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 алгебри,
топології та основ математики

проф. Банах Т. О.

Силабус з навчальної дисципліни
«ЕЛІПТИЧНІ КРИВІ ТА КРИПТОГРАФІЯ»,
що викладається в межах ОПП «Комп'ютерна алгебра,
криптологія та теорія ігор»
першого (бакалаврського) рівня вищої освіти
для здобувачів зі спеціальності 111 – Математика

Львів – 2022

Назва дисципліни	Еліптичні криві та криптографія
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, механіко-математичний факультет, м. Львів, вул. Університетська, 1, 79000
Факультет та кафедра, за якою закріплена дисципліна	Механіко-математичний факультет, кафедра алгебри, топології та основ математики
Галузь знань, шифр та назва спеціальності	Галузь знань: 11 Математика та статистика, Спеціальність: 111 Математика
Викладачі дисципліни	Мельник Іванна Орестівна, кандидат фізико-математичних наук, доцент, доцент кафедри алгебри, топології та основ математики
Контактна інформація викладачів	e-mail: ivanna.melnyk@lnu.edu.ua, https://new.mmf.lnu.edu.ua/employee/melnyk-i-o м. Львів, вул. Університетська, 1, ауд. 375 Роб. тел. (032) 239 41 72
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій або практичних занять (за попередньою домовленістю) за адресою: м. Львів, вул. Університетська 1, ауд. 375. Можливі консультації онлайн на платформі Zoom або Microsoft Teams (за попередньою домовленістю). Для погодження часу консультацій слід писати на електронну пошту викладача.
Сторінка дисципліни	https://new.mmf.lnu.edu.ua/course/eliptychni-kryvi-ta-kryptohrafiia
Інформація про дисципліну	Дисципліна «Еліптичні криві та криптографія» є вибірковою навчальною дисципліною зі спеціальності 111 «Математика» для освітньої програми «Комп'ютерна алгебра, криптологія та теорія ігор» першого (бакалаврського) рівня вищої освіти, яка викладається в шостому семестрі в обсязі 5 кредитів (за Європейською кредитно-трансферною системою ECTS).
Коротка анотація дисципліни	Дисципліна «Еліптичні криві та криптографія» поглиблює знання студентів про властивості комутативних кілець і пов'язаних з ними об'єктів (модулів, ідеалів тощо), а також ознайомлює із застосуваннями комутативної алгебри. Курс має на меті розширити знання студентів з алгебри та допомогти їм здобути практичні навички в застосуванні алгебраїчних методів та їх комп'ютерній реалізації.
Мета та цілі дисципліни	Мета вивчення дисципліни «Еліптичні криві та криптографія»: навчити студентів використовувати еліптичні криві для побудови безпечних криптосистем. Завдання дисципліни: ознайомлення з основними властивостями еліптичних кривих та їхніми застосуваннями в криптографії; вивчення криптографічних протоколів, що використовують еліптичні криві, та їхніх застосувань у практичних задачах; розуміння потенційних загроз безпеці еліптичних криптосистем та способів захисту від них; аналіз ефективних алгоритмів реалізації еліптичних криптосистем.
Література для вивчення дисципліни	1. *Buell D.* Fundamentals of Cryptography. Introducing Mathematical and Algorithmic Foundations. – Springer, 2021. – 279 p. 2. *Washington L. C.* Elliptic Curves: Number Theory and Cryptography, Second Edition. – New York: Chapman and Hall/CRC, 2008. – 536 p.

	3. *Вербіцький О. В.* Вступ до криптології. – Львів: ВНТЛ, 1998. **4.** *Андрійчук В. І., Комарницький М. Я., Іщук Ю. Б.* Вступ до дискретної математики. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2003. **5.** *Koblitz N.* Algebraic aspects of cryptography. – Springer Berlin, Heidelberg, 2012. – 206 p. **6.** *Cox D., Little J. O'Shea D.* Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. – Springer, 2016. – 646 p. **7.** *Eisenbud D.* Commutative Algebra: with a View Toward Algebraic Geometry. – Springer, 1995. – 816 p. **8.** *Fulton W.* Algebraic Curves. An Introduction to Algebraic Geometry. – 2008. – 129 p. **9.** *Дрозд Ю. А.* Вступ до алгебричної геометрії. – Львів: ВНТЛ – Класика, 2004. – 115 с. **10.** *Дрозд Ю. А.* Алгебрична геометрія і її застосування. Курс лекцій. – Київський університет імені Тараса Шевченка, 2001. – 40 с. **11.** *Artin M.* Algebraic Geometry. – American Mathematical Society, 2022. – 318 p. **12.** *Hartshorne R.* Algebraic Geometry. – Springer New York, NY, 2013. – 496 p. **13.** Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – Інформаційні технології. Національний стандарт України. – ДСТУ 4145 – 2002. **14.** *Diffe W., Hellman M.E.* New direction in cryptography. – IEEE Transaction on Information Theory. – 1976. – v. 22. – P. 644-654. **15.** *Merkle R. and Hellman H.* Hiding Information and Signatures in Trap Door Knapsacks. – IEEE Transac. on Inform. Theory, September, 1978. – P. 241-245. **16.** *Rivest R., Shamir A., Adleman L.* A Method for Obtaining Digital Signature and Public Key Cryptosystems. – Communic. of the ACM, February. – 1978. – P. 36-45. **17.** *Miller G.* Riman's Hypothesis and Tests for Primality. – Procieedings of the Seventh Annual ACM Symposium on the Theory of Computing, May. 1975. – P. 47-49. **18.** *Rabin M.* Probabilistic Algorithm for Primality Testing. – Journal of Number Theory, December. 1980. – P. 70-79.
Обсяг дисципліни	**Загальний обсяг:** 150 годин. Всього аудиторних занять: 48 годин. З них 32 години лекцій, 16 годин практичних занять. Самостійна робота: 102 години. Кредитів: 5.
Очікувані результати навчання	Після завершення курсу «Еліптичні криві і криптографія» студент повинен: **Знати:** основні поняття теорії еліптичних кривих, основні алгоритми криптографії, принципи побудови сучасних криптографічних систем та основні математичні методи, що лежать в їх основі, принципи побудови криптографічних алгоритмів та криптографічних стандартів та їх використання, основні напрямки розвитку сучасних криптосистем. **Вміти**: оцінювати складність криптографічної системи, оцінювати складність алгоритму, обирати необхідні алгоритми для розв'язання практичних задач, програмно реалізовувати основні теоретико-числові алгоритми для розв'язання типових задач криптографії.

	У результаті вивчення навчальної дисципліни відповідно до освітньої програми формуються **програмні компетентності.** **Інтегральна компетентність** Здатність розв'язувати складні спеціалізовані практичні завдання в галузі середньої освіти, що передбачає застосування концептуальних методів освітніх наук, знань з математики, педагогіки, психології, теорії та методики навчання математики і характеризується комплексністю та невизначеністю умов організації освітнього процесу в закладах загальної середньої освіти. **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-7.** Здатність учитися і оволодівати сучасними знаннями. **ЗК-8.** Здатність до пошуку, обробки та аналізу інформації з різних джерел. **ЗК-12.** Здатність працювати автономно. **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-4.** Здатність конструювати формальні доведення з аксіомта постулатів і відрізняти правдоподібні аргументи від формально бездоганних. **СК-9.** Здатність застосовувати спеціалізовані мови програмування та пакети прикладних програм; **СК-11.** Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі. **Програмні результати навчання** **РН-1.** Знати основні етапи історичного розвитку математичних знань і парадигм, розуміти сучасні тенденції в математиці. **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-7.** Пояснювати математичні концепції мовою, зрозумілою для нефахівців у галузі математики. **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-11. Розв'язувати конкретні математичні задачі, які сформульовано у формалізованому вигляді; здійснювати базові перетворення математичних моделей. **РН-12.** Відшуковувати потрібну науково-технічну інформацію у науковій літературі, базах даних та інших джерелах інформації. **РН-15.** Знати теоретичні основи і застосовувати алгебраїчні методи для вивчення математичних структур. **РН-23.** Знати основи кодування, захисту інформації та захисту даних і застосовувати алгоритми комп'ютерної алгебри та методи криптології.
Ключові слова	Криптосистема, еліптична крива, тест простоти Соловея-Штрассена, Міллера-Рабіна, дискретний логарифм, числа Ферма, метод факторизації Ферма, ро-метод Полларда.
Формат дисципліни	Очний
Теми	Перелік тем подано в додатку у формі схеми курсу.
Підсумковий контроль, форма	Залік. Залік виставляється за результатами навчальної діяльності студентами протягом семестру.
Пререквізити	Для вивчення дисципліни студенти потребують знань з дисциплін «Загальна алгебра», «Теорія чисел», «Дискретна математика».
Навчальні методи та техніки, які будуть використовуватися під час викладання дисципліни	Лекції, виконання практичних завдань, консультації.
Необхідне обладнання	Дошка, крейда, навчальні посібники, мультимедійний проектор, комп'ютер, доступ до мережі «Інтернет», доступ до платформ Microsoft Teams, Zoom, Telegram, електронна пошта.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Результати навчальної діяльності студентів в семестрі оцінюються за 100-бальною шкалою. **Письмові роботи:** Очікується, що студенти протягом семестру виконають одну контрольну роботу, два колоквіуми та одне індивідуальне завдання. Варіант контрольної роботи включає в себе задачі різних типів та рівнів складності. Колоквіум передбачає виконання тестових теоретичних завдань та надання розгорнутих відповідей на теоретичні питання з доведеннями теорем. Бали нараховуються за таким співвідношенням: • робота під час практичних занять (7 занять): 7% семестрової оцінки; максимальна кількість балів – 7; участь в кожному практичному занятті оцінюється в 1 бал. • одна контрольна роботи (практична частина курсу): 20% семестрової оцінки; максимальна кількість балів – 20. • 2 колоквіуми (теоретична частина курсу) по 20 балів кожний: 40% семестрової оцінки; максимальна кількість балів – 40; 20 х2=40. • одне індивідуальне завдання – 33% семестрової оцінки; максимальна кількість балів – 33. Залік виставляється на останньому занятті за результатами набраних балів. Підсумкова максимальна кількість балів – 100.

Порядок вивчення та оцінювання дисципліни доводиться до відома студентів протягом семестру. Успішність навчання студентів оцінюється за шкалою «зараховано»/ «не зараховано».

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 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 матеріалу, допускав принципові помилки при виконанні більшості передбачених програмою завдань, неспроможний самостійно засвоїти програмний матеріал і потребує повторного вивчення дисципліни.

Політика курсу

Академічна доброчесність. Очікується, що студенти виконуватимуть навчальні завдання, завдання поточного та підсумкового контролю самостійно, не користуються недозволеними засобами, не видають за свої результати роботи інших людей. При використанні чужих ідей і тверджень у власних роботах посилаються на використані джерела інформації. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману. Жодні форми недоброчесності не толеруються.

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття дисципліни. Студенти повинні інформувати викладача про неможливість відвідати заняття. За

	згодою декана та викладача дозволяється перейти на індивідуальний графік занять. У будь-якому випадку студенти зобов'язані дотримуватися термінів виконання усіх передбачених видів робіт. **Література.** Література, яку студенти не зможуть знайти самостійно, може бути 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. **Політика виставлення балів.** Враховуються бали поточного та підсумкового контролю, а також самостійної роботи. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано після завершення курсу.

ДОДАТОК

Схема курсу

Тиждень, год.	Тема, план, короткі тези	Форма діяльності (заняття)* *лекція, самостійна, дискусія, групова робота)	Література. Ресурси в Інтернеті	Завдання, год.	Термін виконання
1	2	3	4	5	6
Перший тиждень, 2 год.	Тема 1. Основні поняття та задачі криптографії	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
Другий тиждень, 4 год.	Тема 1. Основні поняття та задачі криптографії	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
	Тема 1. Основні поняття та задачі криптографії	Практичне заняття, 2 год.	Див. Література для вивчення дисципліни	Виконати домашнє завдання, 4 год.	До наступного заняття
Третій тиждень, 2 год.	Тема 2. Тестування чисел на простоту і побудова великих простих чисел	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
Четвертий тиждень, 4 год.	Тема 2. Тестування чисел на простоту і побудова великих простих чисел	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
	Тема 2. Тестування чисел на простоту і побудова великих простих чисел	Практичне заняття, 2 год.	Див. Література для вивчення дисципліни	Виконати домашнє завдання, 4 год.	До наступного заняття
П’ятий тиждень, 2 год.	Тема 2. Тестування чисел на простоту і побудова великих простих чисел	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
Шостий тиждень, 4 год.	Тема 3. Факторизація цілих чисел	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
	Тема 2. Тестування чисел на простоту і побудова великих простих чисел	Практичне заняття, 2 год.	Див. Література для вивчення дисципліни	Виконати домашнє завдання, 4 год.	До наступного заняття
Сьомий тиждень, 2 год.	Тема 3. Факторизація цілих чисел	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу. Підготуватися до контролю знань, 8 год.	Один тиждень
Восьмий тиждень, 4 год.	Колоквіум №1	Лекція, 2 год.	Див. Література для вивчення дисципліни		Один тиждень
	Тема 3. Факторизація цілих чисел	Практичне заняття, 2 год.	Див. Література для вивчення дисципліни	Виконати домашнє завдання, 4 год.	До наступного заняття
Дев’ятий	Тема 4. Еліптичні криві	Лекція, 2 год.	Див. Література для вивчення	Опрацювати рекомендовану	Один тиждень

тиждень, 2 год.			дисципліни	літературу, 4 год.	
Десятий тиждень, 4 год.	Тема 4. Еліптичні криві	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
	Тема 4. Еліптичні криві	Практичне заняття, 2 год.	Див. Література для вивчення дисципліни	Виконати домашнє завдання, 4 год.	До наступного заняття
Одинадцятий тиждень, 2 год.	Тема 5. Алгоритми дискретного логарифмування	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
Дванадцятий тиждень, 4 год.	Тема 5. Алгоритми дискретного логарифмування	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
	Тема 4. Еліптичні криві	Практичне заняття, 2 год.	Див. Література для вивчення дисципліни	Виконати домашнє завдання, 4 год.	До наступного заняття
Тринадцятий тиждень, 2 год.	Тема 6. Застосування еліптичних кривих для перевірки простоти і факторизації. Дискретне логарифмування на еліптичній кривій	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
Чотирнадцятий тиждень, 4 год.	Тема 6. Застосування еліптичних кривих для перевірки простоти і факторизації. Дискретне логарифмування на еліптичній кривій	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу, 4 год.	Один тиждень
	Тема 5, 6. Застосування еліптичних кривих для перевірки простоти і факторизації. Дискретне логарифмування на еліптичній кривій	Практичне заняття, 2 год.	Див. Література для вивчення дисципліни	Виконати домашнє завдання. Підготуватися до контролю знань. Виконати індивідуальне завдання, 14 год.	До наступного заняття
П’ятнадцятий тиждень, 2 год.	Тема 6. Застосування еліптичних кривих для перевірки простоти і факторизації. Дискретне логарифмування на еліптичній кривій	Лекція, 2 год.	Див. Література для вивчення дисципліни	Опрацювати рекомендовану літературу. Підготуватися до контролю знань, 8 год.	Один тиждень
Шістнадцятий тижень, 4 год.	Колоквіум №2	Лекція, 2 год.			
	Контрольна робота №1	Практичне заняття, 2 год.			
Разом		32 год. лекцій, 16 год. практичних занять		102 год. самостійної роботи	