а також оцінку якості результатів.
- Цілісне уявлення про математику, її сучасний стан, виникнення і шляхи розвитку, її місце у системі наукових знань людства;
- Здатність зрозуміти постановку завдання, пов'язаного із застосуванням математичних методів захисту інформації;
- Здатність математично формалізувати проблему прикладного характеру;
- Здатність обирати та застосовувати математичні методи для розв’язування практичних задач;
- Уміння ефективно співпрацювати, розподіляти роботу і спілкуватись з колегами в процесі командного виконання дослідницьких та програмних проектів;
- Здатність до побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення та аналізу алгоритмів, оцінювання їх ефективності та складності для адекватного моделювання предметних областей і створення програмних та інформаційних систем;
- Здатність застосовувати основні методи та алгоритми прийняття рішень в умовах наявності нечіткої вхідної інформації, здійснювати аналіз отриманих результатів.

5. РЕЗУЛЬТАТИ НАВЧАННЯ

- демонструвати знання й розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці, а також гуманітарних дисциплін підготовки фахівця;
- володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел;
- знати де виникають задачі криптології і основні принципи ефективної формалізації таких задач;

- самостійно працювати над дослідницькою темою, обґрунтовувати і створювати програмну реалізацію розроблених методів;
- знати основні поняття криптології, способи захисту інформації та найпростіші методи шифрування. Знати функціональні можливості застосування сучасних пакетів програмної реалізації криптографічних перетворень та криптографічних бібліотек;
- уміти проводити наукові дослідження, грамотно викладати і представляти опрацьований матеріал і власні результати, в тому числі і з сучасними можливостями візуалізації, створювати комп'ютерну реалізацію розроблених методів.

6. ОРГАНІЗАЦІЯ НАВЧАННЯ КУРСУ

Обсяг курсу	
Вид заняття	Загальна кількість годин
Лекції	30
Практичні	30
Самостійна робота	120

Ознаки курсу				
Спеціальність, освітня програма	Рівень освіти	Курс (рік навчання)	Семестр	Нормативна/ вибіркова
111 математика	Бакалавр	4ий	7ий	вибіркова

Тематика курсу					
Тема, план	Форма заняття	Література	Завдання, год	Вага оцінки	Термін виконання
Елементарна криптографія - абетка - класичні методи - пропозиції XX століття	лекція практ сам. роб.	[1–3, 5, 8]	4 ауд. год., **8** год. с. р.		1 тиждень
Шифри заміни та перестановки, блокові шифри	лекція практ сам. роб.	[1, 3]	4 ауд. год., **8** год. с. р.		2 тиждень
Блокове та потокове шифрування	лекція практ сам. роб.	[1, 3]	4 ауд. год., **8** год. с. р.		3 тиждень
Елементарна криптографія (математичний підхід) - формалізм - арифметика - афінні шифри	лекція практ сам. роб.	[1, 2, 7]	4 ауд. год., **8** год. с. р.		4 тиждень
Афінні шифри	лекція практ сам. роб.	[1, 3, 7, 8]	4 ауд. год., **8** год. с. р.		5 тиждень
Основні види атак, принципи криптоаналізу	лекція практ сам. роб.	[1, 3, 7, 8]	4 ауд. год., **8** год. с. р.		6 тиждень
Складність арифметичних задач - первісні корені - квадратичні лишки - розподіл простих чисел - тестування простоти	лекція практ сам. роб.	[1, 6, 7]	10 ауд. год., **8** год. с. р.		7-9 тиждень

- факторизація - розпізнавання квадратичності і добування квадратних коренів - первісні корені за простим модулем - дискретний логарифм					
Арифметичні задачі в криптології	лекція практ сам. роб.	[1, 3, 6, 7]	4 ауд. год., **8** год. с. р.		10 тиждень
Криптосистеми з відкритим ключем - концепція - RSA - система Рабіна - ймовірнісне криптування - система Ель Гамаля	лекція практ сам. роб.	[1, 3, 4, 8]	8 ауд. год., **8** год. с. р.		11-12 тиждень
Криптографія з відкритим ключем. - електронний цифровий підпис - криптографічні протоколи	лекція практ сам. роб.	[1, 3, 4, 8]	4 ауд. год., **8** год. с. р.		13 тиждень
Моделі захисту інформації	лекція практ сам. роб.	[1, 5, 9]	4 ауд. год., **8** год. с. р.		14 тиждень
Тематичний контроль	контрольна робота	[1–8]	Підг. до к. р., **10** год. с. р. Індивід. завдання, 2 ауд. год.	30	15 тиждень
Практикум з криптології	сам. роб.	[1–8]	Індивідуальні завдання, **30** год. с. р.	20	$9^{ий}$ – $14^{ий}$ тижні
Підсумковий контроль	екзамен			50	

7. СИСТЕМА ОЦІНЮВАННЯ КУРСУ

Загальна система оцінювання	Підсумкова оцінка з дисципліни у є сумою оцінок за кожен з таких видів робіт: авдиторна робота (активна робота на практичних заняттях), самостійна робота (практикум та опрацювання окремих тем), тематичний контроль (контрольна робота) та екзамен (тестування з теорії). Підсумкова оцінка визначається відповідно до поданої нижче таблиці оцінювання за різними шкалами (100-бальна, ECTS, національна).
Авдиторна робота	Максимальна оцінка за активну і змістовну участь у розв'язуванні задач з криптології на практичних заняттях становить 5 балів.
Самостійна робота	Практикум з лінійного/дискретного програмування містить по 5 завдань у кожному з 25 варіантів. Максимальна оцінка за виконання і захист завдань практикуму становить 20 балів за кожне завдання.
Тематичний контроль	Кожен варіант контрольної роботи містить 7 завдань на застосування методів криптографії та криптоаналізу. Максимальна оцінка становить 30 балів. Екзаменаційний тест з криптології містить від 40 завдань змішаного типу на розуміння основних понять, методів та алгоритмів криптології. Максимальна оцінка за тест становить 50 балів.

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
80 – 89	**B**	добре	
70 – 79	**C**		
60 – 69	**D**	задовільно	
50 – 59	**E**		
26 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-25	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

8. ПОЛІТИКА КУРСУ

Усі види навчальної роботи слід виконувати вчасно, щоб зберігати загальний темп курсу, котрий сприяє ефективному засвоєнню матеріалу без шкоди здоров'ю. Наслідками пропущених занять без поважних причин, зазвичай, стають додаткові завдання для самостійної роботи.

При проходженні курсу вітаються комунікативність, активність, креативність, самостійність. Плагіат та інші види академічної недоброчесності не принесуть користі, тому є недоречними.

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Вербіцький О. В. Вступ до криптології. - Львів: ВНТЛ, 1998. - 248с.
2. Берегуляк І. Я. Класичні методи криптування. - Львівський університет, 1997.
3. Бабенко Т.В., Гулак Г.М., Сушко С.О., Фомичова Л.Я. Криптологія у прикладах, тестах і задачах: навч. посібник / Д.: Національний гірничий університет, 2013. - 318 с.
4. Барычев С. Г., Серов Р. Е. Основы современной криптографии.
5. Ященко В.В. Введение в криптографию.
6. Виноградов И. М. Основы теории чисел. - М.: Наука. - 1981.
7. ван дер Варден Б. Л. Алгебра. - М.: Наука. - 1979.
8. Тилборг ван Х. К. А. Основы криптологии / Тилборг ван Х. К.А. – М. : Мир, 2006. - 471 с.
9. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.

Викладач Мазуренко Н. І.