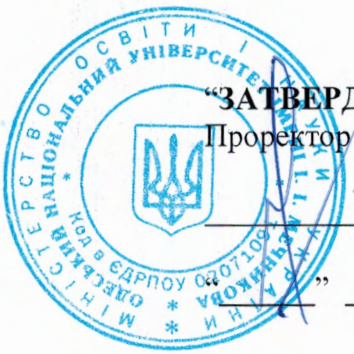
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І. МЕЧНИКОВА
Кафедра математичного забезпечення комп'ютерних систем



"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
_____
"___" _____ 20___ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК25 Криптографія
(назва навчальної дисципліни)

Рівень вищої освіти ***Перший (бакалаврський)***

Галузь знань: ***12 – Інформаційні технології***

Спеціальність ***123 – Комп'ютерна інженерія***
(код і назва спеціальностітей)

Освітньо-професійна програма ***Комп'ютерна інженерія***
(назва ОПП/ОНП)

ОНУ – 2024

Робоча програма навчальної дисципліни «Криптографія» – Одеса:ОНУ, 2024. – 12с.

Розробники: Шпінарева І.М., к.фіз.-м. наук, доцент кафедри МЗКС

Робоча програма затверджена на засіданні кафедри математичного забезпечення комп'ютерних систем

Протокол № 1 від. "28" 08 2024 р.

Завідувач кафедри _____ (Євгеній МАЛАХОВ)
(підпис) (Ім'я ПРІЗВИЩЕ)

Погоджено із гарантом ОПП/ОНП Комп'ютерна інженерія

_____ (Людмила ВОЛОЩУК)
(Ім'я ПРІЗВИЩЕ)

Схвалено навчально-методичною комісією (НМК) з ІТ спеціальностей факультету МФІТ

Протокол № 1 від. "30" 08 2024 р.

Голова НМК _____ (Лариса МАРТИНОВИЧ)
(підпис) (Ім'я ПРІЗВИЩЕ)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____" _____ 20__ р.

Завідувач кафедри _____ (_____)
(підпис) (Ім'я ПРІЗВИЩЕ)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____" _____ 20__ р.

Завідувач кафедри _____ (_____)
(підпис) (Ім'я ПРІЗВИЩЕ)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="16">Загальна кількість:
кредитів – 4

годин – 120

змістових модулів –3</td><td rowspan="16">Галузь знань
<u>12 – Інформаційні технології</u>
(шифр і назва)

Спеціальність
<u>123 – Комп’ютерна інженерія</u>
(шифр і назва)

Рівень вищої освіти:
<u>Перший (бакалаврський)</u></td><td colspan="2">Нормативна / за вибором (ВНЗ/студента)</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td>3-й</td><td>4-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>5-й</td><td>7-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>26 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>34 год.</td><td>6 год</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>60 год.</td><td>108 год.</td></tr>
<tr><td colspan="2">у т.ч. ІНДЗ*:</td></tr>
<tr><td colspan="2">Форма підсумкового контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

* – за наявності

2. Мета та завдання навчальної дисципліни

Метою курсу є оволодіння студентами базових знань в галузі теоретичної криптографії та криптоаналізу, в методах побудови важкооборотних функцій та їх застосувань для побудови асиметричних криптосистем, отримати базові поняття про різноманітні криптографічні протоколи.

Задачі дисципліни:

надати студентам знання в галузі криптографії, вміння розраховувати та застосовувати важкооборотні функції, володіти методами симетричного та асиметричного шифрування, побудови різноманітних криптографічних протоколів, вміння розробляти криптосистеми на еліптичних кривих.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей** (згідно ОПП «Комп'ютерна інженерія» від **2022** р.):

a) загальних:

Z1. Здатність до абстрактного мислення, аналізу і синтезу.

b) фахових:

P4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

Програмні результати навчання (ПРН):

N1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

N3. Знати новітні технології в галузі комп'ютерної інженерії.

N7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

N8. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.

Очікувані результати навчання. У результаті вивчення навчальної дисципліни студент повинен

знати*: основні поняття та методи практичної криптографії, різноманітні типи криптографічних схем та способи їх злому для організації передачі інформації.*

***вміти**: використовувати симетричні та асиметричні криптосистеми для передачі інформації; створювати криптографічні ключі та криптографічні протоколи та застосовувати у прикладних задачах*.

3. Зміст навчальної дисципліни

Змістовний модуль 1. Основні поняття криптографії

Тема 1. Вступ до криптографії. Проблема захисту інформації в сучасному суспільстві. Поняття про криптографію, криптоаналіз. Задачі криптографії.

Класична криптографічна схема. Принцип Керкхоффса. Теорія Шеннона секретного зв'язку. Ідея відкритого ключа. Задача управління ключами.

Тема 2. Історична криптографія. Шифри заміни. Шифр Цезаря. Квадрат Полібія. Частотний метод. Шифр чотирьох квадратів. Шифри перестановки. Шифр Сцитали. Шифри Кардано. Поліалфавітні шифри. Шифри Віженера. Шифр Вернама.

Тема 3. Симетричні криптосистеми. Поняття симетричної криптосистеми. Поточні шифри. Гамування. Блокові шифри. Лінійні та афінні шифри. Шифр Холла. Поняття про криптоаналіз блокових шифрів.

Змістовий модуль 2. Теоретичні основи асиметричної криптографії, основні алгоритми

Тема 4. Елементи теорії скінчених полів. Скінчені поля. Підполя скінченого поля. Мультиплікативна група скінченого поля. Побудування скінчених полів.

Тема 5. Складність арифметичних задач. Задача побудови великих простих чисел. Детерміновані та ймовірнісні тести на простоту. Задача факторизації. Алгоритми факторизації. Задача розпізнавання квадратичності. Алгоритм добування квадратного кореня за mod n. Обчислення значень функції Ейлера. Задача розпізнавання та побудови первісних коренів за mod p (p – просте непарне). Складність дискретного логарифмування. Алгоритми дискретного логарифмування.

Тема 6. Криптосистеми з відкритим ключем. Концепція криптосистем з відкритим ключем. Формальні складові асиметричних систем. Поняття про однобічну функцію. Алгоритм Меркле–Хеллмана. Алгоритм Шаміра. Система RSA. Система Рабіна. Криптосистема Ель-Гамаля. Атаки на схеми з відкритим ключем. Атака Вінера на RSA. Часткове розкриття ключа.

Тема 7. Криптопротоколи. Поняття криптографічного протоколу.Протокол обміну ключами Діффі-Хеллмана

Змістовий модуль 3. Криптосистеми на еліптичних кривих.

Тема 8. Еліптичні криві над скінченним полем.

Тема 9. Криптосистеми RSA, Ель-Гамаля на еліптичних кривих.

Тема 10. Криптопротоколи на еліптичних кривих.

4. Структура навчальної дисципліни

Назви тем	Кількість годин									
	Денна форма					Заочна форма				
	Усього	у тому числі				Усього	у тому числі			
		л	п/с	лаб	ср		л	п/с	лаб	ср
1	2	3	4	5	6	7	8	9	10	11
Змістовий модуль 1. Основні поняття криптографії										
Тема 1.	5	1	2		2	10				10
Тема 2.	8	2	2		4	10				10
Тема 3.	9	3	2		4	14	2	2		10
Разом за змістовим модулем 1	**22**	**6**	**6**		**10**	**34**	**2**	**2**		**30**
Змістовий модуль 2. Теоретичні основи асиметричної криптографії, основні алгоритми										
Тема 1.	18	4	4		10	10				10
Тема 2.	16	2	4		10	14	1	1		12
Тема 3.	18	4	4		10	16	2	2		12
Тема 4.	16	2	4		10	12				12
Разом за змістовим модулем 2	**68**	**12**	**16**		**40**	**52**	**3**	**3**		**46**
Змістовий модуль 3. Криптосистеми на еліптичних кривих.										
Тема 1.	14	4	6		4	12	1	1		10
Тема 2.	10	4	4		4	12				12
Тема 3.	6	2	2		2	10				10
Разом за змістовим модулем 3	**30**	**8**	**12**		**10**	**34**	**1**	**1**		**32**
Усього годин	**120**	**26**	**34**		**60**	**120**	**6**	**6**		**108**

* – за наявності

Форма контролю: **КО** –контрольне опитування (поточне)
ІЗ –індивідуальне завдання
КР – контрольна робота

5. Теми семінарських занять

Семінарські заняття не передбачені.

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Вступ до криптографії. Шифри заміни. Шифр Цезаря. Квадрат Полібія. Частотний метод. Шифр чотирьох квадратів.	2	2
2	Шифри перестановки. Шифр Сцитали. Шифри Кардано. Поліалфавітні шифри. Шифри Віженера. Шифр Вернама.	2	
3	Симетричні криптосистеми. Лінійні та афінні шифри. Шифр Холла. Шифр DES.	2	
4	Задача побудови великих простих чисел. Детерміновані та ймовірнісні тести на простоту.	4	3
5	Криптосистеми з відкритим ключем. Алгоритм Меркле–Хеллмана. Алгоритм Шаміра. Система RSA. Система Рабіна. Криптосистема Ель-Гамаля. Атаки на схеми з відкритим ключем.	10	
6	Протокол обміну ключами Діффі-Хеллмана	2	
7	Еліптичні криві над скінченим полем. Криптосистеми RSA, Ель-Гамаля на еліптичних кривих. Криптопротоколи на еліптичних кривих.	12	1
	Разом	**34**	**6**

7. Теми лабораторних занять

Лабораторні заняття не передбачені

8. Самостійна робота

№ з/п	Назва теми / види завдань	Кількість годин	
		Денна форма	Заочна форма
1	Вступ до криптографії . Проблема захисту інформації в сучасному суспільстві. Принцип Керкхоффса. Теорія Шеннона секретного зв’язку. Задача управління ключами. Підготувати доповідь [1].	3	15
2	Шифри заміни. Шифр Цезаря. Квадрат Полібія. Частотний метод. Шифр чотирьох квадратів. Шифри перестановки. Шифр Сцитали. Шифри	3	15

	Кардано. Поліалфавітні шифри. Шифри Віженера. Шифр Вернама [1].		
3	Симетричні криптосистеми. Поточні шифри. Гамування. Блокові шифри. Лінійні та афінні шифри. Шифр Холла. Поняття про криптоаналіз блокових шифрів [1].	4	15
4	Концепція криптосистем з відкритим ключем. Формальні складові асиметричних систем. Система RSA. Система Рабіна. Криптосистема Ель-Гамаля. Атаки на схеми з відкритим ключем. Атака Вінера на RSA. Часткове розкриття ключа [1].	20	18
5	Протокол експоненційного обміну ключами Діффі-Хеллмана. [1]	6	15
6	Складність арифметичних задач. Алгоритми факторизації. Задача розпізнавання квадратичності. Обчислення значень функції Ейлера. Задача розпізнавання та побудування первісних коренів за mod p (p – просте непарне). Алгоритми дискретного логарифмування [1].	14	15
7	Криптографія на еліптичних кривих. [1].	10	15
	Разом	**60**	**108**

До самостійної роботи відноситься:

[1] – підготовка до лекцій, практичних занять.

9. Методи навчання

Лекції з використанням мультимедійного презентаційного матеріалу.

Пояснювально-ілюстративні методи: лекція, пояснення, самостійне опрацювання літературних джерел, робота з електронними конспектами лекцій та презентаціями, опрацювання наукових публікацій.

Наочні методи: презентації, ілюстрації.

Практичні методи: вправи, тренувальні вправи, творчі вправи, розв’язання розрахункових задач за алгоритмами конкретних методів, практичні роботи.

Методи формування і стимулювання пізнавальної діяльності: навчальні дискусії

10. Методи контролю

Під час **підсумкового контролю** студент повинен відповісти на 2 запитання екзаменатора з переліку, наведеному у п. 11.

Критерії оцінювання на підсумковому модульному контролі:

1. Відповідь повинна бути повною і короткою. Вона не повинна мати в собі матеріал, що не відноситься до сутті питання.

2. Чітко формулювати твердження, вправно застосовувати необхідні формули і знання основних питань програми.
3. Відповіді, що мають помилкові твердження оцінюються виходячи з близькості відповіді до правильної.
4. Пропуски в обґрунтуванні тверджень враховуються і це призводить до зменшення кількості балів.
5. Малі недоліки, неточності при викладенні матеріалу, зменшують кількість балів.
6. Незнання і нерозуміння основної ідеї теоретичного питання або задачі призводить до зняття до 90 % балів.
7. Якщо відповідь на питання відсутня то виставляється нуль балів.

11. Питання для підсумкового контролю

1. Поняття про криптографію і криптоаналіз.
2. Стеганографія і кодування.
3. Три завдання криптографії. Структурні складові криптографії.
4. Основні криптографічні терміни.
5. Класична криптографічна схема.
6. Принцип Керкхоффса.
7. Теорія Шенона секретного зв'язку.
8. Шифри заміни. Шифри Цезаря.
9. Квадрат Полибія. Частотний метод.
10. Шифри перестановки.
11. Шифр Сцитали. Шифри Кардано.
12. Поліалфавитні шифри.
13. Шифр Виженера. Шифр Вернама.
14. Поняття симетричної криптосистеми.
15. Поточні шифри. Гамування. Блокові шифри.
16. Лінійні та афінні шифри. Шифр Холла.
17. Поняття про криптоаналіз блокових шифрів.
18. Питання криптоаналізу. Схема Фейстеля.
19. Концепція криптосистем з відкритим ключем.
20. Формальні складові асиметричних систем.
21. Поняття про однобічну функцію.
22. Опис системи RSA: коректність, ефективність, стійкість.
23. Система Рабина: коректність, ефективність, стійкість.
24. Загальне опис алгоритму DES. Порівняння з ГОСТ 28147-89.
25. Ймовірнісна криптосистема на основі RSA-функції.
26. Ймовірнісна система на основі квадратичності.
27. Криптосистема Ель-Гамаля: коректність, ефективність, стійкість.
28. Атаки на схеми з відкритим ключем.
29. Атака Вінера на RSA.
30. Часткове розкриття ключа.

31. Поняття криптографічного протоколу.
32. Протокол обміну ключами Діффі-Хеллмана.
33. Задача побудови великих простих чисел. Тести на простоту.
34. Псевдопрості числа. Оцінки для числа основ для псевдопростих Ойлера і сильно псевдопростих.
35.Тести Соловея-Штрассена і Міллера-Рабина як імовірнісні алгоритми з однобічною помилкою.
36.Метод побудови великого простого на основі модифікованої малої теореми Ферма.
37. Задача факторизації. Алгоритм Полларда.
38. Задача розпізнавання квадратичності.
39. Добування квадратного кореня по модулю простого числа.
40. Добування квадратного кореня по модулю складового числа.
41.Обчислення значень функції Ейлера.
42.Задача розпізнавання і побудови первісних коренів по простому модулю.
43. Складність дискретного логарифмування.
44.Еліптичні криві над скінченим полем.
45.Криптосистеми RSA, Ель-Гамаля на еліптичних кривих.
46. Криптопротоколи на еліптичних кривих.

Розподіл балів, які отримують студенти

Поточний та періодичний контроль									Сума балів
Змістовий модуль №1			Змістовий модуль № 2			Змістовий модуль №3			
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	
10	10	10	20	10	10	10	10	10	100

Т1, Т2 ... – теми змістових модулів,

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
85-89	B	добре	
75-84	C		
70-74	D	задовільно	
60-69	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

12. Навчально-методичне забезпечення

Конспект лекцій у електронному форматі; методичні вказівки для виконання лабораторних робіт; нормативні документи; презентаційні матеріали.

13. Рекомендована література

Основна

1. Вербіцький О.В. Вступ до криптології Львів: Науково-технічна література, 1998. 248с.
2. Гринченко О.М., Мамчур Є.В. Концептуальні засади захисту інформації в умовах економіки. К.: НУХТ, 2016. 282 с.
3. Гуржій О.В., Красножон Д. В. Криптографія і захист інформації в електронній комерції. К.: Вид-во НПУ ім. М.П. Драгоманова, 2015. 180 с.
4. Задірака В.К., Олексюк О.С.Недашковський М.О. Методи захисту фінансової інформації: навчальний посібник. К.: Вища школа, 2000. 460с.
5. Клесов О.І. Елементарна теорія чисел та елементи криптографії, Київ: ТВіМС, 2017. 394 с.
6. Мазур О.І. Криптографічні алгоритми та протоколи захисту електронних коштів. К.: НАУ, 2015. 188 с.
7. Химич В.І. Криптографічні аспекти безпеки інформаційно-комунікаційних систем. К.: ВПЦ "Київський університет", 2012. 448 с.
8. Шеремета Ю.І. Електронні гроші: криптографічний захист та технології. К.: ТОВ "Техніка", 2004. 256 с.

Допоміжна

1. Buchmann J. A. Introduction to cryptography, second edition. Springer Verlag, New York, 2004. 386c.
2. Koshy T. Elementary Number Theory with Applications. 2nd edition, Elsevier, Amsterdam, 2007. 812c.
3. Rivest, R.L.; Shamir, A.; Adleman, L.M. A Method for Obtaining Digital Signatures and Public Key Cryptosystems; Routledge: London, UK, 2019. 15c.
4. Rosen K. H. Elementary Number Theory. 6th edition, Addison Wesley, Boston MA, 2011. 616 с.

14. Електронні інформаційні ресурси

1.https://onu.edu.ua/uk/science/scientific-library – Сайт бібліотеки ОНУ імені І. І. Мечникова;

2.http://nbuv.gov.ua/ – Сайт Національної бібліотеки України імені В. І. Вернадського;

3.http://www.dnpb.gov.ua/ – Сайт Державної науково-педагогічної бібліотеки України імені В.О. Сухомлинського;
4.http://odnb.odessa.ua/ – Сайт Одеської національної наукової бібліотеки.
5.https://scholar.google.com/ - Google Scholar, пошукова система, яка індексує повний текст наукових публікацій всіх форматів і дисциплін.
6.https://indexcopernicus.com/ - Index Copernicus (IC) – онлайнова наукометрична база даних
7.https://www.scopus.com/home.uri – Scopus, бібліографічна і реферативна база даних
8.https://clarivate.com/products/web-of-science/ – Web of Science, бази наукової літератури і патентів
9.https://doi.org/10.3390/cryptography6030032 – Longo R., Mascia C., Meneghetti A., Santilli G. Adaptable Cryptographic Primitives in Blockchains via Smart Contracts. Cryptography, 2022, 6, 32.
10. https://www.rfc-editor.org/rfc/rfc5639.html – Lochter M., Merkle J. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Technical Report, RFC 5639, March 2010. Available online: (accessed on 20 August 2022). 11.https://doi.org/10.3390/cryptography6030041/ – Nişancı G., Flikkema P. G. , Yalçın T. Symmetric Cryptography on RISC-V: Performance Evaluation of Standardized Algorithms. Cryptography. 2022, 6(3), 41.