



Прикладні питання побудови та аналізу складності алгоритмів

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Третій (доктор філософії)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Прикладна математика</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Очна (денна, вечірня)</i>
Рік підготовки, семестр	<i>2 курс, третій семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 6 кредитів ЕКТС / 180 годин Лекційних занять: 10 годин Практичних занять: 8 годин Самостійна робота студентів: 162 години</i>
Семестровий контроль/ контрольні заходи	<i>Екзамен</i>
Розклад занять	http://rozklad.kpi.ua http://ipt.kpi.ua/navchalnij-protses
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>доц. Кучинська Наталія Вікторівна, к.т.н. (kuchynskanv-ipt@ill.kpi.ua)</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

Навчальна дисципліна «Прикладні питання побудови та аналізу складності алгоритмів» присвячена дослідженню обчислювальних алгоритмів на специфічних алгебраїчних структурах, які наразі широко використовуються у криптографії, зокрема, для створення постквантово стійких криптосистем.

Розглядаються питання ефективної реалізації алгоритмів на еліптичних кривих, представлених у різних формах (Вейерштраса, Монтгомері, Едвардса, Хаффа тощо), впливу способу представлення та особливостей архітектури на складність таких алгоритмів. Також розглядаються алгоритми, які використовують постквантово складні теоретико-числові задачі, та алгоритми на решітках.

При викладенні матеріалу навчальної дисципліни виділяються такі аспекти:

- основні теоретичні поняття;
- математичні задачі та криптографічні алгоритми й протоколи, що ґрунтуються на викладених теоретичних поняттях;
- застосування та перспективне застосування розглянутих криптографічних алгоритмів та протоколів у сучасних інформаційних технологіях.

Міждисциплінарні зв'язки: дисципліну забезпечують дисципліни: «Сучасні методи прикладної математики», «Спеціальні розділи математичного моделювання» та дисципліни, пов'язані з математичними методами захисту інформації.

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

знання:

- означення складності та стійкості (теоретичної та практичної) криптографічних алгоритмів;
- визначення рівня практичної стійкості криптографічного алгоритму згідно міжнародних нормативних документів;
- типи та основні властивості еліптичних кривих у формах Вейерштрасса, Монтгомері, Едвардса, вимоги до стійкості криптосистеми на еліптичних кривих та способи її досягнення;
- визначення складності алгоритмів в моделі обчислень квантового комп'ютера;
- основні важкорозв'язувані задачі, які залишаються навіть за умови існування квантового комп'ютера та можуть бути використані для побудови асиметричних криптосистем, стійких у постквантовий період.

уміння:

- виділяти основні компоненти криптографічного алгоритму та будувати найпростіші оцінки стійкості криптографічних алгоритмів до основних методів криптоаналізу;
- вибирати, обґрунтовувати стійкість та використання криптографічних алгоритмів;
- оцінювати стійкість симетричних та асиметричних криптосистем у постквантовий період.

досвід:

- вільно орієнтуватись у сучасних тенденціях та перспективних напрямках проектування криптографічних алгоритмів та протоколів, використовувати апарат теорії алгоритмів та теорії складності для дослідження задач предметної області.
та адекватність, формулювати умови використання та обмеження на параметри

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

Навчальна дисципліна «Прикладні питання побудови та аналізу складності алгоритмів» є тією частиною математичних знань, яка пов'язана з дослідженням, моделюванням, проектуванням, розробкою та побудовою складних криптографічних систем, систем захисту інформаційних систем, а також систем комп'ютерної обробки та інформаційно-комунікаційних систем різного роду інформації.

Знання сучасних та перспективних криптографічних алгоритмів відіграє надзвичайно важливу роль у формуванні важливих компетенцій майбутніх науковців, пов'язаних із застосуванням інформаційних технологій в професійній та дослідницькій діяльності. Розробка та успішна експлуатація програмних продуктів, систем баз даних, систем захисту, засобів інформаційної безпеки, тощо вимагають від спеціаліста ґрунтовних знань багатьох розділів криптографії та криптоаналізу. Особливої уваги заслуговує сучасний математичний апарат, що лежить в основі криптографічних алгоритмів та протоколів, що використовуються в реальних криптографічно захищених системах, та процесах їх функціонування, та перспективах їх застосування а також заміни у відповідності до розвитку сучасних обчислювальних потужностей та методів криптоаналізу.

3. Зміст навчальної дисципліни

Розділ 1. Криптографічні алгоритми та сучасні вимоги до них.

Тема 1.1. Вимоги до новітніх криптографічних алгоритмів та протоколів

Тема 1.2. Стандартизовані криптографічні алгоритми та протоколи

Розділ 2. Постквантові алгоритми та протоколи.

Тема 2.1. Алгоритми у квантовій моделі обчислень

Тема 2.2. Постквантові криптографічні алгоритми та протоколи

4. Навчальні матеріали та ресурси

Базова рекомендована література

1. Кормен, Томас Г. Вступ до алгоритмів : Переклад з англійської третього видання : [укр.] = Introduction to Algorithms : Third Edition : [пер. з англ.] / Томас Г. Кормен, Чарльз Е. Лейзерсон, Роналд Л. Рівест, Кліфорд Стайн. – К.: К.І.С., 2019. – 1288 с.

2. Introduction to Modern Cryptography Mihir Bellare Phillip Rogaway <https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf>

3. NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process, 2017. <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf>

4. Michele Mosca and Douglas Stebila. Open Quantum Safe – software for prototyping quantum-resistant cryptography. <https://openquantumsafe.org/>

Допоміжна рекомендована література

1. AES. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

2. A New Encryption Standard of Ukraine: The Kalyna Block Cipher <http://eprint.iacr.org/2015/650.pdf>

3. Information technology – Security techniques – Modes of operation for an n-bit block cipher https://webstore.iec.ch/preview/into_isoiec10116%7Bed3.0%7Den.pdf.

4. СТБ 34.101.31 – 2011 <http://apmi.bsu.by/assets/files/std/belt-spec27.pdf>.

5. E. Alkim, N. Bindel, J. Buchmann, O. Dagdelen, P. Schwabe. TESLA: tightly-secure efficient signatures from standard lattices. Cryptology ePrint Archive Report 2015/755, version 20161117:055833 (2015)

6. D. Deutsch and R. Jozsa, Rapid Solution of Problems by Quantum Computation, Proceedings of the Royal Society of London, Series A 439 (1992), 553–558.

7. P.W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing 26 5 (1997), 1484–1509.

8. M. Roetteler and T. Beth, Polynomial-Time Solution to the Hidden Subgroup Problem for a Class of non-abelian Groups. Quantum Physics Archive <http://arxiv.org/abs/quant-ph/9812070>.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Для лекційних та практичних занять використовуються дискусійний метод, дослідницький метод та метод проблемного виконання. На лекціях здобувачі заохочуються до висловлювання власних думок та ведення дискусії із викладачем. На практичних заняттях здобувачі заохочуються до ініціативності, самостійності та творчого пошуку.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
	Розділ 1. Криптографічні алгоритми та сучасні вимоги до них.
1	Криптографічні алгоритми сучасні та на перехідний до квантового період. Вимоги до рівня стійкості алгоритмів..
2	Міжнародні та державні стандарти України в галузі криптографічного захисту інформації та їх актуальність на перехідний період. Сучасні криптографічні алгоритми та протоколи на еліптичних кривих.
3	Криптографічні протоколи розділення секрету та доведення без розголошення, інтерактивні та неінтерактивні.
	Розділ 2. Постквантові алгоритми та протоколи.
4	Постквантові криптографічні алгоритми. Вимоги до постквантових криптографічних алгоритмів. Конкурс NIST та основні результати проміжних етапів конкурсу. Постквантові криптографічні алгоритми цифрового підпису та інкапсуляції ключа.
5	Основні класи математичних задач, що використовуються в постквантових алгоритмах. Алгоритми в квантовій моделі обчислень Алгоритми Шора, Гровера.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Аспекти реалізації, впровадження та застосування державних стандартизованих криптографічних алгоритмів.
2	Оцінювання асимптотичної швидкості росту складності розв'язання задач криптоаналізу сучасних криптографічних алгоритмів. Експрес контроль.
3	Аспекти реалізації та впровадження постквантових криптографічних алгоритмів.
4	Оцінювання асимптотичної швидкості росту складності розв'язання задач криптоаналізу сучасних постквантових криптографічних алгоритмів.

6. Самостійна робота студента

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи здобувачам пропонується виконати дослідження одного з існуючих стандартизованих алгоритмів або перспективного криптографічного алгоритму, що відповідає сучасним вимогам щодо стійкості та є найбільш близьким до тематики наукових досліджень студента. Пропонується провести перспективний аналіз зазначеного криптографічного алгоритму щодо стійкості у перехідний до квантового та постквантовий період. Дослідити стійкість відносно існуючих методів криптоаналізу, шляхи та методи вдосконалення. Оцінити швидкодію його програмних/апаратних реалізацій у порівнянні з наразі існуючими реалізаціями алгоритмів, що виконують ту ж криптографічну задачу.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань,

контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички.

Пропущені контрольні заходи

Студент, який без поважних причин пропустив експрес контроль, одержує за нього нуль балів без можливості перескладання. Якщо пропуск стався з поважних причин (наприклад, хвороби), підтверджених відповідними документами, студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини не допускається.

Студент, який без поважних причин пропустив опитування, одержує за нього нуль балів без можливості перескладання. Якщо пропуск стався з поважної причини, студенту буде надана можливість скласти теоретичне опитування у інший узгоджений із викладачем час.

Пропущений екзамен не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості “не з’явився” та повинен скласти екзамен вже на додатковій сесії..

Оголошення результатів контрольних заходів

Результати виконання домашніх завдань оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються коментарями, в яких студенти можуть побачити свою оцінку за певними критеріями, а також виокремлення основних помилок та зауваження.

Результати експрес контролю вказуються на бланках для роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Опитування проходить в усній формі (колоквіум) або у вигляді тесту, в залежності від форми навчання. На колоквіумі зауваження на свої відповіді студент одержує безпосередньо під час спілкування; оцінка за колоквіум оголошується наприкінці його проходження. При виконанні тесту оцінка оголошується після перевірки, і студент може одержати розгорнуте пояснення щодо виставленої оцінки та зауваження по своїх відповідях.

Результати письмової частини екзамену вказуються на бланках для письмової екзаменаційної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Результати усної частини екзамену оголошуються наприкінці його проходження.

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>.

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 оціночного листа та/або зауважень.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

Рейтинг студента з дисципліни складається з балів, які він отримує за:

- 1) дві відповіді на практичних заняттях ;
- 2) експрес контролі (дві роботи) .

Система рейтингових балів та критерії оцінювання

1. Робота (відповіді) на практичних заняттях

Ваговий бал – 10. Максимальна кількість балів на всіх практичних заняттях дорівнює $10 \text{ балів} \times 2 = 20 \text{ балів}$.

- Володіння теоретичним матеріалом та вміння застосувати його до розв'язування практичних завдань. Отримано правильну відповідь та обґрунтовано всі ключові моменти розв'язування задачі 10 балів
- У відповіді присутні окремі незначні помилки 7-9 балів
- Наведено логічно правильну послідовність кроків розв'язання задачі. Окремі ключові моменти розв'язування обґрунтовано недостатньо. Можливі 1 – 2 негрубі помилки. 4-6 балів
- Незнання теоретичного матеріалу та невміння сформулювати послідовність кроків розв'язування задачі 0-3 балів

2. Експрес контроль

Ваговий бал – 20. Максимальна кількість балів за експрес-контроль (чотири тематичні роботи) дорівнює $20 \text{ балів} \times 2 = 40 \text{ балів}$.

- Повне виконання, отримано правильні відповіді до всіх задач 20 балів
- Непринципові помилки, недостатньо повне обґрунтування 18-19 балів
- У правильній послідовності ходу розв'язання відсутні деякі етапи 15-17 балів
- Присутні ідеї без реалізації, ключові моменти не обґрунтовано 12-15 балів
- Роботу не зараховано 0 балів

3. Заохочувальні бали

- Регулярне виконання домашніх завдань 3 бали
- Відсутність пропусків на практичних заняттях 3 бали
- Відсутність пропусків на лекційних заняттях 3 бали

Розмір шкали рейтингу $RD = r_C + r_E = 100$.

Розмір стартової шкали $r_C = 60$ балів.

Розмір екзаменаційної шкали $r_E = 40$ бали.

Умови допуску до екзамену: стартовий рейтинг $r_C \geq 30$ балів.

Критерії екзаменаційного оцінювання:

Екзаменаційний білет містить два теоретичні питання та дві задачі. Ваговий бал – 10.

Критерії оцінювання теоретичного питання:

- Вичерпна відповідь 10 балів
- Відповідь з незначними неточностями 8-9 балів
- Правильні формулювання з відсутністю доведень або прикладів 5-7 балів
- Грубі помилки у формулюванні та невміння будувати приклади 1-4 балів

- Повне незнання теоретичного питання 0 балів

Критерії оцінювання екзаменаційної задачі:

- Отримано правильну відповідь, обґрунтовано всі етапи розв'язування 10 балів
- Наведено логічно правильну послідовність кроків розв'язування. Можливі описки або недостатнє обґрунтування 8-9 балів
- У правильній послідовності ходу розв'язування відсутні окремі етапи 5-7 балів
- Присутні ідеї без реалізації 1-4 бали
- Повне незнання алгоритму розв'язування задачі 0 балів

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

<i>Кількість балів</i>	<i>Оцінка</i>
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: доцент кафедри ММЗІ, к.т.н. Кучинська Наталія Вікторівна

Ухвалено кафедрою математичних методів захисту інформації (протокол №6/2024 від 19.06.2024).

Погоджено Методичною комісією НН ФТІ (протокол №6/2024 від 27.06.2024)