МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра програмування

Затверджено
На засіданні кафедри програмування
факультету прикладної математики
Львівського національного університету
імені Івана Франка
(протокол № 1 від 31 серпня 2021 р.)

Зав. кафедри к. ф.-м. н., доц. Ярошко С. А.

Силабус навчальної дисципліни
«Математичні основи криптології» (VI семестр),
що викладається в межах ОПП Комп'ютерні науки
першого (бакалаврського) рівня вищої освіти
для здобувачів зі спеціальності 122 Комп'ютерні науки
(Інформатика)

Львів 2021 р.

Назва дисципліни	Математичні основи криптології
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики, кафедра програмування
Галузь знань, шифр та назва спеціальності	Галузь знань: 12 Інформаційні технології Спеціальність: 122 Комп'ютерні науки Спеціалізація: Інформатика
Викладачі дисципліни	Малець Романна Богданівна, к. ф.-м. н., доцент, доцент кафедри програмування
Контактна інформація викладачів	Електронна пошта: romanna.malets@lnu.edu.ua веб-сторінки: https://ami.lnu.edu.ua/employee/malets-r-b
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі он-лайн консультації через Microsoft Teams. Для погодження часу он-лайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/course/
Інформація про дисципліну	Курс "Математичні основи криптології" є вибірковою дисципліною зі спеціальності 122 Комп'ютерні науки (інформатика) для освітньої програми Комп'ютерні науки, яку викладають у шостому семестрі в обсязі 5 кредитів (за Європейською кредитно-трансферною системою ECTS)
Коротка анотація дисципліни	Розглядаються класичні та сучасні підходи до побудови та аналізу криптографічних протоколів та криптосистем. Значна увага звертається на важливість теоретичного аналізу коректності та надійності криптографічних алгоритмів. Вводяться поняття криптографії та криптоаналізу, надійності та ефективності криптосистем. Описані класичні криптографічні методи (шифри перестановки та заміни, поліграмні та поліалфавітні шифри, шифр Віженера, шифр одноразового блокноту, афінні шифри). Наведено формальне визначення криптосистеми, властивості шифрувальних відображень, шифри, що утворюють групу. Розглянуто деякі математичні аспекти (класичний та розширений алгоритми Евкліда, групи та кільця по модулю, арифметика лишків, конгруенції). Подано ідею криптосистем з відкритим ключем (опис, коректність та надійність алгоритму RSA). Розглянуто проблему сертифікації та обміну ключів (алгоритм обміну ключами Діффі-Гелмана) та ідею цифрового підпису (коректність та надійність системи цифрового підпису Ель-Гамала.
Мета та цілі дисципліни	Метою вибіркової дисципліни «Математичні основи криптології» є ознайомити студента з історією криптографії та криптоаналізу, фатальними наслідками нехтування надійним захистом інформації, з основними методами симетричного шифрування, з ідеєю асиметричних систем, вивчити основні математичні методи для побудови та реалізацій надійних систем шифрування, протоколи, цифровий підпис, сформувати поняття про важкооборотні функції та їх роль у криптографії, поняття про еліптичні криві.
Література для вивчення дисципліни	*Основна література* 1. В.В.Ященко. Введение в криптографию. – Ст.-Петербург. – 2001. – 288 с. 2. Д. Кнут. Искусство программирования на ЭВМ. – Т.2: Получисленные алгоритмы. – М., 1977. 3. С. Бернет, С. Пейн. Криптография. Официальное руководство RSA Security. М., 2002. 4. О.В.Вербіцький. Вступ до криптології. Львів. – 1998. – 248 с. 5. А.Ю. Щеглов. Защита компьютерной информации от несанкционованного доступа. С.-Петербург. – 2004. – 384 с. 6. Баричев С.Г., Серов Р.Е. Основы современной криптографии. 2006. – 152 с. 7. Жиль Брассар. Современная криптология. М., 1999. –176 с.

	Додаткова література 8. С.Коутинхо. Введение в теорию чисел. Алгоритм RSA. – М., 2001. – 328 с. 9. М.А.Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. М., 2001. – 368 с. 10.С. Сингх. Книга шифров. М., 2007.
Обсяг курсу	5 кредитів ЄКТС – 150 годин. З них 32 години лекцій, 32 години лабораторних занять та 86 годин самостійної роботи
Очікувані результати навчання	Після завершення цього курсу студент буде: ***Знати:*** • основні проблеми, що виникають в процесі конфіденційного обміну інформації, та методи їх розв”язання; • типи основних класичних криптосистем та їх властивості; • формально-математичний підхід до задання класичних криптосистем та криптосистем із відкритим ключем; • підходи до реалізації різноманітних криптографічних протоколів. ***вміти***: • використовувати основні принципи побудови та аналізу коректності криптосистем до розв’язування конкретних практичних задач; • будувати та реалізовувати алгоритми шифруваня та дешифрування; • реалізовувати широкий клас алгоритмів цілочислової арифметики та арифметики за модулем; • проводити практичний та теоретичний аналіз отриманих результатів.
Компетентності	*Інтегральна:* Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі комп’ютерних наук або у процесі навчання, що передбачають застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов. *Загальні (ЗК):* ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК8. Здатність генерувати нові ідеї (креативність). ЗК12. Здатність оцінювати та забезпечувати якість виконуваних робіт. СК2,3,4,6,7,8,10,11,16 *Спеціальні (фахові, предметні) компетентності (СК):* СК3. Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв’язності та нерозв’язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем. СК7. Здатність застосовувати теоретичні та практичні основи методології та технології моделювання для дослідження характеристик і поведінки складних об'єктів і систем, проводити обчислювальні експерименти з обробкою й аналізом результатів. СК8. Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об’єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління. СК10. Здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника.
Програмні результати навчання	ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук. ПР5. Проектувати, розробляти та аналізувати алгоритми розв’язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та

	обчислюваних функцій. ПР6. Використовувати методи чисельного диференціювання та інтегрування функцій, розв'язання звичайних диференціальних та інтегральних рівнянь, особливостей чисельних методів та можливостей їх адаптації до інженерних задач, мати навички програмної реалізації чисельних методів. ПР9. Розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв'язання задач в галузі комп'ютерних наук. ПР15. Застосовувати знання методології та CASE-засобів проектування складних систем, методів структурного аналізу систем, об'єктно-орієнтованої методології проектування при розробці і дослідженні функціональних моделей організаційно-економічних і виробничо-технічних систем.
Ключові слова	коректність, надійність та ефективність криптографічних алгоритмів; класичні криптосистеми (шифри перестановки та заміни, поліграмні та поліалфавітні шифри, шифр Віженера, шифр одноразового блокноту, афінні шифри); криптосистем з відкритим ключем (важкооборотні функції, опис, коректність та надійність алгоритму RSA); сертифікації та обміну ключів (алгоритм обміну ключами Діффі-Гелмана); аутентифікація та цифровий підпис; використання еліптичних кривих для реалізації криптографічних алгоритмів.
Формат курсу	Очний: проведення лекцій, лабораторних робіт та консультацій в приміщеннях університету, а в умовах карантину – онлайновий на платформі Microsoft Teams
Теми	

Тижд.	Тема, план, короткі тези	Форма заняття	Тривалість, год	Термін виконання
1	Основні поняття криптографії та криптоаналізу. Надійність та ефективність криптосистем. Типи атак на шифр.	Лекція	2	
	Побудова криптосистеми на основі шифрів зсуву.	Лабораторна робота	2	Наступне лабораторне заняття
2	Класичні криптосистеми. Шифр простої заміни. Частотний аналіз. ліалфавітні шифри. Шифр Віженера. Блочні шифри..	Лекція	2	
	Побудова криптосистеми на основі шифрів зсуву.	Лабораторна робота	2	
3	Шифр одноразового блокноту. Стандарт шифрування даних (DES).	Лекція	2	
	Криптосистема на основі шифру Тритеміуса	Лабораторна робота	2	Наступне лабораторне заняття
4	Композиція шифрів. Вплив на надійність.	Лекція	2	
	Криптосистема на основі шифру Тритеміуса	Лабораторна робота	2	
5	Формальне задання криптосистеми. Властивості шифруючих відображень.	Лекція	2	
	Криптосистема на основі шифру гамування..	Лабораторна робота	2	
6	Алгоритм Евкліда. Групи та кільця. Арифметика лишків. Конгруенції.	Лекція	2	
	Криптосистема на основі шифру гамування..	Лабораторна робота	2	Наступне лабораторне заняття
7	Кільце лишків. Функція Ейлера. Шифр зсуву та лінійний шифр. Афінні шифри.	Лекція	2	
	Криптосистема на основі шифру гамування.	Лабораторна робота	2	
8	Важкооборотні функції. Дискретний логарифм.	Лекція	2	
	Шифр Віженера.	Лабораторна робота	2	Наступне лабораторне заняття
9	Поняття криптосистеми з відкритим ключем. RSA: опис, коректність та надійність.	Лекція	2	
	Шифр Віженера.	Лабораторна робота	2	
10	Криптографічні протоколи (обмін ключем, цифровий підпис, аутентифікація, ідентифікація, підкидання монети по телефону).	Лекція	2	
	Шифрування з відкритим ключем.	Лабораторна робота	2	
11	Алгоритм обміну ключами Діффі-Хелмана для двох та більше абонентів. Коректність алгоритму.	Лекція	2	

		Шифрування з відкритим ключем.	Лабораторна робота	2	Наступне лабораторне заняття
	12	Цифровий підпис. Використання криптосистем з відкритим ключем для цифрового підпису.	Лекція	2	
		Шифрування з відкритим ключем.	Лабораторна робота	2	
	13	Система цифрового підпису Ель-Гамала. Коректність алгоритму.	Лекція	2	
		Протокол обміну ключами Діффі-Гелмана.	Контрольна робота	2	
	14	Криптографічні алгоритми на основі еліптичних кривих.	Лекція	2	
		Протокол обміну ключами Діффі-Гелмана.	Лабораторна робота	2	Наступне лабораторне заняття
	15	Поняття криптографічної хеш-функції. Побудова хеш-функції на основі RSA.	Лекція	2	
		Протокол обміну ключами Діффі-Гелмана.	Лабораторна робота	2	
	16	Проблема достовірності інформації. Контроль незмінності даних з допомогою кодів MAC та MDC. Порівняльний аналіз.	Лекція	2	
		Підсумкове заняття.	тест	2	
Підсумковий контроль, форма	залік в кінці семестру				
Пререквізити	Для вивчення курсу студенти потребують знань з таких дисциплін: – Чисельні методи; – Програмування; – Функціональний аналіз.				
Навчальні методи та техніки, які використовують під час викладання курсу	Лекції з мультимедійними презентаціями; лабораторні заняття у вигляді проектування криптосистем та їх програмних реалізацій, програмна реалізація певних типів атак на криптосистеми; самостійне опрацювання навчальних матеріалів: підручників, конспектів лекцій, додаткових навчальних посібників, розміщених у хмарному сховищі (Moodle, Microsoft Teams). Обговорення теоретичного та практичного матеріалу в онлайн сервісах, формулювання творчих завдань для студентів, виконання яких готує до вивчення нового теоретичного матеріалу.				
Необхідне обладнання	Для проведення лекцій: комп'ютер, проектор, доступ до мережі інтернет. Для проведення лабораторних та виконання завдань: комп'ютер, ОС Windows, доступ до інтернету, програмне забезпечення Microsoft Visual Studio. Вся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.				
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	**Оцінювання** проводиться за 100-бальною шкалою. 60 балів нараховують за виконання лабораторних завдань, ще 40 балів за засвоєння теоретичного матеріалу, виставлені після опитувань упродовж семестру (у формі тестувань, семінарів тощо). Лабораторні завдання всі індивідуальні. Упродовж семестру студент виконує не менше 6 лабораторних робіт, кожну з яких оцінюють у 10 балів. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу. Активність під час проведення лекцій і лабораторних заохочується балами. Студенти зобов'язані дотримуватися усіх термінів визначених для виконання лабораторних робіт та тестового завдання, передбачених курсом. Виконані роботи завантажують у відповідне хмарне сховище. Альтернативою відвідування лабораторних занять в університеті може бути дистанційна онлайнова робота за розкладом проведення занять. Активність на лекціях і лабораторних ураховують при оцінюванні відповідного лабораторного завдання. **Академічна доброчесність**: очікується, що роботи студентів будуть їхнім оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів, представлення чужих комп'ютерних програм як своїх становлять, але не обмежують, приклади можливої академічної недоброчесності.				

	Виявлення ознак академічної недоброчесності студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано після завершення курсу.