

**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 29 серпня 2025 р.)



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

**Силабус навчальної дисципліни**  
**«Математичні основи криптології»,**  
**що викладається в межах ОПП Середня освіта (Інформатика)**  
**першого (бакалаврського) рівня вищої освіти для здобувачів з**  
**спеціальності А4.09 – Середня освіта (Інформатика)**

Львів 2025 р.

<b>Назва дисципліни</b>	Математичні основи криптології
<b>Адреса викладання дисципліни</b>	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
<b>Факультет та кафедра, за якою закріплена дисципліна</b>	Факультет прикладної математики та інформатики, кафедра програмування
<b>Галузь знань, шифр та назва спеціальності</b>	A – Освіта/Педагогіка A4.09 – Середня освіта (Інформатика)
<b>Викладачі дисципліни</b>	Малець Романна Богданівна, к. ф.-м. н., доцент, доцент кафедри програмування
<b>Контактна інформація викладачів</b>	Електронна пошта: <a href="mailto:romanna.malets@lnu.edu.ua">romanna.malets@lnu.edu.ua</a> веб-сторінки: <a href="https://ami.lnu.edu.ua/employee/malets-r-b">https://ami.lnu.edu.ua/employee/malets-r-b</a>
<b>Консультації з питань навчання по дисципліні відбуваються</b>	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.
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/course/mathematical-basics-of-cryptology-informatics">https://ami.lnu.edu.ua/course/mathematical-basics-of-cryptology-informatics</a>
<b>Інформація про дисципліну</b>	Курс “Математичні основи криптології” є вибірковою дисципліною зі спеціальності A4.09 – Середня освіта (Інформатика) для освітньої програми Середня освіта (Інформатика), яку викладають у шостому семестрі в обсязі 4,5 кредитів (за Європейською кредитно-трансферною системою ECTS)
<b>Коротка анотація дисципліни</b>	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).
<b>Мета та цілі дисципліни</b>	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.
<b>Література для вивчення дисципліни</b>	<i>Основна література</i> 1. Курко Н.М. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. — 248 с. 2. Лісовський П.М. Контррозвідка: квантова безпека та громадськість : навч. посібник. /— К. : Видавничий дім «Кондор», 2019. — 188 с. 3. Henk van Tilborg Encyclopedia of Cryptography and Security. Henk van Tilborg and others., Springer-Verlag, 2022 4. Гребенніков В.В. Історія криптології та секретного зв'язку. – КНТ, 2023, 800с. 5. О.В.Вербіцький. Вступ до криптології. Львів. – 1998. – 248 с.

	<p><i>Додаткова література</i></p> <ol style="list-style-type: none"> <li>1. С.Коутинхо. Введение в теорию чисел. Алгоритм RSA. – М., 2001. – 328 с.</li> <li>2. М.А.Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. М., 2001. – 368 с.</li> <li>3. С. Сингх. Книга шифров. М., 2007.</li> </ol>
<b>Обсяг курсу</b>	4,5 кредитів ЄКТС – 135 годин. З них 32 години лекцій, 32 години лабораторних занять та 71 годин самостійної роботи
<b>Очікувані результати навчання</b>	<p>Після завершення цього курсу студент буде:</p> <p><b>Знати:</b></p> <ul style="list-style-type: none"> <li>• основні проблеми, що виникають в процесі конфіденційного обміну інформації, та методи їх розв’язання;</li> <li>• типи основних класичних криптосистем та їх властивості;</li> <li>• формально-математичний підхід до задання класичних криптосистем та криптосистем із відкритим ключем;</li> <li>• підходи до реалізації різноманітних криптографічних протоколів.</li> </ul> <p><b>вміти:</b></p> <ul style="list-style-type: none"> <li>• використовувати основні принципи побудови та аналізу коректності криптосистем до розв’язування конкретних практичних задач;</li> <li>• будувати та реалізовувати алгоритми шифрування та дешифрування;</li> <li>• реалізовувати широкий клас алгоритмів цілочислової арифметики та арифметики за модулем;</li> <li>• проводити практичний та теоретичний аналіз отриманих результатів.</li> </ul>
<b>Ключові слова</b>	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.
<b>Формат курсу</b>	Очний: проведення лекцій, лабораторних робіт та консультацій в приміщеннях університету, а в умовах карантину – онлайн-овий на платформі Microsoft Teams

<b>Теми</b>				
Тижд.	Тема, план, короткі тези	Форма заняття	Тривалість (с.р.), год	Термін виконання
1	Основні поняття криптографії та криптоаналізу. Надійність та ефективність криптосистем. Типи атак на шифр.	Лекція	2(2)	
	Побудова криптосистеми на основі шифрів зсуву.	Лабораторна робота	2(2)	Наступне лабораторне заняття
2	Класичні криптосистеми. Шифр простої заміни. Частотний аналіз. ліалфавітні шифри. Шифр Віженера. Блочні шифри..	Лекція	2(2)	
	Побудова криптосистеми на основі шифрів зсуву.	Лабораторна робота	2(2)	
3	Шифр одноразового блокноту. Стандарт шифрування даних (DES).	Лекція	2(2)	
	Криптосистема на основі шифру Третемиуса	Лабораторна робота	2(2)	Наступне лабораторне заняття
4	Композиція шифрів. Вплив на надійність.	Лекція	2(2)	
	Криптосистема на основі шифру Третемиуса	Лабораторна робота	2(2)	
5	Формальне задання криптосистеми. Властивості шифруючих відображень.	Лекція	2(2)	
	Криптосистема на основі шифру гамування..	Лабораторна робота	2(2)	
6	Алгоритм Евкліда. Групи та кільця. Арифметика лишків. Конгруенції.	Лекція	2(2)	
	Криптосистема на основі шифру гамування..	Лабораторна робота	2(2)	Наступне лабораторне заняття
7	Кільце лишків. Функція Ейлера. Шифр зсуву та лінійний шифр. Афінні шифри.	Лекція	2(2)	
	Криптосистема на основі шифру гамування.	Лабораторна робота	2(2)	
8	Важкооборотні функції. Дискретний логарифм.	Лекція	2(2)	
	Шифр Віженера.	Лабораторна робота	2(3)	Наступне лабораторне заняття
9	Поняття криптосистеми з відкритим ключем. RSA: опис, коректність та надійність.	Лекція	2(2)	
	Шифр Віженера.	Лабораторна робота	2(3)	
10	Криптографічні протоколи (обмін ключем, цифровий підпис, аутентифікація, ідентифікація, підкидання монети по телефону).	Лекція	2(2)	
	Шифрування з відкритим ключем.	Лабораторна робота	2(3)	
11	Алгоритм обміну ключами Діффі-Хелмана для двох та більше абонентів. Коректність алгоритму.	Лекція	2(2)	
	Шифрування з відкритим ключем.	Лабораторна робота	2(3)	Наступне лабораторне заняття
12	Цифровий підпис. Використання криптосистем з відкритим ключем для цифрового підпису.	Лекція	2(2)	
	Шифрування з відкритим ключем.	Лабораторна робота	2(3)	
13	Система цифрового підпису Ель-Гамала. Коректність алгоритму.	Лекція	2(2)	
	Протокол обміну ключами Діффі-Гелмана.	Контрольна робота	2(3)	
14	Криптографічні алгоритми на основі еліптичних кривих.	Лекція	2(2)	
	Протокол обміну ключами Діффі-Гелмана.	Лабораторна робота	2(3)	Наступне лабораторне заняття
15	Поняття криптографічної хеш-функції. Побудова хеш-функції на основі RSA.	Лекція	2(2)	
	Протокол обміну ключами Діффі-Гелмана.	Лабораторна робота	2(3)	
16	Проблема достовірності інформації. Контроль незмінності даних з допомогою кодів MAC та MDC. Порівняльний аналіз.	Лекція	2(2)	
	Підсумкове заняття.	тест	2	

<b>Підсумковий контроль, форма</b>	залік в кінці семестру
<b>Пререквізити</b>	Для вивчення курсу студенти потребують знань з таких дисциплін: <ul style="list-style-type: none"> <li>– Чисельні методи;</li> <li>– Програмування;</li> <li>– Функціональний аналіз.</li> </ul>
<b>Навчальні методи та техніки, які використовують під час викладання курсу</b>	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.
<b>Необхідне обладнання</b>	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.
<b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b>	<p><b>Оцінювання</b> 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, кожен з яких оцінюють у 10 балів.</p> <p>Для кожного завдання визначено термін виконання: зазвичай до закінчення навчального тижня. Вчасно виконані завдання оцінюють так (у відсотках від максимальної оцінки):</p> <ul style="list-style-type: none"> <li>• 100% – умови завдання виконано повністю, алгоритми складено правильно, програма містить належні коментарі, роботу програми перевірено на достатньому наборі тестових даних, автор відповідає на всі запитання щодо використаних підходів, чітко інтерпретує отримані результати, немає ознак недоброчесності;</li> <li>• 80% – наведено логічно правильну послідовність розв'язування, алгоритми складено правильно, бракує окремих коментарів чи тестів, автор не досить повно пояснює використані підходи, немає ознак недоброчесності;</li> <li>• 60% – у правильній послідовності розв'язування допущено окремі помилки, які автор уміє виправити після зауваження викладача, бракує коментарів чи тестів, на запитання щодо використаних підходів автор відповідає з помилками, немає ознак недоброчесності;</li> <li>• 40% – у правильній послідовності розв'язування пропущено окремі етапи, завдання виконано частково, автор не розуміє недоліків поданої роботи, не вміє їх виправити, немає ознак недоброчесності;</li> <li>• 20% – завдання виконано частково, немає тестів, програма працює правильно для окремих наборів вхідних даних, автор не може самостійно інтерпретувати отримані результати, виправити помилки, немає ознак недоброчесності;</li> <li>• 0% – завдання не виконано, написана програма не відповідає умові, або ж виявлено ознаки недоброчесності: запозичення, фрагменти коду, дію яких автор пояснити не може, автор не володіє відповідним теоретичним матеріалом тощо;</li> <li>• можуть бути нараховані додаткові бали за повністю виконане завдання, яке містить кілька способів розв'язування, використовує особливо ефективний спосіб, демонструє креативність автора тощо.</li> </ul> <p>Запізнення зменшує максимальну оцінку за завдання: кожного наступного після терміну виконання тижня оцінка зменшується удвічі.</p> <p><b>Відвідання занять</b> 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</p>

	<p>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 онлайн робота за розкладом проведення занять. Активність на лекціях і лабораторних ураховують при оцінюванні відповідного лабораторного завдання.</p> <p><b>Академічна доброчесність:</b> 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.</p>
<p><b>Опитування</b></p>	<p>Анкету-оцінку з метою оцінювання якості курсу буде надано після завершення курсу.</p>