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

Затверджено
на засіданні
кафедри обчислювальної математики
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол № _1_ від _29 серпня_ 2023 р.)

Завідувач кафедри

Роман ХАПКО

Силабус з навчальної дисципліни
«Основи криптології»,
що викладається в межах першого (бакалаврського) рівня вищої освіти для здобувачів
зі спеціальності 113 – Прикладна математика

Львів 2023 р.

Назва дисципліни	Основи криптології
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра обчислювальної математики
Галузь знань, шифр та назва спеціальності	11 Математика та статистика 113 Прикладна математика
Викладачі дисципліни	Гарасим Ярослав Степанович, старший викладач кафедри обчислювальної математики; Музичук Юрій Анатолійович, доцент кафедри обчислювальної математики;
Контактна інформація викладачів	iaroslav.harasym@lnu.edu.ua; https://ami.lnu.edu.ua/employee/harasym; yuriy.muzychuk@lnu.edu.ua; https://ami.lnu.edu.ua/employee/muzychuk-yuriy; Головний корпус ЛНУ ім. І. Франка, каб. 262. м. Львів, вул. Університетська, 1.
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/course/basics-of-cryptology-applied-mathematics
Інформація про дисципліну	Дисципліна “Основи криптології” є дисципліною на вибір зі спеціальності 113 – прикладна математика, яка викладається в 8-му семестрі (4 кредити ECTS).
Коротка анотація дисципліни	Курс включає певний об’єм лекційних та лабораторних занять, а також передбачає виконання студентами індивідуальних завдань у галузі криптографії з елементами криптоаналізу. Предметом вивчення є сучасні методи криптографії та криптоаналізу, відповідний математичний апарат, різного призначення протоколи з використанням наявного інструментарія. В процесі вивчення курсу здійснюється порівняльний аналіз різних методів криптування з метою виявлення доцільності їх використання в кожному конкретному випадку.
Мета та цілі дисципліни	Метою вивчення дисципліни є ознайомлення зі сучасними методами захисту інформації.
Література для вивчення дисципліни	1. Вербіцький О.В. Вступ до криптології / О.В. Вербіцький. – Львів, ВНТЛ, 1998. – 248 с. 2. Kölbl Stefan Design and analysis of cryptographic algorithms / Stefan Kölbl. – Technical University of Denmark, DTU Compute, 2016. 3. Bourke Chris Cryptography and Computer Security / Chris Bourke. – University of Nebraska, 2015. 4. Samsonu Ch. Cryptography and network security / Ch. Samsonu. – Kallam

<table>
<tr><td></td><td>Haranadhareddy Institute of Technology, 2020.
5. Danniel Yang, Zhiyang He, Maxwell Johnson, etc. Lecture Notes on Introduction to Cryptography / Yang Danniel, He Zhiyang, Johnson Maxwell, etc. – Vipul Goya, 2020.
6. Bellare Mihir, Rogaway Phillip Introduction to Modern Cryptography / Mihir Bellare, Phillip Rogaway. – San Diego, California, 2005.</td></tr>
<tr><td>Обсяг курсу</td><td>Загальний обсяг: 120 годин. Аудиторних занять: 56 год., з них 28 год. лекційних та 28 години лабораторних робіт. Самостійної роботи: 64 год.</td></tr>
<tr><td>Очікувані результати навчання</td><td>Після завершення цього курсу студент буде:
Знати:
- основні симетричні та асиметричні методи криптування;
- базові протоколи передачі ключової інформації;
- основи побудови функцій хешування;
- принципи побудови та перевірки електронного підпису;
- принципи функціонування сертифікаційних центрів.
Вміти:
- застосовувати на практиці методи криптології при розв’язуванні різних задач захисту інформації;
- програмно реалізувати комплексну систему захисту даних.</td></tr>
<tr><td>Ключові слова</td><td>Криптологія, криптографія, криптоаналіз, стеганографія, хешування, електронний підпис, центр сертифікації, захист інформації.</td></tr>
<tr><td>Формат курсу</td><td>Очний.
Проведення лекцій, лабораторних робіт і консультацій.</td></tr>
<tr><td>Теми</td><td>Подано нижче у таблиці Схема курсу “Основи криптології”</td></tr>
<tr><td>Підсумковий контроль, форма</td><td>Залік.</td></tr>
<tr><td>Пререквізити</td><td>Для вивчення курсу студенти потребують базових знань з
- Лінійної алгебри;
- Чисельних методів лінійної алгебри;
- Програмування.</td></tr>
<tr><td>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</td><td>Презентації, лекції (лекція-розповідь, лекція-бесіда).
Індивідуальні завдання.</td></tr>
<tr><td>Необхідне обладнання</td><td>Комп’ютер із програмним забезпеченням Python, C#, Visual Studio, Visual Studio Code, Java, IntelliJ IDEA; доступ до Internet мережі.</td></tr>
<tr><td>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</td><td>Оцінювання проводиться за 100-бальною шкалою.
<table>
<tr><th colspan="2" rowspan="2">Оцінка за шкалою ECTS</th><th rowspan="2">Оцінка в балах</th><th colspan="3">Оцінка за національною шкалою</th></tr>
<tr><th colspan="2">Екзамен, диференційований залік</th><th>залік</th></tr>
<tr><td>A</td><td>Відмінно</td><td>100 - 90</td><td>Відмінно</td><td>5</td><td></td></tr>
</table></td></tr>
</table>

B	Дуже добре	81- 89	Добре	4	зараховано
C	Добре	71 -80			
D	Задовільно	61 - 70	Задовільно	3	
E	Достатньо	51- 60			
FX (F)	Незадовільно	0 - 50	Незадовільно	2	не зараховано

Впродовж семестру студент може отримати 100 балів. З них:
- за виконання індивідуальних завдань: максимальна кількість – 80 балів (8 завдань по 10б); 80% семестрової оцінки;
- за написання тестів (20 балів: 2 практичних завдання по 10б.); 20% семестрової оцінки.

Індивідуальні завдання:
Кожен студент отримує задачу, яку потрібно запрограмувати, використовуючи один із розглянутих на лекціях методів. Всі завдання мають термін здачі.

Критерії оцінювання індивідуальних завдань:

10балів	**Критерії оцінювання**
10балів	студент повністю і вчасно виконав умови завдання, алгоритм реалізовано правильно, відповідає на всі запитання, пов'язані з тематикою завдання, проводить чіткий аналіз та порівняння отриманих результатів;
8 балів	студент повністю виконав умови завдання, на деякі запитання, алгоритм реалізовано правильно, пов'язані з тематикою завдання, відповідає з незначними неточностями, проводить аналіз отриманих результатів з незначними неточностями; завдання виконане із затримкою;
6 балів	студент виконав завдання з незначними помилками, але самостійно їх виправляє, якщо на них вкаже викладач, на деякі запитання, пов'язані з тематикою завдання, відповідає з неточностями, проводить аналіз отриманих результатів з неточностями; завдання виконане із затримкою;
4 балів	студент виконав завдання частково, алгоритм реалізовано з помилками, які частково може виправити, якщо на них вкаже викладач, на запитання відповідає з помилками, проводить аналіз отриманих результатів з помилками; завдання виконане із затримкою;
2 бали	студент виконав завдання частково або з грубими помилками, які самостійно не може виправити, переважно не відповідає на запитання;
0 балів	студент не виконав завдання.

Тест. Проводиться у письмовій формі (2 завдання по 10 балів кожне).

Критерії оцінювання завдань на тест:

10 балів	**Критерії оцінювання**
10 балів	студент правильно виконав завдання;

	7-9 бали	студент виконав завдання з незначними помилками (на кінцевому етапі), але алгоритм розв'язування знає і вміє його застосовувати;
	3-6 балів	студент виконав завдання з помилками, алгоритм виконання, в основному, знає; володіє навчальним матеріалом на достатньому рівні;
	1-2 бали	студент виконав лише частину завдання або повністю, але зі значними помилками;
	0 балів	студент не виконав завдання.

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 незарахування викладачем, незалежно від масштабів плагіату чи обману.

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття 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 можуть 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 за індивідуальні завдання та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного 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.

Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу «Основи криптології»

Тиж-день	Тема, план, короткі тези	Форма діяльності (заняття)	Література. Ресурси в інтернеті	Завдання, год.	Термін виконання
1	**Тема 1.** Огляд задач криптології. Математичний апарат, односторонні функції, групи, кільця. Базові елементи теорії чисел.	лекція (2 год.)	[1, 5, 6]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Основи частотного аналізу. *Індивідуальне завдання №1*.	лабораторне заняття (2 год.)	[1, 5, 6]	Виконання завдання № 1 (3год.)	2 тижні
2	**Тема 2.** Класичні алгоритми криптування. Симетричні потокові алгоритми.	лекція (2 год.)	[1-3, 5-6]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Алгоритм Цезаря. Криптоаналіз. *Індивідуальне завдання №2*.	лабораторне заняття (2 год.)	[1-3, 5-6]	Виконання завданнь № 1-2 (3год.)	2 тижні
3	**Тема 3.** Модульна арифметика. Розширений алгоритм Евкліда. Афінний щифр.	лекція (2 год.)	[1-3, 5-6]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Афінний алгоритм. Криптоаналіз. *Індивідуальне завдання №3*. *Здача індивідуального завдання №1*.	лабораторне заняття (2 год.)	[1-3, 5-6]	Виконання завданнь № 1-3 (3год.)	2 тижні
4	**Тема 4.** Математична модель класичних алгоритмів криптування. Класифікація. Алгоритми Потра, Віженера, Альберті.	лекція (2 год.)	[1-3, 5]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Алгоритм Віженера. Методи його криптоаналізу. *Індивідуальне завдання №4*. *Здача індивідуального завдання №2*.	лабораторне заняття (2 год.)	[1-3, 5]	Виконання завданнь № 2-4 (3год.)	2 тижні
5	**Тема 5.** Блочні шифри. Маршрутні перестановки. Шифри Кардано та частокола	лекція (2 год.)	[1-3, 5]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Шифр Кардано. Криптоаналіз. *Індивідуальне завдання №5*. *Здача індивідуального завдання*	лабораторне заняття (2 год.)	[1-3, 5]	Виконання завданнь № 3-5 (3год.)	2 тижні

	№3.				
6	**Тема 6.** Арифметика довгих чисел. Теореми обгрунтування арифметичниз алгоритмів. Представлення довгих чисел структурами даних.	лекція (2 год.)	[1, 6]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Класичні методи роботи з довгими числами. *Здача індивідуального завдання №4.*	лабораторне заняття (2 год.)	[1, 6]	Виконання завданнь № 4-5 Програмування (3год.)	1 тиждень
7	**Тема 7.** Мала теорема Ферма. Функція Ейлера та її властивості. Тести простоти чисел.	лекція (2 год.)	[1, 4-6]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Побудова великих простих чисел. *Індивідуальне завдання №6. Здача індивідуального завдання №5.*	лабораторне заняття (2 год.)	[1, 4-6]	Виконання завданнь № 5-6 (2год.)	2 тижні
8	**Тема 8.** Асиметричні шифри. Алгоритм RSA. Стійкість алгоритму. Метод факторизації Ферма.	лекція (2 год.)	[1, 4-6]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Алгоритм RSA. Методи криптоаналізу. *Індивідуальне завдання №7. Здача індивідуальних завданнь.*	лабораторне заняття (2 год.)	[1, 4-6]	Виконання завданнь № 6-7 (2год.)	2 тижні
9	**Тема 9.** Асиметричні шифри. Алгоритми Поліга-Хелмана та Ель-Гамаля. Методи передачі ключів. Алгоритм Діффі-Хелмана. Дво та тристоронні протоколи.	лекція (2 год.)	[1, 4-6]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Керування ключами. *Здача індивідуального завдання №6.*	лабораторне заняття (2 год.)	[1, 4-6]	Виконання завданнь № 6-7 Програмування (3год.)	1 тиждень
10	**Тема 10.** R. Функції хешування. Принципи побудови. Основи алгоритмів MD та SHA.	лекція (2 год.)	[3]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Алгоритми MD2 та SHA512. *Здача індивідуального завдання №7.*	лабораторне заняття (2 год.)	[3]	Виконання завдання № 7 Програмування (2год.)	1 тиждень
11	**Тема 11.** Схема електронного	лекція	[1, 5]	Опрацювання	1 тиждень

	підпису. Основи функціонування центру сертифікації відкритих ключів.	(4 год.)		лекційного матеріалу (2год.)	
	Побудова електронного підпису на базі алгоритму RSA. *Індивідуальне завдання №8. Здача індивідуальних завдань.*	лабораторне заняття (2 год.)	[1, 5]	Виконання завдання № 8 Програмування (3год.)	2 тижні
12	**Тема 12.** Схема розділення секрету. Алгоритм Шаміра та його модифікації.	лекція (2 год.)	[5]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Алгоритм розділення секрету. *Здача індивідуальних завдань*.	лабораторне заняття (2 год.)	[5]	Виконання завдання № 8 Програмування (2год.)	1 тиждень
13	**Тема 13.** Еліптичні криві. Основні операції на кривих. Геометрична інтерпретація.	лекція (4 год.)	[1-6]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Приклади реалізації методів на основі еліптичних кривих. *Здача індивідуального завдання №8*.	лабораторне заняття (2 год.)	[1-6]	Виконання завдання № 8 Програмування (2год.)	1 тиждень
14	**Тема 14.** Захист програмного забезпечення. Основи захисту даних від копіювання.	лекція (2 год.)	[4]	Опрацювання лекційного матеріалу (2год.)	1 тиждень
	Здача індивідуальних завдань. Письмовий тест.	лабораторне заняття (2 год.)	[4]	Виконання тесту (2год.)	під час заняття