Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра фундаментальної математики

"ЗАТВЕРДЖУЮ"
В.о. декана факультету
математики і інформатики

Євген МЕНЯЙЛОВ

"__" серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Вступ до математичної криптографії

рівень вищої освіти перший (бакалаврський)

галузь знань 11 Математика та статистика

спеціальність 113 Прикладна математика

освітня програма «Прикладна математика»

спеціалізація

вид дисципліни за вибором

факультет математики і інформатики

2025 / 2026 навчальний рік

Програму рекомендовано до затвердження Вченою радою факультету математики і інформатики

“26” серпня 2025 року, протокол № 10

РОЗРОБНИК ПРОГРАМИ:
Гончарук Анна Борисівна, доктор філософії, викладач кафедри фундаментальної математики.

Програму схвалено на засіданні кафедри фундаментальної математики

Протокол від “26” серпня 2025 року №1.

В.о. завідувача кафедри Сергій ГЕФТЕР

Програму погоджено з гарантом освітньо-професійної програми

Гарант освітньо-професійної програми «Прикладна математика»

Сергій ПОСЛАВСЬКИЙ

Програму погоджено науково-методичною комісією факультету математики і інформатики

Протокол від “26” серпня 2025 року № 1

Голова науково-методичної комісії факультету математики і інформатики

Євген МЕНЯЙЛОВ

ВСТУП

Програма навчальної дисципліни **«Вступ до математичної криптографії»** складена відповідно до освітньо-професійної програми підготовки бакалавр
спеціальності F1 «Прикладна математика»
освітньо-професійна програма «Прикладна математика»

Опис навчальної дисципліни

1. **Опис навчальної дисципліни**

1.1. Метою викладання навчальної дисципліни є ознайомлення майбутніх спеціалістів з основними розділами сучасної криптографії.

1.2. Основними завданнями вивчення дисципліни є

1) Ознайомити студентів з основними поняттями криптографії, історією розвитку криптографії та основними класичними загальновідомими методами шифрування
2) Надати уявлення про сучасні криптографічні алгоритми асиметричного шифрування, такими як обмін ключами Діффі-Геллмана, протокол RSA,ECC та інші та про математичне підґрунтя цих протоколів: необхідні теореми теорії чисел, теорії груп, теорії полів, теорії алгоритмів тощо
3) Розглянути основні напрямки застосування криптографічних протоколів для аутентифікації, цифрового підпису, електронних платежів тощо
4) Надати уявлення про методи криптоаналізу та приклади можливих вразливостей криптографічних систем
5) Ознайомити зі структурою статей по криптографії

1.3. Кількість кредитів – **4**

1.4. Загальна кількість годин* – **120**

1.5. Характеристика навчальної дисципліни	
За вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
3-й	
Семестр	
5-й	
Лекції	
32	
Практичні, семінарські заняття	
32	
Лабораторні заняття	
-	
Самостійна робота	
56	
в тому числі індивідуальні завдання	
-	

** у разі формування малочисельних груп обсяг аудиторного навчального навантаження, відведеного на вивчення навчальної дисципліни, зменшується відповідно до Положення про планування й звітування науково-педагогічних працівників Харківського національного університету імені В.Н. Каразіна.*

1.6. Перелік компетентностей, що формує дана дисципліна
1.6.1. Формування наступних інтегральної та загальних компетентностей
ІК01. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми прикладної математики у професійній діяльності або у процесі навчання, що передбачає застосування математичних теорій та методів і характеризується комплексністю та невизначеністю умов.
ЗК02. Здатність застосовувати знання у практичних ситуаціях.
ЗК06. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК07. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
1.6.2. Формування наступних фахових компетентностей
ФК02. Здатність виконувати завдання, сформульовані у математичній формі.
ФК18. Здатність оцінити рівень математичного обґрунтування методів, які застосовуються для розв'язання конкретних прикладних задач.

1.7. Перелік результатів навчання, що формує дана дисципліна
РН01. Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.
РН02. Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами.
РН04. Виконувати математичний опис, аналіз та синтез дискретних об'єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів.

1.8. Пререквізити: «Елементи алгебри та теорії чисел»

2. Тематичний план навчальної дисципліни

Тема 1. Класична криптографія

2. Шифр Цезаря, Шифр Віженера, Афінний шифр

Тема 2. Асиметрична криптографія

3. Складність алгоритмів
4. Протокол обміну ключем Діффі-Геллмана.
5. Протокол RSA. Електронний підпис оснований на протоколі RSA. Особливості використання RSA
6. Алгоритм Ель-Гамаля. Електронний підпис на основі алгоритму Ель-Гамаля

Тема 3. Функція хешування

7. Функція хешування
8. Колізія хеш-функції, перебір за словником, атака "днів народження"

Тема 4. Криптоаналіз. Криптографічна система RSA

9. Засліплення, атака «людина посередині»
10. Вибір значень: маленька відкрита експонента, теорема Копперсміта і атака Хадстеда, маленька закрита експонента і атака Вінера
11. Атаки на реалізацію: атака по часу і атака Блейхенбахера

Тема 5. Еліптична криптографія

12. Скінченні поля

13. Еліптичні криві. Еліптичні криві над скінченними полями. Теорема Гассе. Протокол Діффі-Геллмана для еліптичних кривих. Цифровий підпис ECDSA

Тема 6. Застосування криптографічних алгоритмів

14. Підкидання монетки по телефону
15. Не відстежувані електронні платежі. Електронна готівка
16. Доведення з нульовим знанням. Алгоритм Шнорра

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	Денна форма						Заочна форма					
	Усього	у тому числі					Усього	у тому числі				
		л	п	лаб	інд	ср		л	п	лаб	інд	ср
1	2	3	4	5	6	7	8	9	10	11	12	13
Тема 1. Класична криптографія	6	2	2			2						
Тема 2.Асиметрична криптографія	26	4	6			16						
Тема 3. Функція хешування	4	2	2									
Тема 4. Криптоаналіз. Криптографічна система RSA	42	10	12			20						
Тема 5. Еліптична криптографія	26	8	8			10						
Тема 6. Застосування криптографічних алгоритмів	16	6	2			8						
Разом	**120**	**32**	**32**			**56**						

4. Теми семінарських (<u>практичних</u>, лабораторних) занять

№ з/п	*Назва теми*	*Кількість годин*
1	Класична криптографія. Шифр Цезаря, Шифр Віженера, Афінний шифр. Розв’язання задач.	2
2	Складність алгоритмів.	2
3	Обмін ключем Діффі-Геллмана. Алгоритм RSA. Реалізація.	2
4	Функція хешування: атака «днів народження», доведення в задачах.	2
5	Електронний підпис. Алгоритм Ель Гамаля. Засліплення. Реалізація.	2
6	Розв’язання задач: алгоритм RSA, електронний підпис	6
7	Атака Хастеда, атака Вінера, атака Копперсміта	4
8	Атака Блейхенбахера. Розбір статті.	2
9	Еліптичні криві. Операції з точками. Скінченні поля	4
10	Еліптична криптографія. Реалізація	2

11	Контрольна робота	2
12	Підкидання монетки по телефону. Доведення з нульовим знанням	2
Разом		32

5. Завдання для самостійної роботи

№ з/п	*Види, зміст самостійної роботи*	*Кількість годин*
1	Розв'язання задач: класична криптографія	2
2	Протокол Діффі-Геллмана і складність алгоритмів	4
3	Розбір статті: атаки на RSA	10
4	Алгоритм RSA і атаки на нього	10
5	Розбір статті: атака Блейхенбахера	10
6	Розв'язання задач: алгоритм RSA, алгоритм Ель Гамаля, цифровий підпис	8
7	Еліптичні криві. Еліптична криптографія	8
8	Підготовка до заліку	4
Разом		56

6. Індивідуальні завдання

відсутні

7. Методи навчання

Пояснювально-ілюстративний, репродуктивний, частково-пошуковий.

8. Методи контролю

Перевірка виконання домашніх завдань, поточне опитування за лекційним матеріалом, перевірка залікової роботи.

9. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завдання					Залікова робота	Сума
Домашні завдання				Контрольна робота		
Тема 1	Тема 2	Тема 4	Тема 5			
5	14	15	11	15	40	100

Не передбачається мінімальна кількість балів з навчальної дисципліни, яку здобувач вищої освіти повинен набрати під час поточного контролю, самостійної роботи, контрольної роботи для допуску до складання підсумкового контролю (заліку).

Здобувачам освіти, які отримали сертифікат про проходження курсу з тематики математичної криптографії у неформальній освіті, окремі теми можуть бути зараховані (у залежності від результатів навчання, отриманих у неформальній освіті). Зокрема, можуть бути враховані сертифікати, отримані при проходженні курсів з тематики математичної криптографії компанії Distributed Lab (https://distributed.education). Визнання результатів навчання регулюється Порядком визнання результатів навчання, отриманих у неформальній освіті, в Харківському національному університеті імені В.Н. Каразіна.

Критерії оцінювання:

Поточний контроль: бали нараховуються за виконання домашніх завдань і активність під час практичних занять. Домашні завдання передбачають письмове виконання завдань з поясненнями.

Контрольна робота містить десять розрахункових задач: п’ять по 1 балу, і п’ять по 2 бали.

Залікова робота проводиться у письмовій формі, передбачає відповідь на чотири питання:

1) один з алгоритмів, що розбиралися в курсі (відповідь має включати опис алгоритму, обґрунтування і приклад реалізації для малих чисел).

2) задача або питання за темою «асиметричне шифрування» або «атаки на алгоритм RSA» (відповідь має бути обґрунтованою)

3) задача на одну з тем «складність алгоритмів», «класичне шифрування» або «атака “днів народження”» (відповідь має бути обґрунтованою)

4) задача або питання з теми «скінченні поля» або «еліптична криптографія» (відповідь має бути обґрунтованою)

Максимальна оцінка за залікову роботу – 40 балів, за кожне питання по 10 балів.

Шкала оцінювання: *дворівнева*

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
50-100	зараховано
1-49	не зараховано

10.Рекомендована література

Основна література

1. О.І.Клесов. Елементарна теорія чисел та елементи криптографії. К.: -- ТВіМС, 2016
2. Л.Я. Глинчук. Криптологія. Навчальний посібник. Вежа-друк. Луцьк. 2014
3. Н.О. Щур, О.А. Покотило. Основи криптології. Навчальний посібник. Житомир. 2021
4. Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. Криптологія у прикладах, тестах і задачах. Навчальний посібник. Дніпропетровськ. НГУ. 2013

Допоміжна література

1. D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In CRYPTO '98, volume 1462 of Lecture Notes in Computer Science, pages 1-12. Springer-Verlag, 1998.
2. R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and PublicKey Cryptosystems. Commun. ACM 21, 2, pp. 120-126. 1978
3. Dan Boneh. Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS, pp. 203-213, 1999
4. Quisquater Jean-Jacques, Guillou Louis, Berson Tom. How to Explain Zero-Knowledge Protocols to Your Children, Advances in Cryptology - CRYPT0 ‘89, LNCS 435, pp. 628-631, 1990
5. Blum Manuel. Coin flipping by telephone. A protocol for solving impossible problems. SIGACT News 15, 1, pp. 23-27, 1983
6. Richard A. Mollin. An Introduction to Cryptography (Discrete Mathematics and Its Applications), 2nd edition. Chapman and Hall/CRC, 2006
7. Lawrence W. Washington, Elliptic Curves Number Theory and Cryptography, Second Edition, 2008.