МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І. І. МЕЧНИКОВА
Кафедра комп'ютерної алгебри та дискретної математики

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
Олександр ЗАПОРОЖЧЕНКО
12 вересня 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВБ «Економічна криптографія»

Рівень вищої освіти	**другий (магістерський)**
Галузь знань	**11 Математика та статистика**
Спеціальність	**113 Прикладна математика**
Освітньо-професійна програма	**Прикладна математика**

ОНУ
2022

Робоча програма навчальної дисципліни «Економічна криптографія». – Одеса: ОНУ, 2022.

Розробник:
Савастру Ольга Володимирівна, кандидат фізико-математичних наук, доцент, доцент кафедри комп'ютерної алгебри та дискретної математики

Робоча програма затверджена на засіданні кафедри комп'ютерної алгебри та дискретної математики

Протокол № 1 від "26" серпня 2022 р.

Завідувач кафедри _____ Павло ВАРБАНЕЦЬ

Погоджено із гарантом ОПП "Прикладна математика" (Ольга Кічмаренко)

Схвалено навчально-методичною комісією (НМК) з математики факультету математики, фізики та інформаційних технологій

Протокол № 1 від "9" вересня 2022 р.

Голова НМК _____ Євген СТРАХОВ

Переглянуто та затверджено на засіданні кафедри комп'ютерної алгебри та дискретної математики

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____

Переглянуто та затверджено на засіданні кафедри комп'ютерної алгебри та дискретної математики

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, спеціалізація, рівень вищої освіти	Характеристика навчальної дисципліни
		очна (денна, вечірня) форма навчання
Загальна кількість: кредитів –4	Галузь знань **11 Математика та статистика**	Дисципліна вільного вибору
		Рік підготовки:
годин –120		1-й
		Семестр
змістових модулів –3	Спеціальність **113 Прикладна математика**	2-й
		Лекції
		20 год.
		Практичні, семінарські
	Рівень вищої освіти: **другий (магістерський)**	20 год.
		Лабораторні
		год.
		Самостійна робота
		80 год.
		Форма підсумкового контролю: залік

2. Мета та завдання навчальної дисципліни

Мета дисципліни: 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.

Завдання дисципліни: надати студентам знання в галузі криптографії, вміння розраховувати та застосовувати важкооборотні функції, володіти методами побудови різноманітних криптографічних протоколів, зокрема, протоколів аутентифікації, цифрового підпису, криптографічних протоколів у електронній комерції, в тому числі у блокчейн-технологіях, вміння розробляти криптосистеми на еліптичних кривих.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей**:

Інтегральна компетентність :

Здатність розв'язувати складні задачі і проблеми прикладної математики у професійної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

а) загальних (ЗК):

ЗК.01 Здатність генерувати нові ідеї (креативність) й нестандартні підходи до їх реалізації.

ЗК.03. Здатність ставити та вирішувати задачі на основі абстрактного мислення, аналізу й синтезу.

б) спеціальних/фахових (СК/ФК):

ФК.02. Здатність розробляти методи побудови й дослідження моделей складних систем у різних галузях людської діяльності, будувати математичні моделі природних та соціальних явищ та чисельно їх розраховувати.

ФК.04. Здатність до розвитку нових та удосконалення існуючих математичних методів аналізу, моделювання, прогнозування, розв'язування нових проблем у нових галузях знань.

ФК.07. Знання на рівні новітніх досягнень, необхідні для практичної та/або інноваційної діяльності у сфері прикладної математики.

У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

знати: основні поняття, результати, методи сучасної практичної криптографії, мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у предметі навчальної дисципліни

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

Вміти критично осмислювати проблеми у галузі прикладної математики та на межі з іншими галузями знань. Бути здатним до проведення досліджень з метою розвитку нових знань та процедур, бути здатним інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах, бути здатним розв'язувати проблеми у

нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності, бути здатним продовжувати навчання з високим ступенем автономії.

Що забезпечує наступні програмні результати навчання (ПРН):

ПРН 01. Знати та вміти застосовувати процедури формального опису та моделювання поведінки реальних природних, технічних, соціально-економічних систем, впливів некерованих чинників, потрібних для прийняття раціональних рішень.

ПРН 06. Вміти застосовувати математичний апарат при вирішенні актуальних задач на практиці

ПРН 07. Вміти будувати моделі складних систем, обирати методи їх дослідження, реалізовувати побудовані моделі програмно та перевіряти їх адекватність за допомогою комп'ютера .

ПРН 09. Виявляти здатність до самонавчання та продовження професійного розвитку.

3. Зміст навчальної дисципліни

Змістовий 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. Криптосистеми з відкритим ключем. Концепція криптосистем з відкритим ключем. Формальні складові асиметричних систем. Поняття про однобічну функцію. Система RSA. Система Рабина. Ймовірнісна схема систем з відкритим ключем Гольдвассера і Мікели. Криптосистема ЕльГамала. Атаки на схеми з відкритим ключем. Атака Вінера на RSA. Часткове розкриття ключа.

Тема 5. Хеш-функції. Криптографічні властивості. Загальні схеми побудови та характеристики хеш-функцій, найбільш уживаних у системах захисту інформації

Тема 6. Цифровий підпис. Поняття криптографічного протоколу. Протокол експоненційного обміну ключами Діффі-Хеллмана. Застосунки. Задачі цифрового підпису. Загальна схема. Цифровий підпис у схемі RSA з використанням хеш-функцій. Цифрові підписи Эль-Гамаля, Шнорра, Рабіна. Сліпий підпис.

Змістовий модуль 3. Криптопротоколи, криптосистеми на еліптичних кривих

Тема 7. Сучасні криптопротоколи
Протоколи розподілу секретів. Протоколи доведення без розголошення. Імовірнісне шифрування. Схеми пред'явлення випадкових бітів. Багаторівнева криптографія. Протоколи електронної готівки. Ідентифікація та аутентифікація. Електронні вибори на базі RSA. Електронні гроші на базі RSA. Дерево Меркле. Консенсуси.
Тема 8. Складність арифметичних задач. Задача побудування 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 побудування первісних коренів за mod *p* (*p* – просте непарне). Складність дискретного логарифмування. Алгоритми дискретного логарифмування("Крок велетня, крок ліліпута" і Силвера-Поліга-Хеллмана дискретного логарифмування.).
Тема 9. Криптографія на еліптичних кривих. Еліптичні криві над скінченим полем. Криптосистеми RSA, ЕльГамаля і Рабіна на еліптичних кривих. Криптопротоколи на еліптичних кривих. Алгоритм ЦП на основі теорії еліптичних кривих.

4. Структура навчальної дисципліни

Назви тем	Кількість годин				
	Очна (денна, вечірня) форма				
	Усього	у тому числі			
		л	п/с	лаб	ср
1	2	3	4	5	6
Змістовий модуль 1. Основні поняття криптографії					
Тема 1. Вступ до криптографії	14	2	2		10
Тема 2. Історична криптографія	14	2	2		10
Тема 3. Симетричні криптосистеми	14	2	2		10
Разом за змістовим модулем 1	42	6	6		30
Змістовий модуль 2. Теоретичні основи асиметричної криптографії, основні алгоритми					
Тема 4. Криптосистеми з відкритим ключем	18	4	4		10
Тема 5. Хеш-функції	14	2	2		10
Тема 6. Цифровий підпис	14	2	2		10
Разом за змістовим модулем 2	46	8	8		30
Змістовий модуль 3. Криптопротоколи, криптосистеми на еліптичних кривих					
Тема 7. Сучасні криптопротоколи	14	2	2		10

Тема 8. Складність арифметичних задач	8	2	2		4
Тема 9. Криптографія на еліптичних кривих	10	2	2		6
Разом за змістовим модулем 3	32	6	6		20
Усього годин	**120**	**20**	**20**		**80**

5. Теми семінарських занять

Семінарські заняття не передбачені.

6. Теми практичних занять

№ з/п	Назва теми/види завдань	Кількість годин
1	Вступ до криптографії. Шифри заміни. Шифр Цезаря. Квадрат Полібія. Частотний метод. Шифр чотирьох квадратів.	2
2	Шифри перестановки. Шифр Сцитали. Шифри Кардано. Поліалфавітні шифри. Шифри Віженера. Шифр Вернама.	2
3	Симетричні криптосистеми. Лінійні та афінні шифри. Шифр Холла.	2
4	Криптосистеми з відкритим ключем. Система RSA. Система Рабина. Ймовірнісна схема систем з відкритим ключем Гольдвассера і Мікели. Криптосистема ЕльГамала.	4
5	Хеш-функції. Загальні схеми побудови	2
6	Цифровий підпис. Протокол Діффі-Хеллмана. Цифровий підпис у схемі RSA з використанням хеш-функцій. Цифрові підписи Эль-Гамаля, Шнорра, Рабіна.	2
7	Криптопротоколи. Протоколи розподілу секретів. Протоколи доведення без розголошення. Протоколи електронної готівки. Ідентифікація та аутентифікація. Електронні вибори на базі RSA. Електронні гроші на базі RSA. Дерево Меркле. Консенсуси.	2
8	Детерміновані та ймовірнісні тести на простоту. Алгоритми факторизації. Задача розпізнавання квадратичності. Обчислення значень функції Ейлера. Задача розпізнавання та побудування первісних коренів за mod p (p – просте непарне). Алгоритми дискретного логарифмування("Крок велетня, крок ліліпута" і Силвера-Поліга-Хеллмана дискретного логарифмування.).	2
9	Криптосистеми RSA, ЕльГамаля і Рабіна на еліптичних кривих.	2
	Разом	20

В основу кожного практичного заняття покладені типові завдання, навчання розв'язанню яких є основою змістовного освоєння матеріалу курсу.

7. Теми лабораторних занять

Лабораторні заняття не передбачені.

8. Самостійна робота

№ з/п	Назва теми/види завдань	Кількість годин
1	Вступ до криптографії . Проблема захисту інформації в сучасному суспільстві. Принцип Керкхоффса. Теорія Шеннона секретного зв'язку. Задача управління ключами. Підготувати доповідь.	10
2	Шифри заміни. Шифр Цезаря. Квадрат Полібія. Частотний метод. Шифр чотирьох квадратів. Шифри перестановки. Шифр Сцитали. Шифри Кардано. Поліалфавітні шифри. Шифри Віженера. Шифр Вернама.	10
3	Симетричні криптосистеми. Поточні шифри. Гамування. Блокові шифри. Лінійні та афінні шифри. Шифр Холла. Поняття про криптоаналіз блокових шифрів.	10
4	Концепція криптосистем з відкритим ключем. Формальні складові асиметричних систем. Система RSA. Система Рабина. Криптосистема ЕльГамала. Атаки на схеми з відкритим ключем. Атака Вінера на RSA. Часткове розкриття ключа.	10
5	Хеш-функції.	10
6	Цифровий підпис. Поняття криптографічного протоколу. Протокол експоненційного обміну ключами Діффі-Хеллмана. Задачі цифрового підпису. Загальна схема. Цифровий підпис у схемі RSA з використанням хеш-функцій. Цифрові підписи Эль-Гамаля, Шнорра, Рабіна. Сліпий підпис.	10
7	Криптопротоколи. Протоколи розподілу секретів. Протоколи доведення без розголошення. Імовірнісне шифрування. Протоколи електронної готівки. Ідентифікація та аутентифікація. Електронні вибори на базі RSA. Електронні гроші на базі RSA. Дерево Меркле. Консенсуси. Підготувати доповідь.	10
8	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	4
9	Криптографія на еліптичних кривих.	6
	Разом	80

До самостійної роботи відноситься підготовка до лекцій, практичних занять.

Перевірка самостійної роботи здійснюється:
1. під час лекційних занять (короткими опитуваннями підготовленості студентів);
2. під час практичних занять;
4. перевірка викладачем індивідуальних завдань.

9. Методи навчання

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. Форми контролю і методи оцінювання

Усне опитування, контрольні письмові роботи, оцінювання виконання розв'язання розрахункових задач, захист результатів практичних робіт, тестування (бланкове або комп'ютерне), оцінювання виконання практичних навичок.
Примітка: максимальна кількість балів за кожною темою вказана в п.12.
Форма підсумкового контролю – залік. Підсумкова оцінка визначається як сума балів за результатами всіх видів контролю (згідно зі шкалою оцінювання з п. 12).

Критерії оцінювання навчальних досягнень здобувачів вищої освіти:

Оцінка за національною шкалою та **відсоток від максимальної кількості балів**	Теоретична підготовка	Практична підготовка
	Здобувач освіти	
зараховано (90-100% від максимальної кількості балів)	у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає під час усних виступів та письмових відповідей; глибоко та всебічно розкриває зміст теоретичних питань, використовуючи при цьому нормативну, обов'язкову та додаткову літературу; робить самостійні висновки, виявляє причинно-наслідкові зв'язки; самостійно знаходить додаткову інформацію та використовує її для реалізації поставлених перед ним завдань. Здобувач здатен виділяти суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно-наслідкові зв'язки, формувати висновки і узагальнення, вільно оперувати фактами та відомостями.	глибоко та всебічно розкриває сутність практичних/ розрахункових завдань, використовуючи при цьому нормативну, обов'язкову та додаткову літературу; може аргументовано обрати раціональний спосіб виконання завдання й оцінити результати власної практичної діяльності; виконує творчі завдання та ініціює нові шляхи їх виконання; вільно використовує набуті теоретичні знання при аналізі практичного матеріалу; проявляє творчий підхід до виконання індивідуальних та колективних завдань при самостійній роботі.
зараховано (75-89% від максимальної кількості балів)	достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, використовуючи при цьому нормативну та обов'язкову літературу; при представленні деяких питань не вистачає достатньої глибини та аргументації, застосовує знання для розв'язання стандартних ситуацій; самостійно аналізує, узагальнює і систематизує навчальну інформацію, але допускаються при цьому окремі несуттєві неточності та незначні помилки.	правильно вирішив більшість розрахункових /тестових завдань за зразком; має стійкі навички виконання завдання
зараховано (60-74% від	володіє навчальним матеріалом на репродуктивному рівні або відтворює певну частину навчального	може використовувати знання в стандартних ситуаціях, має

максимальної кількості балів)	матеріалу з елементами логічних зв’язків, знає основні поняття навчального матеріалу; має ускладнення під час виділення суттєвих ознак вивченого; під час виявлення причинно-наслідкових зв’язків і формулювання висновків.	елементарні, нестійкі навички виконання завдання. Правильно вирішив половину розрахункових/тестових завдань. Здобувач має ускладнення під час виділення суттєвих ознак вивченого; під час виявлення причинно-наслідкових зв’язків і формулювання висновків.
незараховано (35-59% від максимальної кількості балів)	володіє навчальним матеріалом поверхово й фрагментарно (без аргументації та обґрунтування); безсистемно виокремлює випадкові ознаки вивченого; не вміє робити найпростіші операції аналізу і синтезу; робити узагальнення, висновки; під час відповіді допускаються суттєві помилки	недостатньо розкриває сутність практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив окремі розрахункові/тестові завдання за допомогою викладача, відсутні сформовані уміння та навички.
незараховано (0-34% від максимальної кількості балів)	не володіє навчальним матеріалом	виконує лише елементи завдання, потребує постійної допомоги викладача

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. Ймовірнісна схема систем з відкритим ключем Гольдвассера і Мікели.
25. Ймовірнісна криптосистема на основі RSA-функції.

26. Ймовірнісна система на основі квадратичності.
27. Криптосистема ЕльГамаля: 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 експоненційного обміну ключами Діффі-Хеллмана.
33. Поняття про хеш-функції.
34. Протоколи цифрового підпису. Його загальна схема, види нападів.
35. Протокол цифрового підпису Шнорра.
36. Протоколи розподілу секретів.
37. Протоколи доведення без розголошення.
38. Імовірнісне шифрування.
39. Схеми пред'явлення випадкових бітів.
40. Багаторівнева криптографія.
41. Протоколи електронної готівки.
42. Ідентифікація та аутентифікація.
43. Електронні вибори на базі RSA.
44. Електронні гроші на базі RSA.
45. Дерево Меркле.
46. Консенсуси.
47. Задача побудови великих простих чисел. Тести на простоту.
48. Псевдопрості числа. Оцінки для числа основ для псевдопростих Ойлера і сильно псевдопростих.
49. Тести Соловея-Штрассена і Міллера-Рабина як імовірнісні алгоритми з однобічною помилкою.
50. Метод побудови великого простого на основі модифікованої малої теореми Ферма.
51. Задача факторизації. Алгоритм Полларда.
52. Задача розпізнавання квадратичності.
53. Добування квадратного кореня по модулю простого числа.
54. Добування квадратного кореня по модулю складового числа.
55. Обчислення значень функції Ойлера.
56. Задача розпізнавання і побудови первісних коренів по простому модулю.
57. Складність дискретного логарифмування.
58. Алгоритм Сільвера-Поліга-Хеллмана.
59. Алгоритм "Великих і малих кроків".
60. Еліптичні криві над скінченим полем.
61. Криптосистеми RSA, ЕльГамала і Рабіна на еліптичних кривих.
62. Криптопротоколи на еліптичних кривих.
63. Алгоритм ЦП на основі теорії еліптичних кривих.

12. Розподіл балів, які отримують здобувачі

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

Розподіл балів за видами навчальної роботи

Види навчальної роботи	**Змістовий модуль 1**			**Змістовий модуль 2**			**Змістовий модуль 3**		
	Кіль-кість балів за 1 заняття (завдання)	Кіль-кість занять (зав-дань)	**Сумар-на кіль-кість балів (max)**	Кіль-кість балів за 1 заняття (завдання)	Кіль-кість занять (зав-дань)	**Сумар-на кіль-кість балів (max)**	Кіль-кість балів за 1 заняття (завдання)	Кіль-кість занять (завдань)	**Сумар-на кіль-кість балів (max)**
Поточний контроль на лекціях	2	3	**6**	2	4	**8**	2	3	**6**
Практичні заняття	8	3	**24**	8	4	**32**	8	3	**14**
Разом			**30**			**40**			**30**
Залік									
Підсумкова сума балів	**100**								

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

13. Навчально-методичне забезпечення

1. Робоча програма, силабус, конспект лекцій, мультимедійні презентації, плани практичних занять.

14. 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.

Додаткова

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

15. 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.