МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Факультет математики та інформатики

Кафедра алгебри та геометрії

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Криптологія та захист інформації

Освітня програма: Математика комп'ютерних технологій
Спеціальність: 111 Математика
Галузь знань: 11 Математика та статистика

Затверджено на засіданні кафедри
Протокол № 1 від 22 серпня 2023 р.

м. Івано-Франківськ – 2023 рік

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Криптологія та захист інформації**
Освітня програма	Математика комп'ютерних технологій
Спеціалізація (за наявності)	-
Спеціальність	111 Математика
Галузь знань	11 Математика та статистика
Освітній рівень	магістр
Статус дисципліни	нормативна
Курс / семестр	1/2
Розподіл за видами занять та годинами навчання (якщо передбачені інші види, додати)	Лекційні заняття – 30 год Практичні заняття – 30 год Самостійна робота – 120 год Іспит
Мова викладання	українська

Контактна інформація

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

2. Опис курсу

Анотація:

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.

Мета та цілі:

Курс забезпечує набуття знань з математичних основ криптографічного захисту інформації. Його метою є виклад базових принципів побудови математичного обґрунтування 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.

3. Структура курсу

Тема, план	Форма заняття	Література	Години	Кільк. балів	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-ий тижд
Шифри заміни та перестановки, блокові шифри	лекція практ сам. роб.	[1, 3]	**4** ауд. год., **8** год. с. р.		2-ий тижд
Блокове та потокове шифрування	лекція практ сам. роб.	[1, 3]	**4** ауд. год., **8** год. с. р.		3-ій тижд
Елементарна криптографія (математичний підхід) - формалізм - арифметика - афінні шифри	лекція практ сам. роб.	[1, 2, 7]	**4** ауд. год., **8** год. с. р.		4-ий тижд
Афінні шифри	лекція практ сам. роб.	[1, 3, 7, 8]	**4** ауд. год., **8** год. с. р.		5-ий тижд
Основні види атак, принципи криптоаналізу	лекція практ сам. роб.	[1, 3, 7, 8]	**4** ауд. год., **8** год. с. р.		6-ий тижд
Складність арифметичних задач - первісні корені - квадратичні лишки	лекція практ сам. роб.	[1, 6, 7]	**10** ауд. год., **8** год. с. р.		7-9 тижні

- розподіл простих чисел - тестування простоти - 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 тижд
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 тижні
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 тижд
Моделі захисту інформації	лекція практ сам. роб.	[1, 5, 9]	**4** ауд. год., **8** год. с. р.		14 тижд
Тематичний контроль	контрольна робота	[1–8]	Підг. до к. р., **10** год. с. р. Індивід. завдання, **2** ауд. год.	**30**	15 тижд
Практикум з криптології	сам. роб.	[1–8]	Індивід. завдання, **30** год. с. р.	**20**	$1^{ий}$ – $14^{ий}$ тижні
Підсумковий контроль	іспит			**50**	
			Разом:	**100** балів	

4. 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 іспит (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 містить по 5 завдань у кожному з 7 варіантів. Максимальна оцінка за виконання і захист завдань практикуму становить 4 бали за кожне завдання.
Тематичний контроль	Кожен варіант контрольної роботи містить 6 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

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

5. 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.

6. 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.: Націон. гірничий університет, 2013.-318 с.
4. Остапов С. Е., Валь Л. О. *Основи криптографії*. - Чернівці : Книги - XXI, 2008.
5. Коркішко Т., Мельник А., Мельник В. *Алгоритми та процесори симетричного блокового шифрування*. - Львів : БаК, 2003.
6. Олійник О. *Захист інформації в умовах інформаційного успільства*. - Право України.- К., 2005.-10 .- С.100-103

7. Коваленко М. М. *Комп'ютерні віруси і захист інформації* [Текст]: навч. посіб. - К.:Наукова думка,1999 .-268 с.
8. 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.

7. Компетентності

Відповідно до освітньо-професійної програми «Математика комп'ютерних технологій»:

ЗК-1 Здатність до абстрактного мислення, аналізу та синтезу;
ЗК-2 Здатність застосовувати знання у практичних ситуаціях;
ЗК-3 Знання й розуміння предметної області та професійної діяльності;
ЗК-6 Здатність використовувати інформаційні та комунікаційні технології;
СК-1 Знання на рівні новітніх досягнень, необхідні для дослідницької та/або інноваційної діяльності у сфері математики та її практичних застосувань;
СК-4 Спроможність розробляти математичну модель ситуації з реального світу та переносити математичні знання у нематематичні контексти.

8. Результати навчання

Відповідно до освітньо-професійної програми «Математика комп'ютерних технологій»:

ПРН-1 Знати та розуміти фундаментальні і прикладні аспекти наук у сфері математики;
ПРН-2 Відтворювати знання фундаментальних розділів математики в обсязі, необхідному для володіння математичним апаратом комп'ютерних наук і використання математичних методів у інформаційних технологіях;
ПРН-3 Володіти основами математичних дисциплін і теорій, зокрема які вивчають моделі природничих і соціальних процесів;
ПРН-5 Уміти використовувати фундаментальні математичні закономірності у професійній діяльності.

Викладач Мазуренко Н. І.