МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Проректор з наукової роботи

_____ Микола ДИВАК
«_____»_____2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Оцінка складності алгоритмів шифрування»

Ступінь вищої освіти (освітньо – кваліфікаційний рівень) – **доктор філософії**

Галузь знань – **12 Інформаційні технології**

Спеціальність – **125 Кібербезпека та захист інформації**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	СРС (год.)	Разом (год.)	Екз. (сем.)
Денна	1	2	20	20	80	150	2

Тернопіль – ЗУНУ
2024

Робоча програма складена на основі освітньо-наукової програми підготовки доктора філософії, галузь знань 12 - «Інформаційні технології», спеціальності: 125 “Кібербезпека та захист інформації ” затвердженої Вченою радою ЗУНУ (протокол № 11від 26 червня 2024 р.)

Робочу програму склав к.т.н., доцент, декан факультету комп’ютерних інформаційних технологій Якименко Ігор Зіновійович

Розглянуто та схвалено групою забезпечення спеціальності
протокол № 1 від 30 серпня 2024 р.

Голова ГЗС _____ Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Оцінка складності алгоритмів шифрування»

Опис дисципліни «Оцінка складності алгоритмів шифрування»

Дисципліна «Оцінка складності алгоритмів шифрування»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 4	Галузь знань: 12 - Інформаційні технології	Обов'язкова
Кількість залікових модулів	Спеціальності – 125 "Кібербезпека та захист інформації"	Рік підготовки: *Денна – 1* Семестр: *Денна – 2*
Кількість змістових модулів – 2	Ступінь вищої освіти – доктор філософії	Лекції: *Денна – 20* Практичні заняття: *Денна – 20*
Загальна кількість годин – 120		Самостійна робота: *Денна – 80*
Тижневих годин: з них аудиторних: 4		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Оцінка складності алгоритмів шифрування»

2.1. Мета вивчення дисципліни.

Метою дисципліни «Оцінка складності алгоритмів шифрування» є отримання знань та умінь, які необхідні для оцінки складності алгоритмів шифрування.

2.2. Завдання вивчення дисципліни:

Завдання дисципліни **«Оцінка складності алгоритмів шифрування»** дати студентам теоретичну та практичну підготовку з методів оцінки складності алгоритмів шифрування.

2.3 Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

СК-3. Здатність ефективно застосовувати методи аналізу, математичне моделювання, виконувати натурні та математичні експерименти при проведенні наукових досліджень.

СК-4. Здатність інтегрувати знання з різних дисциплін, застосовувати системний підхід та враховувати нетехнічні аспекти при розв'язанні інженерних задач та проведенні досліджень.

СК-6. Уміння відслідковувати тенденції й напрямки розвитку інформаційної та кібербезпеки, а також суміжних і прикладних областей.

2.4. Результати навчання

В результаті вивчення дисципліни аспірант повинен:

ПРН-3. Уміти вести дискусії і полеміки, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.

ПРН-6. Вміти розв'язувати задачі синтезу та аналізу об'єктів професійної діяльності кібербезпеки.

ПРН-13. Вміти обґрунтовувати вибір методів розв'язання науково-прикладних задач та критично оцінювати отримані результати, аргументовано захищаючи прийняті рішення.

3. Зміст дисципліни «Оцінка складності алгоритмів шифрування»

Змістовий модуль 1. Основи теорії чисел та математичних основ захисту інформації.

Тема 1. Предмет математичних основ захисту інформації. Етапи розвитку методів захисту інформації. Основні поняття криптології. Основні види криптографічних атак. Приклади. Вступ до області математичних основ

захисту інформації. Історія розвитку криптографічних методів, їх класифікація та основні етапи розвитку.

Література: основна [1, 2].

Тема 2. Машинні моделі. Детерміновані, недетерміновані та три стрічкові машини Тюрінга. Поняття складності обчислення в часі і пам'яті. Основні математичні поняття: відношення, відношення порядку та функціональні відношення. Властивості функціональних відношень та їх класифікація: ін'єкції, сюр'єкії, бієкції. Порядок росту функцій та методи їх знаходження.

Література: основна [4,5].

Тема 3. Класи складності P і NP. Поняття односторонньої функції та його роль в криптографії. Приклади побудови односторонніх функцій. Розглядається теорія складності за Тюрінгом. Описуються класи складності P і NP. Формулюється необхідна умова стійкості криптографічної системи.

Література: основна [1, 3, 4,11].

Тема 4. Основні поняття теорії ймовірностей. Випадкові величини та їх властивості. Рівномірний, біноміальний та інші розподіли. Поняття стійкості криптосистеми. Теорема Шеннона. - 2год. Наводяться основні поняття теорії ймовірностей: поняття випадкової величини, її ймовірності, основні дискретні розподіли та умовна ймовірність. Ілюстрація понять на прикладах.

Література: основна [1, 3, 4].

Тема 5. Основні поняття теорії груп. Розклад групи за підгрупою. Нормальний дільник групи. Теорема Лагранжа та її наслідки .

Література: основна [1, 3, 4].

Змістовий модуль 2. Основні області застосування симетричних та асиметричних криптосистем. Проблеми обміну ключами та основні методи генерації та обміну ключами. Принципи побудови асиметричних криптосистем. Приклади асиметричних шифрів.

Тема 6. Кільця та їх властивості. Ідеали кільця та його властивості. Поняття дискретного логарифму та алгоритм його обчислення. Поле, характеристика поля та побудова скінченних полів. -2 год. Кільця та їх основні властивості. Кільце лишків цілих чисел та його властивості. Дільники нуля, дільники одиниці, ідеали кільця. Основні твердження про породжуючи елементи скінченного кільця.

Література: основна [1, 2, 4, 5, 7, 8, 9].

Тема 7. Елементи теорії чисел. Відношення подільності та його властивості. НСД і НСК, примітивна рекурсивність цих функцій. Алгоритм Евкліда знаходження НСД та його варіації. Факторизація. Означення відношення подільності та його властивості. Основна теорема арифметики та наслідки з неї. Проблема факторизації та її зв'язок з проблемою тестування чисел на простоту. Приклади використання.

Література: основна [1, 4, 6, 7].

Змістовий модуль 3. Хеш-функції та цифровий підпис

Тема 7. Хеш-функції. Криптографічні властивості. Завдання для СРС. Засвоєння лекційного матеріалу. Виконання вправ.

Література: основна [1, 4, 6, 7].

Тема 8. Факторизація цілих чисел. Найпростіші методи факторизації. Метод Ферма, Рабіна та ρ-метод. Функція Ейлера та її властивості. – 2 год. Розглядаються найпростіші методи факторизації: решето Ератосфена, пробного ділення, на основі малої теореми Ферма. Приклади роботи цих методів.

Література: основна [6, 7].

Тема 9. Криптографічні системи та їх класифікація. Характеристика криптографічних систем. Симетричні та асиметричні системи. Протоколи обміну ключами та їх генерація. Шифр Щаміра та RSA, їх властивості. Розглядаються два шифри, які відносяться до криптосистем з відкритим ключем. Досліджуються їх властивості та недоліки. Ілюстрація методів на прикладах.

Література: основна [1, 4, 6, 7].

Тема 10. Протоколи обміну ключами та їх реалізація: Діффі-Хеллмана та Ель Гамаля. Шифр Щаміра та його властивості. Порівняльна характеристика цих методів. Розглядаються порівняння за модулем та методи їх розв'язання. Єдиність розв'язку та його існування. Теорема Діріхле. Ілюстрація методів на прикладах.

Література: основна [1, 4, 6, 7].

4. Структура залікового кредиту з дисципліни «Оцінка складності алгоритмів шифрування»

	Кількість годин	
	Лекції	Практичні заняття
Змістовий модуль 1. Основи теорії чисел та математичних основ захисту інформації.		
Тема 1. Предмет математичних основ захисту інформації.	2	
Тема 2. Машинні моделі.	2	2
Тема 3. Класи складності P і NP. Поняття односторонньої функції та його роль в криптографії.	2	2
Тема 4. Основні поняття теорії ймовірностей. Випадкові величини та їх властивості. Рівномірний, біноміальний та інші розподіли. Поняття стійкості криптосистеми.	2	2
Тема 5. Основні поняття теорії груп.	2	2
Змістовий модуль 2. Основні області застосування симетричних та асиметричних криптосистем. Проблеми обміну ключами та основні методи генерації та обміну ключами. Принципи побудови асиметричних криптосистем. Приклади асиметричних шифрів.		
Тема 6. Кільця та їх властивості. Ідеали кільця та його властивості. Поняття дискретного логарифму та алгоритм його обчислення.	2	4
Тема 7. Хеш-функції. Криптографічні властивості.	2	2
Тема 8. Факторизація цілих чисел.	2	2
Тема 9. Криптографічні системи та їх класифікація.	2	2
Тема 10. Протоколи обміну ключами та їх реалізація: Діффі-Хеллмана та Ель Гамаля.	2	2
Разом	20	20

5. Тематика практичних (семінарських або лабораторних) занять

Практичне заняття №1

Тема: Обчислення асимптотики функцій складності**.**

Мета: Обчислення та дослідження асимптотики функцій складності.

Питання для обговорення:

1. Рекурсивні програми та методи їх складнісного аналізу: підстановки, розв'язання рекурентної залежності, метод генератрис

Література: 1, 2

Практичне заняття №2

Тема: Оцінка складності в моделі Тюрінга алгоритмів обчислення НСД та НСК та їх реалізація в різних мовах програмування: C, JAVA, Pyton.

Мета: Оцінити складності в моделі Тюрінга алгоритмів обчислення НСД та НСК та реалізувати їх в різних мовах програмування: C, JAVA, Pyton.

Питання для обговорення:

1. Моделі Тюрінга алгоритмів обчислення НСД
2. Моделі Тюрінга алгоритмів обчислення НСК

Література: 1, 2.

Практичне заняття №3

Тема: Основні дискретні розподіли.

Мета: Вивчення та дослідження основних дискретних розподілів.

Питання для обговорення:

1. Ланцюги Маркова та робота з ними.
2. Обчислення матриці переходів за початковими даними..

Література: 1, 2.

Практичне заняття №4

Тема:. Алгоритми і приклади застосування методів теорії груп в криптографії.

Мета: вивчити та дослідити алгоритми і приклади застосування методів теорії груп в криптографії..

Питання для обговорення:

1. Теорія груп в криптографії
2. Дискретний логарифм та його криптоаналіз.
3. Основні завдання відстеження вимог.

Література: 1, 2.

Практичне заняття №5

Тема: Обчислення в скінченних кільцях та алгоритми їх реалізації.

Мета: Вивчення та дослідження обчислень в скінченних кільцях та алгоритмів їх реалізації.

Питання для обговорення:

1. Алгоритми реалізації в скінченних кільцях
2. Незвідні поліноми над скінченними полями лишків.
3. Побудова полів порядку p n та обчислення в таких полях. Застосування в криптографії.

Література: 1, 4

Практичне заняття №6

Тема: Основна теорема арифметики та наслідки з неї.

Мета: Вивчення та дослідження основної теореми арифметики та наслідки з неї.

Питання для обговорення:

1. Проблема факторизації та її зв'язок з проблемою тестування чисел на простоту.
2. Алгоритми побудови простого числа великої розрядності та їх реалізація.

Література: 1, 3.

Практичне заняття №7

Тема: Факторизація цілих чисел..

Мета: Вивчення та дослідження методів факторизації цілих чисел.

Питання для обговорення:

1. Найпростіші методи факторизації: решето Ератосфена, метод Ферма.
2. Функція Ойлера та її властивості.
3. Алгоритми розв'язання конгруенцій.

Література: 1, 2.

Практичне заняття №8

Тема: Реалізація: шифру Шаміра та RSA.

Мета: Вивчення та дослідження шифру Шаміра та RSA.

Питання для обговорення:

1. Шифр Шаміра.
2. Шифр RSA.
3. Оцінка стійкості цих шифрів.

Література: 1, 2.

Практичне заняття №9

Тема: Реалізація: алгоритмів Діффі-Хеллмана та Ель Гамаля.

Мета: Вивчення та дослідження алгоритмів Діффі-Хеллмана та Ель Гамаля.

Питання для обговорення:

1. Алгоритмів Діффі-Хеллмана.
2. Алгоритми Ель Гамаля.

Література: 1, 3.

6. Самостійна робота

№ п/п	Тематика
1	Криптографія еліптичних кривих
2	Криптографічний алгоритм Рабіна
3	Алгоритми переходу від однієї основи систем числення до іншої основи.
4	Приклади на обчислення складності функцій.
5	Оцінки складності алгоритмів обчислення поліномів, множення матриць.
4	Складність алгоритмів обчислення додавання, віднімання, множення та ділення в різних системах числення.
5	Алгоритми переходу від однієї основи систем числення до іншої основи.
6	Основні дискретні розподіли. Ланцюги Маркова та робота з ними. Приклади побудови ланцюга Маркова, обчислення матриці переходів за початковими даними. Ентропія і інформація, основні властивості.
7	Побудова скінченних груп та їх підгруп. Приклади побудови криптосистеми на основі кілець.
8	Охарактеризувати значення проблеми P≠NP в криптографії. Дати означення односторонньої функції та її властивостей
9	Дати означення складності алгоритму в часі і пам’яті. Навести класифікацію проблем, виходячи з цього означення.
10	Навести означення детермінованої МТ, недетермінованої МТ та багато стрічкової МТ. Який часовий зв’язок існує між цими моделями обчислень.
11	Довести примітивну рекурсивність арифметичних операцій, функцій НСД і НСК.
12	Означення групи, кільця та поля. Навести основні властивості цих алгебр та їх роль у криптографії.

13	Метод частотного аналізу природо мовних текстів та його роль в криптоаналізі.
14	Алгоритми обчислення теоретико-числових функцій.
15	Розглянути відповідні розділи загальної алгебри стосовно скінченних кілець полів.
16	Алгоритими модульної арифметики та їх реалізація в різних мовах програмування: C, JAVA, Pyton. Порівняння часових оцінок виконання алгоритмів в різних реалізаціях.
17	Алгоритм розв'язання системи порівнянь та його реалізація
18	Методи розв'язання рівнянь та порівнянь в полях та кільцях лишків.
19	Побудувати 6-7 прикладів, які ілюструють роботу шифру Шаміра та оцінити складність кожного приклада на предмет стійкості до зламу.

7. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни **«Безпека та конфіденційність Інтернет-речей»** використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- залікове модульне тестування та опитування;
- оцінювання виконання практичних завдань;
- презентації та виступи на наукових заходах;
- інші види індивідуальних та групових завдань;
- екзамен.

Шкала оцінювання:

За шкалою ТНЕУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)

1-34		F (незадовільно з обов'язковим повторним курсом)

8. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Мультимедійний проектор	1 - 10
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 10

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272с.
2. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Ришковець Ю. В. Алгоритмізація та програмування. Ч. 1 : навчальний посібник / Ю. В. Ришковець, В. А. Висоцька. – Львів : "Новий Світ-2000", 2020. – 337 с.
4. Ришковець Ю. В. Алгоритмізація та програмування. Ч. 2: навчальний посібник / Ю. В. Ришковець, В. А. Висоцька. – Львів : "Новий Світ-2000", 2020. – 314 с.
5. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
6. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
7. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
8. Асиметричні алгоритми шифрування у системі залишкових класів / Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138
9. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
10. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
11. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків/ І.З. Якименко, Л.М. Тимошенко, М.М. Касянчук. Сучасна спеціальна техніка, №2, 2018. С.63-71.