МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Механіко-математичний факультет
Кафедра алгебри, топології та основ математики

Затверджено
На засіданні кафедри алгебри, топології та основ математики
механіко-математичного факультету
Львівського національного університету
імені Івана Франка
(протокол № 1 від 29 серпня 2022 р.)

Завідувач кафедри
доктор фізико-математичних наук, професор
Банах Т.О.

Силабус з навчальної дисципліни

«Криптологія»,

що викладається в межах освітньо-професійної програми
«Комп'ютерна алгебра, криптологія та теорія ігор»
підготовки першого освітнього рівня вищої освіти
для здобувачів за спеціальністю **111 «Математика»**

Львів 2022 р.

Назва дисципліни	Криптологія
Адреса викладання дисципліни	Львівський національний факультет імені Івана Франка, Механіко-математичний факультет, вул. Університетська 1, м. Львів
Факультет та кафедра, за якою закріплена дисципліна	Механіко-математичний факультет, кафедра алгебри, топології та основ математики
Галузь знань, шифр та назва спеціальності	11 Математика та статистика, 111 Математика
Викладачі дисципліни	Банах Тарас Онуфрійович, д.ф.-м.н., професор
Контактна інформація викладачів	taras.banakh@lnu.edu.ua
Консультації з питань навчання по дисципліні	Консультації в день проведення лекцій (за попередньою домовленістю).
Сторінка дисципліни	https://new.mmf.lnu.edu.ua/course/liniyna-alhebra-opp-komp-iuterna-alhebra-kryptolohiia-ta-ekonometryka
Інформація про дисципліну	Дисципліна "Криптологія" є нормативною навчальною дисципліною циклу професійної та практичної підготовки зі спеціальності 111 «Математика» для освітньо-професійньої бакалаврської програми «Комп'ютерна алгебра, криптологія та теорія ігор», яка викладається в сьомому семестрі в обсязі 4 кредитів (за Європейською кредитно-трансферною системою ECTS).
Коротка анотація дисципліни	Курс ознайомлює з математичними основами криптології, класичними криптосистемами, а також криптосистемами з відкритим ключем
Мета та цілі дисципліни	Метою і завданням навчальної дисципліни "Криптологія " є ознайомлення з математичними методами криптології та їх застосуваннями до класичних криптосистем та криптосистем з відкритим ключем.
Література для вивчення дисципліни	**Основна література:** 1. О.В. Вербіцький, *Вступ до криптології*, Львів, ВНТЛ, 1998. 2. N. Koblitz, *A course in number theory and cryptography*, Springer, 1994. 3. N. Koblitz, A.J. Menezes, Yi-Hong Wu, R.J. Zuccherato, *Algebraic aspects of cryptography*, Springer, 1998. 4. A.R. Meijer, *Algebra for Cryptologists*, Springer, 2016. 5. J. Hoffstein, J. Pipher, J.H. Silverman, *An Introduction to Mathematical*, Springer, 2014. **Додаткова література:** 1. C. Paar, *Understanding Cryptography*, Springer, 2009. 2. S. Singh, *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, 2000. 3. N. Ferguson, B. Schneier, T. Kohno, *Cryptography Engineering* *Design Principles and Practical Applications*, Wiley, 2010. 4. W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson, 2016. 5. A. Sweigart, *Cracking Codes with Python. An Introduction to Building and Breaking Ciphers*, No Starch Press, 2018. 6. C. Nez, J. Schiess Avila, *Code Talker: The First and Only Memoir By One of the Original Navajo Code Talkers of WWII*, Dutton Caliber, 2012.

	7. N. Ferguson, B. Schneider, *Practical Cryptography*, Wiley, 2013.
Обсяг курсу	Всього 120 годин: 80 год аудиторних занять, з них 48 год лекційних занять та 32 год практичних занять, 100 год самостійної роботи
Очікувані результати навчання	Після завершення курсу «Криптологія» студент буде володіти сучасними математичними методами криптології та вміти застосовувати її в подальшій професійній діяльності. У результаті вивчення навчальної дисципліни відповідно до освітньої програми формуються **програмні компетентності.** **Інтегральна компетентність** Здатність розв'язувати складні математичні задачі та практичні проблеми у професійній діяльності або у процесі навчання, що передбачає застосування теорій та методів математики, статистики й комп'ютерних технологій і характеризується комплексністю та/або невизначеністю умов. **Загальні компетентності** **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**. Навички використання інформаційних і комунікаційних технологій; **ЗК-7.** Здатність учитися і оволодівати сучасними знаннями. **ЗК-8.** Здатність до пошуку, обробки та аналізу інформації з різних джерел; **ЗК-9.** Здатність приймати обґрунтовані рішення. **ЗК-13.** Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків. **Фахові компетентності спеціальності** **СК-1.** Здатність формулювати проблеми математично та в символьній формі з метою спрощення їхнього аналізу й розв'язання. **СК-2.** Здатність подавати математичні міркування та висновки з них у формі, придатній для цільової аудиторії, а також аналізувати та обговорювати математичні міркування інших осіб, залучених до розв'язання тієї самої задачі. **СК-3.** Здатність здійснювати міркування та виокремлювати ланцюжки міркувань у математичних доведеннях на базі аксіоматичного підходу, а також розташовувати їх у логічну послідовність, у тому числі відрізняти основні ідеї від деталей і технічних викладок. **СК-5.** Здатність до кількісного мислення; **СК-8.** Здатність до аналізу математичних структур, у тому числі до оцінювання обґрунтованості й ефективності використовуваних математичних підходів; **СК-9.** Здатність застосовувати спеціалізовані мови програмування та пакети прикладних програм. **Програмні результати навчання** **РН-2**. Розуміти правові, етичні та психологічні аспекти професійної діяльності; **РН-3**. Знати принципи modus ponens (правило виведення логічних висловлювань) та modus tollens (доведення від супротивного) і використовувати умови, формулювання, висновки, доведення та наслідки математичних тверджень; **РН-4.** Розуміти фундаментальну математику на рівні, необхідному для досягнення інших вимог освітньої програми; **РН-5.** Мати навички використання спеціалізованих програмних засобів комп'ютерної та прикладної математики і використовувати інтернет-ресурси; **РН-10.** Розв'язувати задачі придатними математичними методами, перевіряти умови виконання математичних тверджень, коректно переносити умови та твердження на нові класи об'єктів, знаходити й аналізувати відповідності між поставленою задачею й відомими моделями. **РН-15.** Знати теоретичні основи і застосовувати алгебраїчні методи для вивчення математичних структур. **РН-19**. Знати теоретичні основи і застосовувати методи математичної фізики для

	моделювання реальних фізичних, біологічних, екологічних, соціально- економічних та інших процесів і явищ. **РН-22**. Знати основи програмування та вміти створювати програмне забезпечення, необхідне в подальшій роботі. **РН-23.** Знати основи кодування, захисту інформації та захисту даних і застосовувати алгоритми комп'ютерної алгебри та методи криптології.

Ключові слова	крипрографія, криптоаналіз, криптосистема, криптосистеми з відкритим ключем, кільце лишків
Формат курсу	Очний Проведення лекцій та практичних занять
Теми	Приведено у Таблиці 1
Підсумковий контроль форма	Іспит Письмова
Пререквізити	Для успішного вивчення дисципліни студенти повинні прослухати та засвоїти нормативні курси «Лінійна Алгебра», «Дискретна математика», «Інформатика і програмування (Python)», «Теорія чисел», «Теорія складності обчислень» та, по можливості, вибірковий курс «Загальна алгебра».
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентація, лекції, практичні, індивідуальні завдання, дискусія
Необхідне обладнання	Мультимедійне обладнання
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	З метою перевірки якості підготовки, знань, умінь здобувача з навчальної дисципліни використовуються такі засоби оцінювання: • для поточного контролю – усне опитування, перевірка домашніх завдань; • для проміжного контролю – дві індивідуальні завдання (по симетричних криптографічних системах та криптосистемах з відкритим ключем); • підсумковий контроль – семестровий екзамен, який включає теоретичні питання і розв'язування задач. Об'єктами контролю знань студентів з навчальної дисципліни «Криптологія» є: • систематичність роботи та активність на практичних заняттях; • виконання домашніх завдань; • виконання індивідуальних завдань; При оцінці систематичності та активності роботи студента на практичних заняттях враховується: • рівень знань, продемонстрований у відповідях на практичних заняттях; • активність при обговоренні задач підвищеної складності; • результати виконання індивідуальних завдань по створенню криптосистем різних типів. При оцінці виконання індивідуального завдання враховується загальний рівень практичних навичок, набутих студентами під час опанування відповідного змістовного модуля. Контроль знань і умінь студентів з навчальної дисципліни «Криптологія» здійснюється згідно з модульною системою організації навчального процесу. Підсумкове оцінювання знань, умінь і навичок здобувачів із навчальної дисципліни здійснюється на основі результатів поточного, проміжного контролю

та підсумкового контролю (екзамену) за 100-бальною шкалою.
Поточний та проміжний контроль за вивченням студентами дисципліни здійснюється викладачами, що забезпечують даний курс відповідно до виду занять. В результаті роботи на практичних заняттях та виконання індивідуальних завдань студенти можуть отримати 0-50 балів.

Контроль успішності здійснюється у формі поточного контролю на лекційних та практичних заняттях, перевірці виконання індивідуальних завдань, та письмового іспиту. Бали нараховуються за таким співвідношенням:

- робота та активність час лекційних та практичних занять: 10% семестрової оцінки; максимальна кількість балів – 10;
- індивідуальні завдання: 40% семестрової оцінки; два індивідуальні завдання по 20 балів; максимальна кількість балів – 40;
- іспит: 50% семестрової оцінки; максимальна кількість балів – 50.

Засоби контролю	**Кількість балів**
Активність під час лабораторних занять	10
Індивідуальне завдання 1	20
Індивідуальне завдання 2	20

У процесі оцінювання систематичності та активності роботи студента на лабораторних заняттях враховується: рівень знань продемонстрований у відповідях на заняттях; активність при обговоренні питань; результати виконання індивідуальних завдань тощо.
Підсумкова максимальна кількість балів – 100.
Форма підсумкового контролю успішності навчання – екзамен.
Екзамен проходить у письмовій формі. У кожному екзаменаційному білеті міститься по п’ять питань: два теоретичних питання з різних змістовних модулів курсу, а також три задачі з криптології. Оцінка за семестр є сумою балів поточного контролю та балів, отриманих під час іспиту.

Порядок вивчення та оцінювання дисципліни доводиться до відома студентів протягом семестру. Успішність навчання студентів оцінюється за шкалою.

Шкала оцінювання: Університету , національна та ECTS

Оцінка в балах	***Оцінка ECTS***	***За національною шкалою***	
		Екзаменаційна оцінка, оцінка з диференційованого заліку	***Залік***
90 – 100	A	Відмінно	Зараховано
81-89	B	Добре	
71-80	C		
61-70	D	Задовільно	
51-60	E		
0-50	F/FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання

Бали в діапазоні 90–100 означають, що студент виявив всебічні, систематизовані, глибокі знання програмного матеріалу, уміння вільно виконувати завдання передбачені програмою. Знання основної і ознайомлення з додатковою літературою, передбачених програмою на рівні творчого використання.

	Бали в діапазоні 71–89 означають, що студент виявив загалом добрі знання навчального матеріалу, але допустив ряд помітних помилок, показав систематичний характер знань з дисципліни, здатний їх використовувати та поповнювати в процесі подальшого навчання. Бали в діапазоні 61–70 означають, що студент виявив знання основного навчального матеріалу, справився з виконанням завдань, передбачених програмою, ознайомився з основою літературою, рекомендованою програмою, допустив значну кількість помилок у відповідях на запитання, тестуванні, при виконанні завдань. Бали в діапазоні 51–60 свідчать про значні недоліки в знаннях основного навчального матеріалу, про принципові помилки при виконанні передбачених програмою завдань. Бали в діапазоні 1–50 означають, що студент не мав знань зі значної частини навчального матеріалу, допускав принципові помилки при виконанні більшості передбачених програмою завдань, неспроможний самостійно засвоїти програмний матеріал і потребує повторного вивчення дисципліни. **Відвідування занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття курсу, а також виконують домашні завдання. Студенти мають інформувати викладача про неможливість відвідати заняття. **Політика виставлення балів**: Враховуються бали, набрані на практичних заняттях, при перевірці домашніх завдань, контрольних робіт, під час дискусій на лекціях, виконанні індивідуальних завдань, внаслідок письмової здачі іспиту. Жодні форми порушення академічної доброчесності не толеруються.
Питання до іспиту	**Розділ 1: Класичні криптосистеми** 1. Шифри простої заміни 2. Шифр зсуву 3. Частотний аналіз 4. Гомофонний шифр Гауса 5. Шифр 4-х квадратів 6. Шифри перестановки 7. Шифр Кардано 8. Шифр Віженера 9. Шифр Віженера з автоключем **Розділ 2: Арифметичні інструменти** 10. Алгоритм Евкліда знаходження найбільшого спільного дільника 11. Швидкість роботи алгоритму Евкліда 12. Розширений алгоритм Евкліда 13. Китайська теорема про остачі, застосування розширеного алгоритму Евкліда до алгоритмічної реалізації китайської теореми про остачі 14. Прості числа, основна теорема арифметики: розклад на прості множники 15. Конгруенції, їх властивості 16. Кільце остач 17. Обчислення обернених елементів 18. Взаємно прості числа, функція Ейлера 19. Обчислення функції Ейлера, асимптотика функції Ейлера 20. Мала теорема Ферма та теорема Ейлера 21. Кільце матриць. Кількість невироджених nxn матриць над кільцем лишків **Розділ 3: Афінні шифри** 22. Шифри зсуву.

	23. Лінійні шифри. 24. Афінні шифри. 25. Алгоритмічна реалізація афінних шифрів (алгоритми шифровування та дешифрування) **Розділ 4: Складність алгоритмічних задач** 26. Задачі обчислення, розпізнавання, пошуку 27. Прямолінійні програми 28. Складність алгоритмів 29. Поліноміальна складність 30. Порівняння складності алгоритмів через (поліноміальне зведення) 31. Клас NP, проблема тисячоліття: чи P=NP. **Розділ 5: Складність арифметичних задач** 32. Швидкий (бінарний) алгоритм підняття до степені та його програмна реалізація 33. Розклад на прості множники 34. Розпізнавання та знаходження первісного кореня (тобто генератора мультиплікативної групи скінченного поля простого порядку) 35. Зведення задачі розпізнавання первісного кореня до задачі розкладу на множники 36. Прості числа Сен Жермен та їх застосування до розпізнавання та знаходження первісних коренів 37. Квадратичні лишки, розпізнавання квадратичних лишків за простим модулем 38. Символ Лежандра, та його властивості 39. Критерій Ойлера, алгоритми розпізнавання квадратичних лишків за простим модулем 40. Символ Якобі, його властивості. 41. Квадратичний закон взаємності Гауса 42. Обчислення символу Якобі за допомогою квадратичного закону взаємності Гауса (алгоритм обчислення символу Якобі) 43. Розподіл простих чисел: постулат Бертрана та його покращені версії **Розділ 6: Тестування простоти** 44. Сито Ератосфена та його програмна реалізація 45. Псевдопрості числа Ферма 46. Числа Кармайкла 47. Псевдопрості числа Ейлера 48. Сильно псевдопрості числа 49. Ймовірнісний тест простоти Соловея-Штрассена 50. Ймовірнісний тест простоти Міллера-Рабіна 51. Детермінований поліноміальний тест простоти для чисел менших за 25 000 000 000 52. Детермінований поліноміальний тест простоти у припущенні гіпотези Рімана 53. Детермінований поліноміальний тест простоти AKS (Agrawal–Kayal–Saxena) 54. Генератори простих чисел 55. Генератори простих чисел Блюма та Сен Жермен **Розділ 7. Факторизація та квадратні корені** 56. Розклад на прості множники (алгоритми) 57. Розпізнавання квадратичності (за простим та довільним модулем) 58. Алгоритм добування квадратного кореня за простим модулем 59. Алгоритм добування квадратного кореня за довільним модулем 60. Добування кореня по модулю чисел Блюма 61. Обчислення функції Ойлера та зведення цієї задачі до проблеми факторизації і навпаки 62. Алгоритми генерації первісних коренів по модулю простого числа Сен Жермен 63. Складність дискретного логарифмування **Розділ 8. Криптосистеми з відкритим ключем** 64. Концепція криптосистем з відкритим ключем 65. Криптосистема RSA, її обгрунтування та алгоритмічна реалізація 66. Криптосистема Рабіна та її алгоритмічна реалізація

	67. Ймовірнісне шифрування: концепція 68. Ймовірнісне шифрування на основі RSA 69. Ймовірнісне шифрування на основі квадратичності 70. Криптосистема ЕльГамала, її обгрунтування та алгоритмічна реалізація **Розділ 9. Протоколи** 71. Обмін ключами 72. Цифровий підпис, реалізація в RSA 73. Цифровий підпис, реалізація в ElGamal 74. Підкидання монети по телефону 75. Гра в карти заочно 76. Розподіл таємниці 77. Доведення без розголошення (на основі квадратичності) 78. Ідентифікація
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Таблиця 1. Схема курсу «Криптологія»

Тиж-день	Тема	План, короткі тези	Форма діяльності	Термін виконання
1	Класичні криптосистеми	1. Шифри простої заміни 2. Шифр зсуву 3. Частотний аналіз 4. Гомофонний шифр Гауса 5. Шифр 4-х квадратів 6. Шифри перестановки 7. Шифр Кардано 8. Шифр Віженера 9. Шифр Віженера з автоключем	л – 3 год п – 2 год	Один тиждень
2	Криптосистеми першої половини XX-го століття	1. Оцифровка повідомлень 2. Шифр одноразового блокноту 3. Шифри часів 2-й світової війни 4. Стандарт шифрування даних DES	л – 3 год п – 2 год	Один тиждень
3	Арифметичні інструменти	1. Алгоритм Евкліда знаходження найбільшого спільного дільника 2. Швидкість роботи алгоритму Евкліда 3. Розширений алгоритм Евкліда 4. Китайська теорема про остачі, застосування розширеного алгоритму Евкліда до алгоритмічної реалізації китайської теореми про остачі 5. Прості числа, основна теорема арифметики: розклад на прості множники	л – 3 год п – 2 год	Один тиждень
4	Обчислення в кільці остач	1. Кільце остач 2. Група оборотніх елементів кільця остач 3. Обчислення оборотніх елементів в кільці остач 4. Взаємно прості числа, функція Ейлера 5. Обчислення функції Ейлера, асимптотика функції Ейлера 6. Мала теорема Ферма та теорема Ейлера 7. Кільце матриць. Кількість невироджених nxn матриць над кільцем лишків	л – 3 год п – 2 год	Один тиждень
5	Афінні шифри	1. Шифри зсуву. 2. Лінійні шифри. 3. Афінні шифри. 4. Алгоритмічна реалізація афінних шифрів (алгоритми шифрування та дешифрування)	л – 3 год п – 2 год	Один тиждень
6	Захист індивідуальних завдань	Захист індивідуальних завдань з класичних та афінних шифрів	л – 3 год п – 2 год	Один тиждень
7	Складність алгоритмічних задач	1. Задачі обчислення, розпізнавання, пошуку 2. Прямолінійні програми 3. Складність алгоритмів 4. Поліноміальна складність 5. Порівняння складності алгоритмів через (поліноміальне зведення) 6. Клас NP, проблема тисячоліття: чи P=NP.	л – 3 год п – 2 год	Один тиждень
8	Складність арифметичних	1. Швидкий (бінарний) алгоритм підняття до степені та його програмна реалізація 2. Розклад на прості множники	л – 3 год п – 2 год	Один тиждень

	задач	3. Розпізнавання та знаходження первісного кореня 4. Зведення задачі розпізнавання первісного кореня до задачі розкладу на множники 5. Прості числа Сен Жермен та їх застосування до розпізнавання та знаходження первісних коренів 6. Дискретний логарифм		
9	Квадратичні лишки	1. Квадратичні лишки, розпізнавання квадратичних лишків за простим модулем 2. Символ Лежандра, та його властивості 3. Критерій Ойлера, алгоритми розпізнавання квадратичних лишків за простим модулем 4. Символ Якобі, його властивості. 5. Квадратичний закон взаємності Гауса 6. Обчислення символу Якобі за допомогою квадратичного закону взаємності Гауса (алгоритм обчислення символу Якобі)	л – 3 год п – 2 год	Один тиждень
10	Прості числа та тестування простоти	1. Розподіл простих чисел: постулат Бертрана та його покращені версії 2. Сито Ератосфена та його програмна реалізація 3. Псевдопрості числа Ферма 4. Числа Кармайкла 5. Псевдопрості числа Ейлера 6. Сильно псевдопрості числа 7. Ймовірнісний тест простоти Соловея-Штрассена	л – 3 год п – 2 год	Один тиждень
11	Генератори простих чисел	1. Ймовірнісний тест простоти Міллера-Рабіна 2. Детермінований поліноміальний тест простоти для чисел менших за 25 000 000 000 3. Детермінований поліноміальний тест простоти у припущенні гіпотези Рімана 4. Детермінований поліноміальний тест простоти AKS (Agrawal–Kayal–Saxena) 5. Генератори простих чисел 6. Генератори простих чисел Блюма та Сен Жермен	л – 3 год п – 2 год	Один тиждень
12	Добування квадратних коренів	1. Розпізнавання квадратичності (за простим та довільним модулем) 2. Алгоритм добування квадратного кореня за простим модулем 3. Алгоритм добування квадратного кореня за довільним модулем 4. Добування кореня по модулю чисел Блюма	л – 3 год п – 2 год	Один тиждень
13	Криптосистеми з відкритим ключем	1. Концепція криптосистем з відкритим ключем 2. Криптосистема RSA, її обгрунтування та алгоритмічна реалізація 3. Криптосистема Рабіна та її алгоритмічна реалізація 4. Криптосистема ЕльГамала, її обгрунтування та алгоритмічна реалізація	л – 3 год п – 2 год	Один тиждень
14	Ймовірнісне шифрування	1. Ймовірнісне шифрування: концепція 2. Ймовірнісне шифрування на основі RSA	л – 3 год п – 2 год	Один тиждень

		3. Ймовірнісне шифрування на основі квадратичності		
15	Протоколи	1. Обмін ключами 2. Цифровий підпис, реалізація в RSA 3. Цифровий підпис, реалізація в ElGamal 4. Підкидання монети по телефону 5. Гра в карти заочно 6. Розподіл таємниці 7. Доведення без розголошення (на основі квадратичності) 8. Ідентифікація	л – 3 год п – 2 год	Один тиждень
16	Захист індивідуальних завдань	Захист індивідуальних завдань по криптосистемах з відкритим ключем	л – 3 год п – 2 год	Один тиждень