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 2023 р.)

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

Силабус навчальної дисципліни

«Математичні основи криптології»,

викладається в межах ОПП “Інформатика”

першого (бакалаврського) рівня вищої освіти

для здобувачів зі спеціальності 122 Комп’ютерні науки

Львів – 2023 р.

Назва дисципліни	Математичні основи криптології
Адреса викладання дисципліни	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
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/mathematical-basics-of-cryptology-informatics
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. Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В. Кібербезпека: основи кодування та криптографії: навч. Посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов. – Харків: ХПІ, 2023. – 658 с. 2. Стасюк М. Елементи математичних основ криптографії : навчальний посібник / М. Стасюк. – Львів : ЛДУ БЖД, 2021. – 216 с. 3. Щур Н.О. Основи криптології: навч. Посібник / Н.О. Щур, О.А. Покотило. – Житомир: Державний університет «Житомирська політехніка» . – 2021. – 120с. 4. Barakat M. An Introduction to Cryptography [Electronic resource]. / Mohamed Barakat, Christian Eder, Timo Hanke . – September 20, 2018. – 145 pp. –. Available at: https://agag-ederc.math.rptu.de/~ederc/download/Cryptography.pdf. 5. Bellare M. Introduction to modern cryptography [Electronic resource]. – / Mihir Bellare and Phil Rogaway. – May 11, 2005. – 283 pp. – Available at: https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf. 6. Bourke C. CSCE 477/877: Cryptography and Computer Security [Electronic resource] / Chris Bourke. – Department of Computer Science & Engineering, University of Nebraska–Lincoln. – 2015. – 138 pp. – Available at: https://cse.unl.edu/~cbourke/cryptoNotes.pdf . 7. Boneh D. A Graduate Course in Applied Cryptography / Dan Boneh, Victor Shoup. – 2020. – 943 p. 8. Kerr M. Lecture notes Number Theory and Cryptography [Electronic resource] /Matt Kerr. – 2020 – 264 pp. – Available at: 9. Kölbl S. Design and Analysis of Cryptographic Algorithms [Electronic resource] : [A Report on Ph.D. thesis] / Stefan Kölbl.– DTU Compute PHD-2016. – Number 434. – Kgs. Lyngby, Technical University of Denmark. – 2017. – 272 pp. – Available at: Design and analysis of cryptographic algorithms — Welcome to DTU Research Database. 10. Lecture Notes on Introduction to Cryptography [Electronic resource]. – [Course 15356/15856, Fall 2020] / E. Masserova. – Vipul Goyal, CMU. – 119 pp. – Available at: https://www.cs.cmu.edu/~goyal/15356/lecture_notes.pdf. 11. Shivakumar V. A Report on Application of Cryptography and Groups [Electronic resource] – / V. Shivakumar. – May 2020. – 27 pp. – Available at: (PDF) Application of Cryptography and Groups (researchgate.net) . https://www.math.wustl.edu/~matkerr/NTCbook.pdf *Додаткова література* 12. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів. – 1998. – 248 с. 13. Горбенко І. Д. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів / І. Д. Горбенко, Ю. І. Горбенко . – Харків: Видавництво «Форт» . – 2013. – 880 с. 14. Горбенко Ю. І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. – Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За аг.ред. д.т.н., професора І.Д. Горбенка. – Харків: Видавництво «Форт» . – 2015. – 960 с. 15. Лагун А.Е. Криптографічні системи тп пртоколи: навч. Посібник / А.Е. Лагун.– Львів: Видавництво Львівської політехніки, 2013. – 96 с.
Обсяг курсу	5 кредитів ЄКТС – 150 годин. З них 32 години лекцій, 32 години лабораторних занять та 86 годин самостійної роботи

<table>
<tr><td>Очікувані результати навчання</td><td>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.</td></tr>
<tr><td>Компетентності</td><td>Загальні (ЗК):
ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
Спеціальні (фахові, предметні) компетентності (СК):
СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.</td></tr>
<tr><td>Програмні результати навчання</td><td>ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.</td></tr>
<tr><td>Ключові слова</td><td>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.</td></tr>
<tr><td>Формат курсу</td><td>Очний: проведення лекцій, лабораторних робіт та консультацій в приміщеннях університету, а в умовах карантину – онлайновий на платформі Microsoft Teams</td></tr>
<tr><td>Теми</td><td>
<table>
<tr><th>Тижд.</th><th>Тема, план, короткі тези</th><th>Форма заняття</th><th>Тривалість год .</th><th>Термін виконання</th></tr>
<tr><td rowspan="2">1</td><td>Основні поняття криптографії та криптоаналізу. Надійність та ефективність криптосистем. Типи атак на шифр.</td><td>Лекція</td><td>2</td><td></td></tr>
<tr><td>Побудова криптосистеми на основі шифрів зсуву.</td><td>Лабораторна робота</td><td>2</td><td>Наступне лабораторне заняття</td></tr>
<tr><td rowspan="2">2</td><td>Класичні криптосистеми. Шифр простої заміни. Частотний аналіз. ліалфавітні шифри. Шифр Віженера. Блочні шифри..</td><td>Лекція</td><td>2</td><td></td></tr>
<tr><td>Побудова криптосистеми на основі шифрів зсуву.</td><td>Лабораторна робота</td><td>2</td><td></td></tr>
<tr><td rowspan="2">3</td><td>Шифр одноразового блокноту. Стандарт шифрування даних (DES).</td><td>Лекція</td><td>2</td><td></td></tr>
<tr><td>Криптосистема на основі шифру Тритеміуса</td><td>Лабораторна робота</td><td>2</td><td>Наступне лабораторне заняття</td></tr>
<tr><td rowspan="2">4</td><td>Композиція шифрів. Вплив на надійність.</td><td>Лекція</td><td>2</td><td></td></tr>
<tr><td>Криптосистема на основі шифру Тритеміуса</td><td>Лабораторна робота</td><td>2</td><td></td></tr>
<tr><td rowspan="2">5</td><td>Формальне задання криптосистеми. Властивості шифруючих відображень.</td><td>Лекція</td><td>2</td><td></td></tr>
<tr><td>Криптосистема на основі шифру гамування..</td><td>Лабораторна робота</td><td>2</td><td></td></tr>
</table>
</td></tr>
</table>

	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	
		Задача рюкзака.	Лекція	2	
	8	Важкооборотні функції. Дискретний логарифм.	Лекція	2	
		Задача рюкзака.	Лабораторна робота	2	Наступне лабораторне заняття
	9	Поняття криптосистеми з відкритим ключем. RSA: опис, коректність та надійність.	Лекція	2	
		Задача рюкзака.	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				
Пререквізити	Чисельні методи; Програмування; Функціональний аналіз.				
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Створення команди курсу в MS Teams. 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.

Захист лабоработних завдань та самостійна робота							**Сума балів**
ЛЗ1	ЛЗ2	ЛЗ3	ЛЗ4	ЛЗ5	ЛЗ6	тест	
10	**10**	**10**	**10**	**10**	**10**	**40**	**100**

ЛЗ1, ЛЗ2, …, ЛЗ6 – лабораторні заняття

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.

Запитання тесту

1. Яка операція властива кільцям?
2. Для яких бінарних операцій кілець справджуються дистрибутивні закони?
3. Які властивості не притаманні кільцям?
4. Яка основна відмінність між афінним шифром та шифром Цезаря?
5. Що забезпечує алгоритм Діффі-Гелмана?
6. Що виробляється за протоколом Діффі-Гелмана розподілу ключів?
7. Для чого використовуються проміжні результати обчислення $\mathbf{g^x \bmod p}$ за протоколом Діффі-Гелмана?
8. Чому в протоколі Діффі-Гелмана доцільно передбачати аунтентифікацію абонентів?
9. Яка функція називається важкооборотною (односторонньою)?
10. Коли натуральне число **l** називають дискретним логарифмом елемента **a** з основою **b?**
11. Які методи розв'язання задачі дискретного логарифмування?
12. Що гарантує так званий "ефект лавини"?
13. Які основні недоліки афінного шифру?
14. Стійкі криптосистеми, приклади.
15. Що є результатом ділення кілець лишків?
16. У чому полягає ідея лінійного шифру?
17. Що називається порядком групи точок еліптичної кривої над полем **GF(p)?**
18. Яка математична проблема забезпечує стійкість криптосистем, побудованих на еліптичних кривих?
19. Які еліптичні криві є сингулярними?
20. Що забезпечує стійкість ECC?
21. Рівнянням Вейєрштрасса для еліптичної кривої $\mathbf{E_p(a,b)}$ над полем **GF(p).**
22. В яких випадках автентифікація є однобічною?

	23. Що таке атака відображенням? 24. У чому полягає функція конфіденційності криптографічного протоколу? 25. Як називається ідентифікація людини за унікальними, властивими тільки їй, біологічними ознаками? 26. Як використовується RSA у алгоритмах MASH? 27. Який суттєвий недолік притаманний алгоритмам MASH? 28. Які вимоги накладаються на криптографічну хеш-функцію? 29. На чому базуєтьсяє надійність криптосистеми RSA? 30. Визначення криптографічної хеш-функції. 31. Що таке RSA? 32. За допомогою якого методу можна знайти цілі числа p і q близькі одне до одного? 33. За допомогою якого рівняння обчислюється зашифрований текст C, якщо **m** текст для шифрування алгоритмом RSA і **e** відкритий ключ? 34. Обчислити значення відкритого ключа для двох простих різних числа **p**=3557 і **q**=2579 та відкритої експоненти **e**=3 . 35. Що використовується для підтвердження достовірності отриманої інформації в вебі? 36. Які основні вимоги накладаються на алгоритм MAC? 37. Яка різниця між MAC і HMAC при передачі інформації? 38. Для чого використовується MAC? 39. На чому базується криптографічна стійкість алгоритму Ель-Гамаля базується на складності? 40. Якщо **(p,g,h)** – відкритий ключ, **a** – секретний ключ криптосистеми Ель-Гамала, **(C_1,C_2)** – отриманий шифротекст, у результаті зашифрування відкритого повідомлення M, наведіть рівняння розшифрування. 41. Нехай **p=17, g=3** відкриті параметри криптосистеми Ель-Гамала, спільні для декількох користувачів, **a=7** – секретний ключ одного з них. Завершіть формування його відкритих ключів. 42. Яким не буває відображення: **f: X -> Y** згідно з теоремою про обернене відображення. 43. Перечисліть всі елементи, якими формально можна задати криптосистему чи шифр. 44. Що називають порядком скінченної групи? 45. Скільки обернених відображень існує для будь-якого елемента?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано після завершення курсу.