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

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри П.С.Венгерський

Силабус з навчальної дисципліни
“Основи криптографії”,
що викладається в межах ОПП Кібербезпека
першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	**Основи криптографії**
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 кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Хохлачова Юлія Євгеніївна, кандидат технічних наук, професор кафедри кібербезпеки Трушевський Валерій Миколайович доцент кафедри кібербезпеки
Контактна інформація викладачів	yuliia.khokhlachova@lnu.edu.ua https://ami.lnu.edu.ua/employee/khokhlachova-yu-ye; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/course/matematychna-kryptolohiia-kb
Інформація про дисципліну	Дисципліна “Основи криптографії” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у 4-му семестрі в обсязі 6-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетнтностей у галузі застосування криптографічних методів до захисту інформації, вивчення математичних основ, загальних ідей та концепцій сучасної криптографії, ознайомлення з відомими криптосистемами - від найдавніших до сучасних, вміння здійснювати криптоаналіз, програмна реалізація з застосуванням криптосистем до захисту важливої інформації.
Мета та цілі дисципліни	Метою курсу є вивчення математичних основ симетричних та асиметричних криптосистем, вміння здійснювати криптоаналіз, розуміння ефективності та надійності алгоритмів шифрування для подальшого їх застосування на практиці з метою захисту інформації.
Література для вивчення дисципліни	*Основна* 1. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації: підручник – К.: ЦП «Компринт», 2021. – 296 с. 2. Гаврилова А.А., Хохлачова Ю.Є., Погорелов В.В. Аналіз застосування гібридних криптокодових конструкцій для підвищення рівня стійкості геш-кодів до злому: стаття - Безпека інформації. Том 28 № 2 (2022). С. 87-101. 3. Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В. Кібербезпека: основи кодування та криптографії: навч. посібник. – Харків: ХПІ, 2023. – 658 с.

	4. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посібник. – Запоріжжя : НУ «Зап. пол.», 2020. – 192 с 5. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник – К.: НАУ, 2023. – 312. 6. Стасюк М. Елементи математичних основ криптографії : навчальний посібник – Львів : ЛДУ БЖД, 2021. – 216 с. 7. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120с. 8. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography, 2020. – 943 p. 9. David Wong. Real-World Cryptography, Version 12, 2021 – 369 p. *Додаткова* 10. Вербіцький О.В. Вступ до криптології. Львів, 1998 – 247с. 11. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце у сучасному суспільстві, Одеса, 2003. – 80 с. 12. Корченко О. Г. Прикладна криптологія: системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. 13. Остапов С. Е., Валь Л.О. Основи криптографії: Навчальний посібник. – Чернивці: Книги – ХХІ, 2008. – 188 с. 14. Фільштінський В. А.,Бережний А. В. – Суми: Сумський державний університет, 2011. – 138 с. 15. Douglas R. Stinson. Introduction to modern cryptography. Second Edition. 2015. – 576 p. 16. Douglas R. Stinson, Maura B. Paterson. Cryptography. Theory and Practice. Fourth Edition, 2019. – 580 p. 17. Bruce Schneier. Applied cryptography, second edition, protocols, algorithms, and source code in C, 2015. – 792 p. 18. Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, Gerhard Rosenberger. A Course in Mathematical Cryptography, 2015. – 376 p. 19. Alko R. Meijer. Algebra for Cryptologists, 2016. – 301 p. 20. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, 2014. – 538 p. 21. Nigel P. Smart. Cryptography Made Simple, 2016. – 481 p. 22. Christof Paar · Jan Pelzl. Understanding Cryptography. A Textbook for Students and Practitioners, 2010. – 372 p.
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 80 год., з них 32 год. лекцій та 48 год. лабораторних робіт. Самостійної роботи: 100 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - математичні основи криптографічних методів, основні поняття; - ефективність, надійність та складність криптографічних алгоритмів;

	- елементи криптоаналізу; - класичні криптографічні алгоритми; - роторні криптосистеми; - потокові шифри та їх класифікацію; - математичні основи блокових шифри; - математичні основи криптосистем з відкрити ключем - хеш-функції. **вміти:** - застосовувати різні типи криптографічних систем в залежності від задачі; - оцінювати складність криптографічних алгоритмів; - проводи криптоаналіз зашифрованої інформації; - шифрувати конфіденційні дані стандартними алгоритмами шифрування; - здійснювати проектування (розробку) систем, технологій і засобів кіберзахисту при здійсненні професійної діяльності. **Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 3, КЗ 4, КЗ 5, КЗ 7, КФ 1, КФ 5, КФ 7, КФ 9, КФ 10; та програмних результатів навчання: ПРН 1, ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 7, ПРН 8, ПРН 9, ПРН 16, ПРН 22, ПРН 27, ПРН 31, ПРН 33, ПРН 34, ПРН 44, ПРН 45, ПРН 46, ПРН 47, ПРН 48.**
Ключові слова	Криптологія, криптографія, криптоаналіз, асиметрична криптосистема, симетрична криптосистема, класичні криптографічні алгоритми, кодування даних, математичний підхід до шифрування даних, групи, гомоморфізм, алгоритм Евкліда, ізоморфізм кілець, функція Ейлера, конгруенції, афінні шифри, потокові та блокові шифри, складність алгоритмів, класи складності *P* та *NP*, хеш-функції (SHA-256), поле Галуа.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у схемі курсу нижче
Підсумковий контроль, форма	Екзамен у кінці семестру. Формат екзамену: письмовий тестовий.
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1) Моделі та методи дискретної математики; 2) Застосування дискретної математики в криптології; 3) Обчислювальна геометрія та алгебра; 4) Програмування; 6) Застосування теорії ймовірностей в кібербезпеці; 7) Основи кібербезпеки.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Індивідуальні завдання
Необхідне обладнання	Лабораторія з обладнаними робочими станціями. IDE для програмування мовою C++, C#, Python або Java.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50 • екзамен: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100.

	Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. 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 незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом. **Література.** Уся 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. **Політика виставлення балів.** Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. 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. Жодні форми порушення академічної доброчесності не толеруються.
Питання до екзамену	1. Класифікація методів шифрування. Класична криптографічна схема 2. Криптографічна стійкість, принцип Керкгоффза. Криптографічний аналіз. 3. Шифри перестановки: шифр частоколу, шифр Скитала, матричний шифр обходу, шифр Кардано. Криптоаналіз. 4. Шифри заміни: шифр Цезаря, шифр простої заміни, гомофонний шифр, поліграмні шифри. Частотний криптоаналіз. 5. Поліалфавітні шифри. Шифр Віженера. Криптоаналіз. 6 Роторні криптосистеми. Шифр Enigma. 6. Шифр одноразового блокноту, надійність, ідеальна секретність. Система Вернама. 7. Потокові шифри: WEP 802.11b, WPA. 9. Класифікація потокових шифрів. Шифри A5, RC4. 8. Кількаразове шифрування, ADFFVX. 9. Елементарна криптографія. Основні поняття. Відображення. Теорема про обернене відображення. 10. Блоковий шифр. Дешифрування ітераціями. Метод ітерацій. 11. Групи. Порядок групи. Теорема Лагранжа. Гомоморфізм. Група перестановок. 12. Алгоритм Евкліда. Ефективність. Наслідок з алгоритму Евкліда. 17. Розширений алгоритм Евкліда. Розклад на прості співмножники. 18. Конгруенції та їх властивості. 13. Кільця. Кільце лишків. Обернений елемент в кільці лишків. Функція Ейлера. 14. Китайська теорема про остачі. Ізоморфізм кілець. 15. Кільце матриць. Формула оберненої матриці. Обчислення функції $\phi_k(n)$. 16. Афінні шифри. Лінійний шифр та шифр зсуву. 17. Афінні шифри вищих порядків.

	18. Афінні шифри. Криптоаналіз. 19. Алгоритми та типи їх складності. 20. Асимптотична складність. Нотація Ландау. 21. Класи складності P та NP. 22. NP – повні задачі. Доведення NP – повноти. 23. Криптографічні хеш-функції, основні властивості. Парадокс днів народжень. Захист від колізій 24. Алгоритми стійкого хешування MD5, SHA-512, Купина. 25. Цілісність даних та аунтефікація повідомлень. Код виявлення модифікацій повідомлення MDC і код автентичності повідомлення MAC. 26. Дайджест повідомлення. Хеш-код аутентифікації повідомлення HMAC. CMAC. 27. Арифметичні операції в скінченному полі Галуа $G(2^8)$.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Тиж.	**Тема, план, короткі тези**	**Форма діяльності (заняття)**	**Література**	**Завдан-ня, год.**	**Термін виконання**
1	**Тема 1. Криптологія**. **Основні поняття та приклади**. (Роль криптографічних методів та їх застосування. Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз. Класифікація методів шифрування. Криптографічна стійкість.)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 1. Криптологія. **Основні поняття та приклади**. (Принцип Кергоффза. Методи криптоаналізу)	лаб.	[1-10]	4	
2	**Тема 2. Класичні криптографічні методи.** (Шифри перестановки та простої заміни, Шифр Скитала, шифр Ю. Цезаря, частотний криптоаналіз, гомофонний шифр, поліграмні шифри, Шифр Кардано)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 2. Класичні криптографічні методи. (Програмна реалізація шифрів перестановки, багаторазове шифрування)	лаб.	[1-10]	2	
3	**Тема 3. Поліалфавітні шифри. Шифр Віженера.** (Шифрування, дешифрування, криптоаналіз Казискі)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 3. Поліалфавітні шифри. Шифр Віженера. (Програмна реалізація шифрування, дешифрування та криптоаналізу Казискі)	лаб.		4	
4	**Тема 4. Роторні криптосистеми. Шифр Enigma.** (Роторні криптосистеми з одним та більше роторів. Принцип роботи шифру Enigma)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 4. Роторні криптосистеми. Шифр Enigma. (Криптоаналіз шифру Enigma.)	лаб.	[1-10]	2	
5	**Тема 5. Основи теорії секретного**	лекція,	[1-10]	2	1 тиждень

	зв'язку (К. Шеннона). Семантична та безумовна стійкість. (Гра у підслуховування. Поняття семантичної та безумовної стійкості)	самостійна робота		6	
	Тема 5. Основи теорії секретного зв'язку (К. Шеннона). Семантична та безумовна стійкість. (Доведення семантичної стійкості шифрів. Показати, що шифр Віженера не є семантично стійким)	лаб.	[1-10]	4	
6	**Тема 6. Шифр одноразового блокноту. Потокові шифри.** (Надійність шифру одноразового блокноту, система Вернама, класифікація потокових шифрів, приклади потокових шифрів: WEP 802.11, WPA, A5, RC4)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 6. Шифр одноразового блокноту. Потокові шифри. (Недоліки шифру одноразового блокноту. Ідеальна секретність, доведення безумовної стійкості)	лаб.	[1-10]	2	
7	**Тема 7. Математична криптологія. Основні поняття.** **(**Алфавіт, відображення, теорема про обернене відображення, блоковий шифр, дешифрування ітераціями, мультиплікативна група, порядок групи, група перестановок. Теорема Лагранжа. Гомоморфізм.**)**	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 7. Математична криптологія. Основні поняття. (Криптоаналіз блокових шифрів методом ітерацій, циклічні групи, приклади груп)	лаб.	[1-10]	4	
8	**Тема 8. Елементи теорії чисел. Розширений алгоритм Евкліда.** (Ефективність алгоритму Евкліда. Розширений алгоритм Евкліда, розклад на прості співмножники)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 8. Елементи торії чисел. Розширений алгоритм Евкліда. **(**Програмна реалізація розширеного алгоритму Евкліда**)**	лаб.	[1-10]	2	
9	**Тема 9. Модульна арифметика. Кільце лишків.** (Конгруенції та їх властивості, кільце лишків, поле, обернений елемент в кільці лишків)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 9. Модульна арифметика. Кільце лишків. (Програмна реалізація знаходження оберненого елемента в кільці лишків)	лаб.	[1-10]	4	
10	**Тема 10. Функція Ейлера. Мала теорема Ферма. Китайська теорема про остачі.** (Ізоморфізм кілець, формула для обчислення функції Ейлера, китайська теорема про остачі)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 10. Функція Ейлера. Мала теорема Ферма. Китайська теорема про остачі.	лаб.	[1-10]	2	1 тиждень

	(Обчислення функції Ейлера, практичне застосування китайської теореми про остачі, піднесення до степеня за модулем.)				
11	**Тема 11. Кільце матриць. Афінні шифри.** (Формула оберненої матриці. Лінійні шифри, шифри зсуву, афінні шифри вищих порядків, криптоаналіз.)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 11. Кільце матриць. Афінні шифри. (Програмна реалізація шифрування та дешифрування використовуючи афінні шифр вищих порядків)	лаб.	[1-10]	4	
12	**Тема 12. Алгоритми та їх складність. Класи складності задач *P* та *NP*** (Асимптотична складність, нотація Ландау, *NP*-повні задачі)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
	Тема 12. Алгоритми та їх складність. Класи складності *P* та *NP* (Визначення класів складності задач)	лаб.	[1-10]	2	1 тиждень
13	**Тема 13. Первісні корені. Квадратичні лишки. Тестування простоти.** (Псевдопрості числа. Мала теорема Ферма. Сито Ератосфена. Ймовірносний тест Соловея-Штрассена. Ймовірнісний тест Міллера-Рабіна)	лекція, самостійна робота	[1-10]	2 7	1 тиждень
	Тема 13. Первісні корені. Квадратичні лишки. Тестування простоти. (Програмна реалізація алгоритмів тестування на простоти на основі теореми Ферма)	лаб.	[1-10]	4	
14	**Тема 14. Важко розв'язні задачі. Односторонні функції.** (Задачі факторизації та дискретного логарифму. Добування квадратного кореня за простим модулем.)	лекція, самостійна робота	[1-10]	2 7	1 тиждень
	Тема 14. Важко розв'язні задачі. Односторонні функції.(Програмна реалізація задачі факторизації)	лаб.	[1-10]	2	1 тиждень
15	**Тема 15. Криптографічні хеш-функції. Цілісність даних та аунтефікація повідомлень.** (Основні властивості. Принцип роботи криптографічних хеш-функцій. Парадокс днів народжень. Захист від колізій. Дайджест повідомлення.)	лекція, самостійна робота	[1-10]	2 7	1 тиждень
	Тема 15. Криптографічні хеш-функції. Цілісність даних та аунтефікація повідомлень. (Алгоритми стійкого хешування MD5, SHA-512, Купина. Код виявлення модифікацій повідомлення MDC і код автентичності	лаб.	[1-10]	4	

	повідомлення MAC. Хеш-код аутентифікації повідомлення HMAC. CMAC.)				
16	**Тема 16. Арифметичні операції в скінченному полі Галуа $G(2^8)$.** **(**Додавання, множення та ділення за модулем незвідного полінома**)**	лекція, самостійна робота	[1-10]	2 7	1 тиждень
	Тема 16. Арифметичні операції в скінченному полі Галуа $G(2^8)$. **(**Знаходження оберненого елемента за модулем незвідного полінома.**)**	лаб.	[1-10]	2	