Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра **фундаментальної математики**

"**ЗАТВЕРДЖУЮ**"
Декан факультету
математики і інформатики

Григорій ЖОЛТКЕВИЧ

"30" 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Вступ до криптографії

рівень вищої освіти **бакалавр**

галузь знань **11 – Математика та статистика**

спеціальність **111 - «Математика»**

освітня програма **«Математика»**

вид дисципліни **за вибором**

факультет **математики і інформатики**

2023/2024 навчальний рік

Програму рекомендовано до затвердження вченою радою факультету математики і інформатики

29 серпня 2023 року, протокол № 8

РОЗРОБНИК ПРОГРАМИ:

Каролінський Євген Олександрович, кандидат фізико-математичних наук, доцент кафедри фундаментальної математики, доцент.

Програму схвалено на засіданні кафедри фундаментальної математики
від 28 серпня 2023 року, протокол № 1.

В. о завідувача кафедри Сергій ГЕФТЕР

Програму погоджено з гарантом освітньої (професійної) програми «Математика».

Гарант освітньої (професійної) програми Олександр ЯМПОЛЬСЬКИЙ

Програму погоджено науково-методичною комісією факультету математики і інформатики
від 29 серпня 2023 року, протокол № 1.

Голова науково-методичної комісії Ольга АНОЩЕНКО

ВСТУП

Програма навчальної дисципліни **«Вступ до криптографії»** складена відповідно до освітньо-професійної програми підготовки **бакалавр**

спеціальності **111 - Математика**
освітня програма **«Математика»**

1. Опис навчальної дисципліни

1.1. Мета курсу полягає у навчанні майбутніх спеціалістів основам криптографії з відкритим ключем, а також необхідним відомостям з теорії чисел.

1.2. Основні завдання курсу є навчання студентів основам алгоритмічних аспектів арифметики і їх застосуванню в сучасній криптографії.

1.3. Кількість кредитів – **4**

1.4. Загальна кількість годин – **120**

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

1.6. Заплановані результати навчання:

Знати:

- ✓ Поняття про складність алгоритмів. Складність арифметичних дій.
- ✓ Алгоритм Евкліда і його складність.
- ✓ Прості числа. Факторіальність кільця цілих чисел.
- ✓ Порівняння і кільця лишків.
- ✓ Властивості скінченних полів.
- ✓ Квадратичний закон взаємності.
- ✓ Обчислення квадратного кореня в скінченному полі.
- ✓ Основи “класичної” криптографії.
- ✓ Криптографічну систему RSA.
- ✓ Тести Ферма, Соловея-Штрассена, Міллера-Рабіна.
- ✓ ρ-метод Полларда, метод факторних баз.

✓ Криптографічні системи Діффі-Хеллмана.

Уміти:
✓ Користуватися алгоритмом Евкліда, вести обчислення в кільцях лишків..
✓ Будувати скінченні поля і вести обчислення в них.
✓ Обчислювати символ Лежандра.
✓ Обчислювати квадратний корінь в скінченному полі.
✓ Перевіряти числа на простоту за допомогою тестів Соловея-Штрассена та Міллера-Рабіна.
✓ Користуватися ρ-методом Полларда та методом факторних баз.
✓ Користуватися криптографічною системою RSA.
✓ Користуватися криптографічною системою Діффі-Хеллмана.

2. Тематичний план навчальної дисципліни

Розділ 1. Відомості з теорії чисел.
1. Складність арифметичних дій.
2. Алгоритм Евкліда і його складність.
3. Прості числа. Факторіальність кільця цілих чисел.
4. Порівняння і кільця лишків.
5. Огляд теорії полів.
6. Скінченні поля.
7. Квадратичні лишки. Квадратичний закон взаємності.
8. Обчислення квадратного кореня в скінченному полі.

Розділ 2. Елементи криптографії.
1. “Класична” криптографія.
2. Криптографічна система RSA.
3. Перевірка чисел на простоту. Тести Ферма, Соловея-Штрассена, Міллера-Рабіна.
4. Розкладання чисел на множники: ρ-метод Полларда, метод факторних баз.
5. Дискретний логарифм. Криптографічні системи Діффі-Хеллмана.

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
Розділ 1. Відомості з теорії чисел.	59	16	16			27						
Розділ 2. Елементи криптографії.	59	16	16			27						
Контрольна робота	2					2						
Усього годин	**120**	**32**	**32**			**56**						

4. **Теми практичних занять**

№ з/п	Назва теми	Кількість годин
1	Відомості з теорії чисел.	16
2	Елементи криптографії.	16
	Разом	**32**

5. **Завдання для самостійної роботи**

№ з/п	Види, зміст самостійної роботи	Кількість годин
	Опрацювання додаткового матеріалу за відповідними темами:	
1	Відомості з теорії чисел.	27
2	Елементи криптографії.	27
3	Контрольна робота.	2
	Разом	**56**

6. **Індивідуальні завдання**

Не передбачені навчальним планом.

7. **Методи навчання**

Лекції та практичні заняття проводяться аудиторно. У разі оголошення карантину, заняття проводяться аудиторно або дистанційно (за допомогою платформ ZOOM, MOODLE) відповідно до наказу ректора Харківського національного університету імені В. Н. Каразіна.

8. **Методи контролю**

1) поточний семестровий: Контрольна робота (1)
2) підсумковий семестровий (залік).

9. Схема нарахування балів

Поточний контроль, самостійна робота, контрольна робота, індивідуальні завдання	Підсумковий семестровий контроль (залік)	Сума
60	40	100

Мінімальна кількість балів для допуску до складання підсумкового контролю програмою не передбачена.

Критерії оцінювання

Оцінка	Пояснення

в балах	за національною шкалою	
90–100	Відмінно	Теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
70–89	Добре	Теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками.
50–69	Задовільно	Теоретичний зміст курсу освоєний не повністю, але прогалини не носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань містять помилки, робота з трьома значними помилками.
1–49	Незадовільно	Теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка за національною шкалою	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90–100	відмінно	зараховано
70–89	добре	
50–69	задовільно	
1–49	незадовільно	не зараховано

10. Рекомендована література

Основна література

1. Koblitz N. A Course in Number Theory and Cryptography. Springer, 1994.

Допоміжна література

1. Galbraith S. D. Mathematics of Public Key Cryptography. Cambridge Univ. Press, 2012.

11. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

https://uk.wikipedia.org/wiki/%D0%90%D1%81%D0%B8%D0%BC%D0%B5%D1%82%D1%80%D0%

B8%D1%87%D0%BD%D1%96_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D0%B8_%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F