



# Методи реалізації криптографічних механізмів

## ПО-2

### 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>Обов'язкова</i>
Форма навчання	<i>очна(денна)</i>
Рік підготовки, семестр	<i>I курс, осінній семестр</i>
Обсяг дисципліни	<i>120 годин (4 кредити), 36 год. лекції, 18 год. лабораторні роботи, срс 66 год.</i>
Семестровий контроль/ контрольні заходи	<i>Іспит, модульна контрольна робота</i>
Розклад занять	<i>Rozklad.kpi.ua</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	Лектор: <i>д.т.н., Кудін Антон Михайлович, pplayshner@gmail.com</i> Лабораторні: <i>Селюх Поліна Валентинівна</i>
Розміщення курсу	<i>Посилання на дистанційний ресурс pplayshner@gmail.com</i>

#### ● Програма навчальної дисципліни

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

*Перехід людства до інформаційного суспільства супроводжується революційними змінами в усіх сферах громадської діяльності, а насамперед – в технології захисту інформаційних ресурсів. Ці зміни поширюються і на всі науки, що досліджують проблеми захисту інформації від навмисних та ненавмисних загроз, в тому числі – криптології. Так в останні роки з'явилися численні роботи (зокрема Голдрейха, Гольдвассера та інших), в яких досліджується основи криптології, формулюються специфічні саме для криптології методи досліджень – тобто проходить процес ставлення криптології як самостійної науки, а не тільки як розділу прикладної математики. Іншою рисою останнього часу є створення поняття „відкритої криптографії” і поширення криптографічних методів для захисту інформації в недержавних і „відкритих” автоматизованих системах.*

*Ці фактори приводять до актуалізації проблеми адекватної реалізації базових криптографічних примітивів та протоколів, адекватності створених теоретичних моделей криптології реальним ситуаціям, що виникають при їх застосуванні, вміння практичного застосування методів криптології.*

Саме цим питанням присвячена дисципліна „Методи реалізації криптографічних механізмів захисту інформації”. Курс може бути використаний при створенні та експлуатації систем захисту інформації, а також при проведенні сертифікації та експертизи засобів захисту інформації.

**Мета:** вивчення дисципліни є ознайомлення студентів з сучасними моделями, що застосовуються в криптології та їх практичною реалізацією, надання інформації про алгоритми реалізації криптосистем. Завданням дисципліни є засвоєння студентами вміння адекватно оцінювати стійкість реальних криптосистем, основних алгоритмів їх реалізації, а також установлення взаємозв'язку між теоретичними моделями та реалізаціями криптографічних механізмів в автоматизованих системах.

**Предмет** дисципліни: криптографічні перетворення інформації, криптографічні примітиви, криптографічні алгоритми, криптосистеми.

#### **Загальні компетентності:**

ЗК2 – Здатність генерувати нові ідеї та нестандартні підходи до їх реалізації, адаптуватися та діяти в нових ситуаціях, виявляти ініціативу, інноваційність та підприємливість.

#### **Фахові компетентності:**

ФК2 – Здатність проводити наукові дослідження з розроблення нових та адаптацією існуючих математичних та комп'ютерних моделей для дослідження різноманітних процесів, явищ і систем, проводити відповідні чисельні експерименти з аналізом одержаних результатів.

ФК 5 - Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем

ФК-6 - Здатність розроблювати новітні механізми криптографічного захисту

ФК 7 - Здатність проектувати, розроблювати та реалізовувати системи криптографічного захисту з урахуванням сучасних досягнень науки та існуючої правової та нормативної бази

ФК 8 - Здатність використовувати та впроваджувати існуючі механізми, протоколи та системи криптографічного захисту інформації

#### **Програмні результати<sup>1</sup> навчання:**

РН 2 – Застосовувати існуючий математичний апарат, розробляти нові моделі, методи та алгоритми при вирішенні актуальних практичних задач широкого спектру

РН 9 - Здійснювати математичне і комп'ютерне моделювання складних систем та процесів, обчислювальні експерименти з використанням сучасних методів інтелектуального аналізу даних та комп'ютерних технологій

РН 11 – Проводити аналіз криптографічних алгоритмів, протоколів та систем

РН12– Орієнтуватись у останніх досягненнях криптології

РН13 - Розроблювати нові криптографічні алгоритми, механізми та системи захисту

---

<sup>1</sup> Для нормативних дисциплін зазначається згідно матриці відповідності програмних компетентностей та результатів навчання в освітній програмі.

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

Дисципліна «Методи реалізації криптографічних механізмів захисту інформації» частково використовує знання та вміння, набуті у ході вивчення курсів «Проектування, розробка і реалізація криптографічних систем» та спрямовує їх у напрямку розв'язання відповідних прикладних задач математики із використанням сучасних алгебраїчних криптосистем.

## 3. Зміст навчальної дисципліни

**Тема 1.** Теоретичні моделі симетричних криптографічних систем.

**Тема 2.** Теоретичні моделі асиметричних криптографічних систем.

**Тема 3.** Системи управління ключами.

**Тема 4.** Криптографічні протоколи.

**Тема 5.** Реалізація симетричних криптографічних систем.

**Тема 6.** Реалізація асиметричних криптографічних систем.

**Тема 7.** Системні питання реалізації програмних засобів, які використовують криптографічні методи захисту інформації.

## 4. Навчальні матеріали та ресурси

### Базова література.

1. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія: Підручник. – Київ: 2002. – 504 с
2. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998.- 248 с.
3. Koblitz N. A course in number theory and cryptography.- N.Y.: Springer-Verlag, 1987. – 312 p.
4. Goldreich O. Foundation of cryptography (fragments of a book).-1995.
5. Кос С.К. High-speed RSA implementation /Technical report TR 201 RSA Laboratories, november, 1994.
6. Кос С.К. RSA hardware implementation /Technical report RSA Laboratories, august, 1995.
7. Goldwasser S., Bellare M. Lecture notes on cryptography. – 1997.
8. Bellare M., Rogaway P. Optimal asymmetric encryption – how to encrypt with RSA / Advances in cryptology-Eurocrypt94 proceedings, LNCS.-V.950.-A.De Santis ed., Springer-Verlag, 1994.

### • Навчальний контент

## 5. Методика опанування навчальної дисципліни (освітнього компонента)

Найменування розділів, тем	Розподіл за видами занять				
	Разом	Лекц.	Лабораторні роботи	МКР	СРС в т.ч. МКР
<b>Тема 1.</b> Теоретичні моделі симетричних криптографічних систем.	10	6			4

<i>Тема 2. Теоретичні моделі асиметричних криптографічних систем.</i>	14	6	4		4
<i>Тема 3. Системи управління ключами.</i>	18	10			8
<i>Тема 4. Криптографічні протоколи.</i>	10	4	4		2
<i>Тема 5. Реалізація симетричних криптографічних систем.</i>	6	2			4
<i>Тема 6. Реалізація асиметричних криптографічних систем.</i>	14	6	4		4
<i>Тема 7. Системні питання реалізації програмних засобів, які використовують криптографічні методи захисту інформації.</i>	10	2	6		2
<i>Підготовка до іспиту</i>	36				38
<b><i>Разом в семестрі:</i></b>	<b>120</b>	<b>36</b>	<b>18</b>	<b>2</b>	<b>66</b>

## 6. Самостійна робота студента/аспіранта

Самостійна робота студента складається з:

- підготовки до МКР та іспиту шляхом опанування лекційного матеріалу,
- підготовки до захисту лабораторних робіт.

	<i>Вид самостійної роботи</i>	<i>Кількість годин СРС</i>
	<i>Підготовка до лекційних занять</i>	7
	<i>Підготовка до лабораторних робіт</i>	20
	<i>Підготовка до МКР</i>	14
	<i>Підготовка до іспиту</i>	25
		<b>66</b>

## ● Політика та контроль

### 7. Політика навчальної дисципліни (освітнього компонента)

- **Порушення термінів виконання завдань та заохочувальні бали**

<i>Заохочувальні бали</i>	<i>Штрафні бали</i>
---------------------------	---------------------

<i>Критерій</i>	<i>Ваговий бал, додається до рейтингу</i>	<i>Критерій</i>	<i>Ваговий бал, віднімається від базового балу</i>
<i>Активність на заняттях</i>	<i>+2 бали</i>		

- **Відвідування занять**

*Відвідування лекцій, практичних 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. В разі великої кількості пропусків студент може бути недопущений до іспиту, якщо не встигне виконати навчальний план по лабораторних роботах та МКР.*

- **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**

<i>№ з/п</i>	<i>Контрольний захід</i>	<i>Максимальна кількість балів</i>	<i>Кількість</i>	<i>Всього</i>
<i>1.</i>	<i>МКР</i>	<i>20</i>	<i>1</i>	<i>20</i>
<i>2.</i>	<i>Лабораторні роботи</i>	<i>10</i>	<i>4</i>	<i>40</i>
<i>3.</i>	<i>Іспит</i>	<i>40</i>	<i>1</i>	<i>40</i>
	<i>Всього</i>			<i>100</i>

- **Умови допуску до іспиту**

<i>Обов'язкова умова допуску до екзамену</i>	<i>Критерій</i>
--	-----------------

<i>Поточний рейтинг</i>	<i><math>RD \geq 36</math></i>
<i>Модульна контрольна робота</i>	<i>Набрано не менше 12 балів</i>
<i>Лабораторні роботи</i>	<i>Виконано 4 лабораторних роботи, за кожну лабораторну роботу отримано не менше ніж 6 балів</i>

● **Таблиця переведення рейтингових балів до оцінок за університетською шкалою<sup>2</sup>**

<i>Кількість балів</i>	<i>Оцінка за університетською шкалою</i>	<i>Можливість отримання оцінки «автоматом»</i>
<i>100-95</i>	<i>Відмінно</i>	<i>-</i>
<i>94-85</i>	<i>Дуже добре</i>	<i>-</i>
<i>84-75</i>	<i>Добре</i>	<i>-</i>
<i>74-65</i>	<i>Задовільно</i>	<i>-</i>
<i>64-60</i>	<i>Достатньо</i>	<i>+</i>
<i>Менше 60</i>	<i>Незадовільно</i>	<i>-</i>
<i>Не виконані умови допуску</i>	<i>Не допущено</i>	<i>-</i>

● **Іспит**

Підсумковим контролем є іспит. У цьому разі рейтингова оцінка роботи за семестр складається з результатів роботи в семестрі (RD) (в рамках 60 балів). На іспиті студент одержує білет, в якому містяться два теоретичних питання, кожне з яких оцінюється на 10 балів та практична задача, правильний та повний розв'язок якої оцінюється на 20 балів, відповідно повні та правильні розв'язки всіх завдань білету оцінюються в 40 балів.

**9. Додаткова інформація з дисципліни (освітнього компонента)**

- Сертифікати проходження дистанційних чи онлайн курсів за відповідною тематикою можуть бути зараховані, якщо в програмі курсу розглянуто всі питання, які входять до змісту навчальної дисципліни (п.3) ;

- Перелік питань до іспиту повністю відповідає змісту дисципліни.

Нижче наведений орієнтовний перелік теоретичних питань до іспиту. Цей перелік може корегуватись якщо якісь теми були зменшені або збільшені в обсязі.

1. Класифікація підходів для оцінки стійкості криптосистем. Стійкість у теоретико-інформаційному сенсі.
2. Модель стійкості криптографічних систем Шенона. Теорема про необхідну і достатню умову для досконалої стійкості криптосистеми. Поняття ідеально стійких криптосистем.

<sup>2</sup> Оцінювання результатів навчання здійснюється за рейтинговою системою оцінювання відповідно до рекомендацій Методичної ради КПІ ім. Ігоря Сікорського, ухвалених протоколом №7 від 29.03.2018 року.

3. Припущення, прийняті в моделі Шенона. Адекватність моделі реальним системам зв'язку та обробки інформації з обмеженим доступом.
4. Відстань однозначності. Висновки із формули для відстані однозначності.
5. Модель стійкості секретних систем Вайнера та прийняті у ній припущення. Адекватність реальних систем зв'язку.
6. Модель стійкості секретних систем Маурера та прийняті у ній припущення. Адекватність реальних систем зв'язку.
7. Теоретико-складносний підхід до оцінки стійкості криптосистем. Основні поняття теорії складності алгоритмів. Моделі обчислень. Найпростіша модель обчислень: машина Тюрінга.
8. Ієрархія класів обчислювальної складності алгоритмів.
9. Необхідні та достатні умови існування криптосистем, стійких у теоретико-складносному сенсі. Поняття про односторонні функції та односторонні функції «з лазівкою». "Кандидати" в односпрямовані функції.
10. Загальні моделі стійкості асиметричних систем. Проблеми, що виникають під час спроби побудови моделі стійкості асиметричних криптосистем. Поняття про доведену стійкість асиметричних криптосистем.
11. Формальне визначення асиметричної криптосистеми.
12. Формальні визначення стійкості асиметричних криптосистем. Асиметричні криптосистеми, стійкі у сенсі визначення поліноміальної нерозрізненності.
13. Асиметричні криптосистеми, стійкі у сенсі визначення «семантичної секретності». Відмінності між асиметричними криптосистемами, стійкими у сенсі визначення «поліноміальної нерозрізненності» та «семантичної секретності».
14. Поняття про односторонні предикати «з лазівкою» (trapdoor predicates) та ядра односторонніх функцій «з лазівкою» (hard core predicates). Доказ адекватності "побітової" моделі шифрування.
15. Модель імовірнісного шифрування та її реалізація.
16. Optimal asymmetric encryption та її практичні реалізації. Парадигма ідеальної хеш-функції.
17. Генерація довготривалих ключових параметрів для асиметричних криптосистем. Вимоги до ключових параметрів асиметричних криптосистем, стійкість яких базується на задачах факторизації та дискретного логарифмування. Визначення "сильних" простих чисел.
18. Алгоритми тестування чисел на простоту та їх обчислювальна складність.
19. Алгоритми генерації простих та «сильних» простих чисел.
20. Життєвий цикл ключових даних. Завдання керування ключами.
21. Методи поширення ключів та їх характеристики.
22. Методи ефективною реалізації асиметричних криптосистем, що використовують операції у мультиплікативній групі кінцевого поля. Алгоритми множення для "програмної" моделі обчислення.
23. Алгоритм множення Карацуби-Оффмана та його обчислювальна складність.
24. Алгоритми множення для апаратної моделі обчислення.

25. Алгоритми обчислення залишку від розподілу за модулем простого числа або складового числа, що не має ефективного алгоритму розкладання на прості дільники. Класичний алгоритм та його обчислювальна складність.
26. Алгоритми обчислення залишку від розподілу за модулем простого числа або складового числа, що не має ефективного алгоритму розкладання на прості дільники. Алгоритм Баррета та його обчислювальна складність.
27. Алгоритм множення Монтгомері та його обчислювальна складність.
28. Алгоритми обчислення залишку від розподілу за модулем складового числа, розкладання на прості дільники якого відоме. Китайська теорема про залишки.
29. Алгоритми зведення у ступінь за модулем. Бінарний метод.
30. Алгоритми зведення у ступінь за модулем.  $t$ -арний метод.
31. Атаки за сторонніми каналами.
32. Криптографічні інтерфейси фірми Microsoft (Microsoft CryptoAPI) та RSA Data Security (PKCS # 11).
33. Вимоги щодо безпечної реалізації криптографічних модулів згідно з FIPS 140-2.

### **Лабораторні роботи**

Цикл лабораторних робіт дозволяє студентам придбати такі навички та уміння:

- реалізація бібліотеки арифметичних операцій з багато розрядними числами над полем натуральних чисел та скінченими полями чи групами;
- практичне тестування багато розрядних чисел на належність до класу простих чисел та отримання багато розрядних простих чисел;
- практичну реалізацію криптографічних протоколів;
- розробку програмної реалізації обраної криптосистеми.

#### **Лабораторна робота № 1.**

Тема: „Реалізація алгоритмів арифметики великих чисел (багатократної точності) над скінченими полями та групами”.

#### **Лабораторна робота № 2.**

Тема: Реалізація алгоритмів генерації ключів гібридних криптосистем.

#### **Лабораторна робота № 3.**

Тема: Реалізація основних асиметричних криптосистем.

#### **Лабораторна робота № 4.**

Тема: Дослідження особливостей реалізації існуючих програмних систем, які використовують криптографічні механізми захисту інформації.

### **Робочу програму навчальної дисципліни (силабус):**

Складено професором кафедри ММЗІ, д.т.н., с.н.с. Кудін Антон Михайлович

Ухвалено кафедрою ММЗІ (протокол № 19 від 22.06.2024 р.)

**Погоджено** Методичною комісією НН ФТІ (протокол № 6 від 27.06.2022)