



Сучасні алгебраїчні криптосистеми

ПО-3

Робоча програма навчальної дисципліни (Силабус)

• Реквізити навчальної дисципліни

| | |
|---|---|
| Рівень вищої освіти | <i>Другий (магістерський)</i> |
| Галузь знань | <i>11 Математика і статистика</i> |
| Спеціальність | <i>113 Прикладна математика</i> |
| Освітня програма | <i>Математичні методи криптографічного захисту інформації</i> |
| Статус дисципліни | <i>Нормативна</i> |
| Форма навчання | <i>очна(денна)</i> |
| Рік підготовки, семестр | <i>I курс, осінній семестр</i> |
| Обсяг дисципліни | <i>90 годин (3 кредити) (36 год. лекції, 18 год. лабораторні), срс 36 год.</i> |
| Семестровий контроль/ контрольні заходи | <i>Залік, МКР, ДКР</i> |
| Розклад занять | <i>rozklad.kpi.ua</i> |
| Мова викладання | <i>Українська</i> |
| Інформація про керівника курсу / викладачів | Лектор: <i>д.ф.-м.н., Олійник Андрій Степанович, a.oliynyk@knu.ua¹</i> Лабораторні: <i>к.ф.-м.н., Фесенко Андрій В'ячеславович, fesenko.andrii@lll.kpi.ua</i> |
| Розміщення курсу | <i>Google Classroom</i> |

• Програма навчальної дисципліни

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

При вивченні дисципліни «Сучасні алгебраїчні криптосистеми» здобувачі одержують знання про функціонування та застосування сучасних криптографічних примітивів, а також про абстрактний математичний апарат, який лежить в основі в їхній основі та забезпечує функціонування та стійкість. Здобувачі набувають практичні навички застосування відповідних криптосистем до задач, сформульованих мовою предметної області, аналізу обраних алгоритмів, та побудови більш складних криптографічних систем, які найчастіше є необхідними для розв'язання прикладних задач широкого спектру. Одержані в ході вивчення дисципліни знання та вміння можуть бути використані у майбутній професійній діяльності.

Мета: *здобути знання, навички та вміння використання та аналізу сучасних алгебраїчних криптосистем. Предмет дисципліни:* алгебраїчні криптосистеми, їх математичні основи, аналіз та застосування.

¹ Електронна пошта викладача або інші контакти для зворотного зв'язку, можливо зазначити прийомні години або години для комунікації у разі зазначення контактних телефонів. Для силабусу дисципліни, які викладає багато викладачів (наприклад, історія, філософія тощо) можна зазначити сторінку сайту де представлено контактну інформацію викладачів для відповідних груп, факультетів, інститутів.

Загальні компетентності:

ЗК1 – Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми.

Фахові компетентності:

ФК1 – Здатність формалізувати та розв'язувати складні задачі й проблеми, які потребують оновлення й інтеграції знань, часто в умовах неповної, неточної чи недостатньої інформації та суперечливих вимог.

ФК5 – Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем.

ФК6 - Здатність розроблювати новітні механізми криптографічного захисту

ФК8 - Здатність використовувати та впроваджувати існуючі механізми, протоколи та системи криптографічного захисту інформації

Програмні результати² навчання:

РН1 – Використовувати та адаптувати математичні теорії та моделі для забезпечення теоретичного підґрунтя розв'язання наукових та практичних задач

РН2 – Застосовувати існуючий математичний апарат, розробляти нові моделі, методи та алгоритми при вирішенні актуальних практичних задач широкого спектру

РН11 – Проводити аналіз криптографічних алгоритмів, протоколів та систем

РН12- Орієнтуватись у останніх досягненнях криптології

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

Дисципліна «Сучасні алгебраїчні криптосистеми» частково використовує знання та вміння, набуті у ході навчання за ОП Бакалавр протягом вивчення курсів «Алгебра та геометрія», «Дискретна математика», «Програмування», «Теорія складності», «Асиметричні криптосистеми та протоколи», та спрямовує їх у напрямку розв'язання відповідних прикладних задач математики із використанням сучасних алгебраїчних криптосистем.

Отримані практичні навички та засвоєнні знання необхідні для опанування дисципліни «Квантові обчислення та квантова криптографія» та для виконання науково-дослідницької та прикладної діяльності у галузі криптології.

Отримані практичні навички та засвоєнні знання можуть використовуватись у будь-яких дисциплінах, тематика яких пов'язана із алгоритмізацією задач та побудовою їх ефективних розв'язків, обчислювальними методами, криптографічним захистом інформації.

3. Зміст навчальної дисципліни

Розділ 1. Цілочисельні решітки

Тема 1.1. Вступ, предмет дисципліни. Поняття про решітки. [1,3,4,6]

Тема 1.2. Геометрія цілочисельних решіток [4,5,8]

Тема 1.3. Обчислювальні задачі на решітках [4,5,6,8]

² Для нормативних дисциплін зазначається згідно матриці відповідності програмних компетентностей та результатів навчання в освітній програмі.

Тема 1.4. LLL алгоритм [4,5,7]

Розділ 2. Криптосистеми на основі решіток

Тема 2.1. Безпека криптосистем [1,3,8]

Тема 2.2. Криптосистема GGH [4,5]

Тема 2.3. Криптосистема NTRUCrypt [1,4,5,8]

Тема 2.4. Гомоморфні криптосистеми [1,3,8]

Розділ 3. Спарювання на еліптичних кривих

Тема 3.1. Групи точок еліптичних кривих [1,2,4,5]

Тема 3.2. Дівізори на еліптичних кривих [1,2,4,5]

Тема 3.3. Спарювання, алгоритм Міллера [1,2,4,5]

Розділ 4. Криптосистеми на основі спарювання

Тема 4.1. Шифрування на основі ідентифікаторів [1,2,4,5,8]

Тема 4.2. Функціональне шифрування [1,2,4,5,8]

4. Навчальні матеріали та ресурси

Базова рекомендована література.

1. D. Boneh, V. Shoup A graduate course in applied cryptography, 2020 <http://toc.cryptobook.us> .

2. I F. Blake, G. Seroussi, N. P. Smart (Eds.) Advances in elliptic curve cryptography, Cambridge

University Press, 2005
<https://www.cambridge.org/core/books/advances-in-elliptic-curve-cryptography/136CF5172D2342471E9F5AF5AAFB2744> .

3. J. Katz, Y. Lindell Introduction to modern cryptography CRC Press, 2015
<https://www.crcpress.com/Introduction-to-Modern-Cryptography/Katz-Lindell/p/book/9781466570269> .

4. J.H. Silverman, J. Pipher, J. Hoffstein An introduction to mathematical cryptography, Springer, 2008
<https://link.springer.com/book/10.1007/978-0-387-77993-5> .

Додаткова рекомендована література.

5. S. D. Galbraith Mathematics of public key cryptography, Cambridge University Press, 2012
<https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html> .

6. A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi Classical and quantum computation, AMS, 2002
<http://dx.doi.org/10.1090/gsm/047> .

7. P. Q. Nguyen, B. Vall'ee (Eds.) The LLL algorithm. Survey and applications, Springer, 2010
<https://www.springer.com/gp/book/9783642022944> .

8. N.P. Smart Cryptography made simple, Springer, 2016
<https://link.springer.com/book/10.1007/978-3-319-21936-3> .

• Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Для проведення занять застосовується практичний метод. Для лекційних занять використовуються пояснювально-ілюстративний метод та метод проблемного

виконання, для проведення лабораторних робіт використовується частково-пошуковий та дослідницький методи навчання, при яких викладач ставить перед студентами проблему, і ті вирішують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, підбираючи для цього необхідні джерела інформації, методи, підходи тощо.

Перелік основних питань.

Розділ 1. Цілочисельні решітки

1. Цілочисельні решітки: означення і приклади.
2. Унімодулярні матриці, фундаментальний паралелепіпед, об'єм решітки.
3. Послідовні мінімуми решітки, теореми Блікфельда і Мінковського.
4. Задачі SVP.
5. Задачі CVP.
6. Редуковані базиси решіток.
7. Опис алгоритму LLL.
8. Коректність алгоритму LLL.
9. Обчислювальна складність алгоритму LLL.
10. Алгоритм округлення Бабаї.
11. Незначні функції та їх властивості.

Розділ 2. Криптосистеми на основі решіток

12. Безпека криптосистем щодо CPA.
13. Безпека криптосистем щодо CCA.
14. Гібридні криптосистеми.
15. Криптосистема GGH.
16. Кільця згорткових многочленів: множення, знаходження обернених, центральне підняття.
17. Криптосистема NTRUCrypt.
18. Коректність NTRUCrypt.
19. NTRU-решітки.
20. Криптоаналіз NTRUCrypt.
21. Синтаксис гомоморфних криптосистем.
22. Задачі LWE.
23. Базова криптосистема Бракерські-Джентрі-Вайкутанатана.
24. Допоміжні алгоритми в криптосистемі Бракерські-Джентрі-Вайкутанатана.
25. Повністю гомоморфна криптосистема Бракерські-Джентрі-Вайкутанатана.
26. Білінійне спарювання.

Розділ 3. Спарювання на еліптичних кривих

27. Еліптичні криві. Дівізори. Групи дівізорів.
28. Головні дівізори. Функція Вейля. Закон взаємності Вейля.
29. Алгоритм Міллера.
30. Спарювання Вейля.

Розділ 4. Криптосистеми на основі спарювання

31. Синтаксис шифрування на основі ідентифікаторів.
32. Безпека шифрування на основі ідентифікаторів.
33. Криптосистема на основі ідентифікаторів за допомогою спарювання Вейля.
34. Побудова цифрового підпису за допомогою шифрування на основі ідентифікаторів.
35. Синтаксис функціонального шифрування.
36. Функціональне шифрування на основі предикатів.
37. Синтаксис шифрування на основі скалярного добутку.
38. Побудова шифрування на основі скалярного добутку.

39. Синтаксис і безпека функціонального шифрування з двома аргументами.

40. Побудова функціонального шифрування з двома аргументами.

6. Самостійна робота студента

Самостійна робота студента складається з:

- підготовки до МКР та заліку шляхом опанування лекційного матеріалу та виконання заданих на лекціях домашніх завдань,
- підготовки до захисту лабораторних робіт;
- виконання ДКР.

● Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

● Порушення термінів виконання завдань та заохочувальні бали

| Заохочувальні бали | | Штрафні бали | |
|------------------------|------------------------------------|--------------|---|
| Критерій | Ваговий бал, додається до рейтингу | Критерій | Ваговий бал, віднімається від базового балу |
| Активність на заняттях | +2 бали | - | - |

● Відвідування занять

Відвідування лекцій та лабораторних занять, а також відсутність на них, не оцінюється. Однак, студентам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал, розв'язуються супутні задачі, необхідні для виконання лабораторних робіт та успішного написання МКР.

● Пропущені контрольні заходи

Результат модульної контрольної роботи для студента(-ки), який не з'явився на контрольний захід, є нульовим. У такому разі, студент(-ка) має можливість написати модульну контрольну роботу, але максимальний бал за неї буде дорівнювати 50% від загальної кількості балів. Повторне написання модульної контрольної роботи не допускається.

● Календарний рубіжний контроль

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 кожної атестації поточний рейтинг студента повинен бути не менше половини від суми максимальних балів за всі контрольні заходи, які були проведені на момент атестації.

● 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 контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами (згідно “Положення про систему забезпечення якості вищої освіти у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського”, “Положення про організацію навчального процесу”).

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

- **Рейтингова система оцінювання**

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

- лабораторні роботи (макс. 30 балів)
- домашню контрольну роботу (макс. 30 балів)
- результати модульної контрольної роботи (макс. 40 балів)

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів протягом семестру складає:

$$R_c = 30 + 30 + 40 = 100 \text{ балів.}$$

Семестровий контроль: залік

Зі здобувачами, які мають рейтингову оцінку менше 60 балів, а також з тими здобувачами, хто бажає підвищити свою рейтингову оцінку в семестрі, викладач проводить семестровий контроль у вигляді додаткової контрольної роботи або співбесіди. Попередній рейтинг здобувача скасовується, додаткова контрольна оцінюється в 100 балів.

- **Таблиця переведення рейтингових балів до оцінок за університетською шкалою**

| Рейтингові бали, RD | Оцінка за університетською шкалою |
|--------------------------|-----------------------------------|
| $95 \leq RD \leq 100$ | Відмінно |
| $85 \leq RD \leq 94$ | Дуже добре |
| $75 \leq RD \leq 84$ | Добре |
| $65 \leq RD \leq 74$ | Задовільно |
| $60 \leq RD \leq 64$ | Достатньо |
| $RD < 60$ | Незадовільно |
| Невиконання умов допуску | Не допущено |

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри ММЗІ, д.ф.-м.н. Олійником А.С.

Ухвалено кафедрою ММЗІ (протокол № 6 від 22.06.2022 р.)

Погоджено Методичною комісією НН ФТІ (протокол № 6 від 30.06.2022)