Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий
Фізико-технічний інститут
Кафедра математичних методів
захисту інформації

Теоретико-числові алгоритми в криптології

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*11 Математика і статистика*
Спеціальність	*113 Прикладна математика*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Вибіркова/Цикл професійної підготовки*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*3 курс, весняний семестр*
Обсяг дисципліни	*4 кредити, 120 годин* *Лекційних занять: 36 год* *Практичних занять (КП): 18 год* *Лабораторні роботи: 18 год* *Самостійна робота студентів: 48 год*
Семестровий контроль/ контрольні заходи	*Залік, МКР*
Розклад занять	*http://rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції: асистент Ядуха Дарія Вікторівна (yadukhadv-ipt@lll.kpi.ua)* *Практичні: асистент Ядуха Дарія Вікторівна (yadukhadv-ipt@lll.kpi.ua)* *Лабораторні: асистент Якимчук Олексій Петрович (yakymchukop-ipt@lll.kpi.ua)*
Розміщення курсу	*Google Classroom*

Програма навчальної дисципліни

1 Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

У дисципліні «*Теоретико-числові алгоритми в криптології*» вивчається низка методів, алгоритмів і понять, що лежать в основі роботи та аналізу як симетричних, так і асиметричних криптосистем.

Кредитний модуль знайомить студентів з алгоритмами факторизації цілих чисел; алгоритмами знаходження дискретних логарифмів; з ефективними методами розв'язання систем лінійних та нелінійних рівнянь, алгоритмами на решітках та деякими іншими алгоритмами, що використовуються при реалізації та аналізі криптографічних систем. При цьому робиться наголос на особливостях обчислювальної реалізації зазначених методів та алгоритмів.

Метою вивчення дисципліни є надання майбутнім фахівцям знань у галузі найуживаніших у криптології теоретико-числових, алгебраїчних та обчислювальних методів і алгоритмів, а також практичних навичок їх реалізації та застосування.

Згідно з вимогами програми навчальної дисципліни студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

- **знання:**
  - алгоритмів факторизації цілих чисел;
  - алгоритмів знаходження дискретних логарифмів;
  - алгоритмів розв'язування систем лінійних рівнянь у скінченних полях;
  - основних понять та термінів для роботи з цілочисельними решітками у криптології;
  - алгоритмів на решітках.
- **уміння:**
  - реалізовувати алгоритми факторизації цілих чисел;
  - реалізовувати алгоритми знаходження дискретних логарифмів;
  - реалізовувати алгоритми розв'язування систем лінійних рівнянь у скінченних полях;
  - застосовувати алгоритми на решітках для криптоаналізу.
- **досвід:**
  - застосування алгоритмів факторизації цілих чисел та алгоритмів знаходження дискретних логарифмів у криптоаналізі;
  - комп'ютерної реалізації деяких алгоритмів факторизації цілих чисел та знаходження дискретних логарифмів.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні компетентності та результати навчання за Стандартом вищої освіти:

- **Загальні компетентності**:
  - ЗК 1 – Здатність учитися і оволодівати сучасними знаннями;
  - ЗК 2 – Здатність застосовувати знання у практичних ситуаціях;
  - ЗК 10 – Навички у використанні інформаційних і комунікаційних технологій.
- **Фахові компетентності**:
  - ФК 2 – Здатність виконувати завдання, сформульовані у математичній формі;
  - ФК 3 – Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень;
  - ФК 4 – Здатність розробляти алгоритми та структури даних, програмні засоби та програмну документацію;
  - ФК 8 – Здатність використовувати сучасні технології програмування та тестування програмного забезпечення.
  - ФК 18 – Навички розв'язування специфічних математичних та комп'ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем.
- **Програмні результати навчання**:
  - РН 3 – Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв'язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів;
  - РН 4 – Виконувати математичний опис, аналіз та синтез дискретних об'єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів;
  - РН 11 – Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів;
  - РН 15 – Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.

2 Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Кредитний модуль «Теоретико-числові алгоритми в криптографії» забезпечується такими курсами:

- ЗО 12.1 «Дискретна математика. Частина 1»;
- ЗО 12.2 «Дискретна математика. Частина 2»;
- ЗО 21.1 «Програмування. Частина 1»;
- ЗО 21.2 «Програмування. Частина 2»;
- ПО 1.1 «Прикладна алгебра. Частина 1»;
- ПО 1.2 «Прикладна алгебра. Частина 2»;
- ПО 3 «Спеціальні розділи обчислювальної математики».

3 Зміст навчальної дисципліни

Розділ 1. *Алгоритми факторизації цілих чисел.*
Розділ 2. *Алгоритми розв'язання систем лінійних рівнянь.*
Розділ 3. *Алгоритми розв'язання задачі дискретного логарифмування.*
Розділ 4. *Алгоритми на решітках.*

4 Навчальні матеріали та ресурси

Базова рекомендована література

1. *Т.Кормен, Ч. Лейзерсон, Р. Рівест, К. Стайн.* Вступ до алгоритмів (переклад з англ. Introduction to algorithms). – Київ: К. І. С., 2019. – 1288 с.
2. *Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.* Інформаційна безпека. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
3. *О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс.* Прикладна криптологія: системи шифрування. – Житомир: ДУТ, 2014. – 448 с.
4. *А. В. Анісімов* Алгоритмічна теорія великих чисел. К.: Академперіодика, 2001. – 218 с.
5. *В. Задірака, О. Олексюк* Комп'ютерна арифметика багаторозрядних чисел. – Київ, 2003. – 324 с.

Допоміжна рекомендована література

1. *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.* Handbook of Applied Cryptography, 1996. – 780 с.
2. *Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman.* An Introduction to Mathematical Cryptography, 2008. – 523 с.
3. *Razvan Barbulescu.* Algorithms for discrete logarithm in finite fields. Université de Lorraine, 2013. – 181 с.
4. *Seong Oun Hwang, Intae Kim, Wai Kong LeeModern.* Cryptography with Proof Techniques and Implementations, 2021. – 484 с.
5. *Daniele Micciancio, Sbafi Goldwasser.* Complexity of Lattice Problems a Cryptographic Perspective, 2002. – 220 с.

5 Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

1. Задача факторизації та задача пошуку канонічного розкладу числа, доведення їх поліноміальної еквівалентності. Задача факторизації у криптографії. Метод Ферма.
2. Метод Полларда. Алгоритм Діксона.
3. Наближені та ланцюгові дроби. Алгоритм Брілхарта-Моррісона.
4. Алгоритм квадратичного сита (Померанця). Алгоритми Відемана та Ланцоша, їх застосування у алгоритмах факторизації з використанням факторних баз.
5. Алгоритм Ленстри.
6. Задача дискретного логарифмування. Алгоритм узгодження.
7. Алгоритми Поларда для дискретного логарифмування (ρ-метод та λ-метод).
8. Алгоритм Сільвера-Поліга-Гелмана. Алгоритм index-calculus.
9. Алгоритм Коперсміта.
10. Модифікації задачі дискретного логарифмування та алгоритми їх розв'язання.
11. Решітки: основні поняття та терміни (частина 1).
12. Решітки: основні поняття та терміни (частина 2). Теореми Блікфельда, Ерміта, Мінковського.
13. Алгоритмічні задачі на решітках: задача входження, задача рівності, задача SBR, задачі SVP, CVP та їх модифікації.
14. Алгоритм Бабая. Алгоритм ортогоналізації Грама-Шмідта.
15. Алгоритм LLL.
16. Узагальнення та модифікації LLL.
17. Застосування LLL для криптоаналізу.
18. Залік.

Практичні заняття

1. Розв'язання задач на застосування алгоритмів Ферма та Полларда.
2. Побудова ланцюгових та наближених дробів. Алгоритм Діксона та Брілхарта-Моріссона.
3. Приклади застосування алгоритмів Ленстри та квадратичного сита (Померанця) для факторизації чисел.
4. Проведення частини №1 модульної контрольної роботи.
5. Приклади застосування алгоритму узгодження та ρ-методу Поларда.
6. Розв'язання задач на застосування алгоритмів Сільвера-Поліга-Гелмана та index-calculus.

7. Проведення частини №2 модульної контрольної роботи.

8. Приклади цілочисельних решіток та застосування алгоритму ортогоналізації Грама-Шмідта.

9. Проведення частини №3 модульної контрольної роботи.

Лабораторні роботи

1. Пошук канонічного розкладу великого числа, використовуючи відомі методи факторизації.

2. Реалізація алгоритму Сільвера-Поліга-Геллмана для розв'язання задачі дискретного логарифмування.

3. Реалізація алгоритму index-calculus для розв'язання задачі дискретного логарифмування, використовуючи розпаралелювання.

6 Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал. Перед здачею лабораторної роботи на занятті студенту необхідно самостійно або в бригаді з двох людей виконати лабораторну роботу.

Для кращого засвоєння матеріалу потрібно виконувати домашні завдання, які можна здавати до наступного практичного заняття. Для підготовки до виконання домашніх завдань слід скористатися рекомендованою літературою та конспектом лекцій.

Лабораторні роботи виконуються студентом самостійно, або в бригаді з двох студентів. При виконанні лабораторної роботи не дозволяється використовувати готові реалізації та програмний код, створений іншими особами. Захист лабораторної роботи відбувається студентом самостійно або в бригаді з двох студентів (залежно від обраного типу виконання завдання). При захисті лабораторної роботи студенти зобов'язані продемонструвати процес та результати застосування створеної програмної реалізації, а також відповісти на питання стосовно створеного програмного коду та теоретичні контрольні питання.

При підготовці до складання частини модульної контрольної роботи студенту необхідно повторити теоретичний та практичний матеріал за відповідною темою. При написанні роботи не дозволяється користуватись жодними допоміжними засобами, конспектом тощо. За вимогою викладача студент має пройти захист письмової частини модульної контрольної роботи. При захисті студенту потрібно описати свій спосіб виконання завдань задля обґрунтування самостійності виконання цього завдання. У випадку якщо студент не відповідає на запитання щодо своїх розв'язків, завдання не зараховується.

Політика та контроль

7 Політика навчальної дисципліни (освітнього компонента)

- **Відвідування занять**

  Студенту рекомендується відвідувати леакції та практичні заняття. Під час дії воєнного стану матеріал лекцій та практичних занять дублюється в асинхронному режимі, щоб студенти мали можливість опрацювати матеріал самостійно, якщо не мали можливості бути присутніми на заняттях.

  Система оцінювання орієнтована на виконання занять, які здатні розвинути практичні уміння та навички.

- **Пропущені контрольні заходи**

  Результат частини модульної контрольної роботи для студента, який не виконав контрольний захід в зазначені терміни, є нульовим. Повторне написання частини модульної контрольної роботи не допускається.

- **Оголошення результатів контрольних заходів**

  Захист виконаного домашнього завдання (за вимогою) та модульної контрольної роботи проводиться у формі співбесіді з викладачем. Під час захисту студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами задач.

  Результати виконання домашніх та модульної контрольної робіт вказуються на бланках для частин модульної контрольної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

  Результати письмової частини заліку вказуються на бланках (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Усна частина заліку проводиться у форматі співбесіди зі студентом. Студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами задач.

- **Академічна доброчесність**

  Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code. У випадку, якщо в результаті перевірки лабораторної або домашньої роботи студента виявлено плагіат більше 10%, студент зобов'язаний виконати завдання повторно та не матиме можливість складати залік на основній сесії. У випадку, коли плагіат програмного коду студента становить менше 10%, студент отримає штраф -10 балів до рейтингу.

- **Норми етичної поведінки**

  Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

- **Процедура оскарження результатів контрольних заходів**

  Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

  Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оцінювального листа та/або зауважень.

8 Види контролю та рейтингова система оцінювання результатів навчання (РСО)

№ з/п	Контрольний захід	Макс. бал	Ваговий бал	Кількість	Всього
1.	Домашні роботи	3	1	7	21
2.	Лабораторні роботи	11	1	3	33
3.	Модульна контрольна робота	46	1	1	46
	Всього	100			

Згідно з календарним планом курсу, контрольні заходи проводяться:

- лабораторні роботи:
  - лабораторна робота №1 – на 4-му занятті з лабораторних робіт (7-8 тиждень навчання);
  - лабораторна робота №2 – на 7-му занятті з лабораторних робіт (13-14 тиждень навчання);
  - лабораторна робота №3 – на 9-му занятті з лабораторних робіт (16-17 тиждень навчання);
- модульна контрольна робота:
  - частина №1 МКР – на 3-му практичному занятті (5-6 тиждень навчання);
  - частина №2 МКР – на 6-му практичному занятті (11-12 тиждень навчання);
  - частина №3 МКР – на 8-му практичному занятті (15-16 тиждень навчання);
- залік – на 18-му тижні навчання.

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 8-му та 14-му навчальному тижнях кожного семестру. Для одержання першої атестації поточний рейтинг студента повинен бути щонайменше 10 балів, для одержання другої атестації – щонайменше 20 балів.

Набрані рейтингові бали студента за семестр є його фінальною оцінкою за таких умов:

1. сума рейтингових балів ≥ 60;
2. зараховані усі лабораторні роботи.

У випадку, якщо студент набрав менше за 60 балів протягом семестру або якщо студент хоче спробувати підвищити отриманий результат, студент складає залікова робота. При складанні залікової роботи усі набрані за семестр бали анулюються. Кількість балів, які можна набрати за залікову роботу, дорівнює 100 балів.

Для допуску до перескладання студенту необхідно здати усі лабораторні роботи.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):
Склав: асистент кафедри ММЗІ, Ядуха Дарія Вікторівна.
Ухвалено кафедрою математичних методів захисту інформації (протокол №2 від 16.02.2022).
Затверджено Методичною комісією ННФТІ (протокол №6 від 30.06.2022).