ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні методи криптології

першого (бакалаврського) рівня вищої освіти

м. Кропивницький

1. Загальна інформація

Назва дисципліни	**Математичні методи криптології**
Викладач	Лисенко Ірина Анатоліївна, кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/lysenko-irina/ https://scholar.google.com.ua/citations?user=b5TXV7EAAAAJ&hl=ru&authuser=2 https://orcid.org/0000-0003-4394-4960
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20}
E-mail:	lisenkoia@kntu.kr.ua
Консультації	*Очні консультації* згідно до затвердженого розкладу консультацій. *Онлайн консультації* засобами електронної пошти, месенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні

2. Анотація дисципліни

Дисципліна «Математичні методи криптології» призначена для набуття теоретичних знань та практичних навичок розв'язання задач додаткових розділів математики, які не входять до курсу вищої математики, але використовуються у криптографічних засобах захисту інформації. В курсі розглядаються основи теорії чисел, абстрактної алгебри (теорія груп та скінченних полів) та теорія еліптичних кривих. В якості ілюстрації наводяться деякі основні алгоритми асиметричної криптографії.

3. Мета і завдання дисципліни

Метою викладання дисципліни «Математичні методи криптології» є набуття здобувачами вищої освіти знань основи алгебри множин, порівнянь, обчислень за модулем, елементі теорії чисел, алгебраїчних структур (підгрупи, групи, кільця, поля) та їх властивостей, еліптичних кривих та формування навичок розв'язання задач і побудови алгоритмів на основі теорії чисел, скінченних полів та еліптичних кривих для використання в криптографічних застосуваннях.

Основними **завданнями** вивчення дисципліни є формування наступних компетенцій:

– Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та кібербезпеки.

– Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

5. Результати навчання

У результаті вивчення дисципліни студент повинен забезпечити наступні **програмні результати навчання**:

– Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

– Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	**Денна форма навчання**	**Заочна форма навчання**
	Кількість годин	**Кількість годин**
Кількість кредитів / годин	4/120	4/120
Кількість змістових модулів	2	2
Нормативна / вибіркова	вибіркова	вибіркова
Вид підсумкового контролю : залік	0	0

7. Технічне і програмне забезпечення / обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд. 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти.

8. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.
Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

9. Програма навчальної дисципліни

Тема 1. Вступ. Множини, відношення, функції.
Множини. Відношення. Відношення еквівалентності.
Тема 2. Основи теорії подільності цілих чисел.
Позиційна система. числення. Прості числа. Факторизація чисел. Прості числа. Взаємно прості числа. Функція Ейлера. Найбільший спільний дільник двох чисел і алгоритм Евкліда. Найменше спільне кратне. Розширений алгоритм
Евкліда
Тема 3. Порівняння. Класи лишків.
Повна та зведена система лишків. Теорема Ейлера та теорема Ферма. Модулярні арифметичні операції.
Тема 4. Розв'язання порівнянь першого степеня та систем порівнянь.
Мультиплікативні обернені за модулем. Китайська теорема про залишки. Алгоритм Рівеста-Штайна-Адельмана
Тема 5. Квадратичні порівняння.
Символ Лежандра. Символ Якобі. Квадратичні порівняння за складеним модулем.
Тема 6. Первісні корені. Індекси (дискретні логарифми).
Експонента. Первісні корені. Індекси за модулями p^n, 2p^n
Тема 7. Основи алгебри.
Групи. Підгрупи. Абелеві групи. Циклічні групи. Гомоморфізми груп. Нормальні групи. Класи суміжності. Фактор-групи. Теорема Лагранжа

Тема 8. Кільця. Поля.
Кільце поліномів. Ідеали.
Тема 9. Скінченні поля.
Скінченні розширення полів. Скінченні поля. Поля незвідних многочленів. Будова скінченних полів. Мінімальні многочлени. Ізоморфізми скінченних полів
Тема 10. Основні алгоритми для скінченних полів.
Алгоритм Евкліда для многочленів. Розширений алгоритм Евкліда для многочленів. Мультиплікативні обернені. Модулярний степінь для многочленів. Тестування на незвідність.
Тема 11. Еліптичні криві. Класифікація еліптичних кривих.
Еліптичні криві над полем дійсних чисел. Додавання точок еліптичної кривої. Абелева група точок. Порядок групи і порядок точки
Тема 12. Властивості еліптичних кривих.
Проективні координати. Стистнення точок. Дискримінант та j-інваріант еліптичної кривої
Тема 13. Еліптичні криві над простими полями Галуа p>3 та над розширеними полями характеристики 2.
Межі Хассе для порядку кривої. Побудова кривої із заданим порядком. Методи розв'язання проблеми дискретного логарифмування в групі точок еліптичної кривої
Тема 14. Поняття про квантові комп'ютери та квантову криптографію.

10. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: залік.

Контроль знань і умінь (поточний і підсумковий) з дисципліни « Математичні методи криптології » здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних робіт), для оцінювання якої призначається 100 балів, та заліку.

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, лабораторні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті:

11. Рекомендована література

Базова

1. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел: Навч. посібник – К.: ДУІКТ, 2006. – 126 с.
2. Смарт Н. Криптографія. М.: Техносфера, 2005. – 528 с.
3. Бессалов А.В., Телиженко А.Б. Криптосистеми на еліптичних кривих: навч. посібник. – К.: ІВЦ «Політехніка», 2004. – 224 с.

Допоміжна

4. Клесов О.І. Елементарна теорія чисел та елементи криптографії: Підручник. – Київ: ТВіМС, 2016. – 393 с.
5. Математичні основи криптоаналізу: навч. посіб. / С. О. Сушко, Г. В. Кузнецов, Л. Я. Фомичова, А. В. Корабльов; – Дніпропетровськ: НГУ, 2010. - 465 с.
6. A Course in Number Theory and Cryptography by Neal Koblitz. 2nd ed. New York, USA : Springer, 2012. 235 p.

Інформаційні ресурси

7. Курс "Математичні методи криптології" в системі дистанційної освіти ЦНТУ Moodle. Режим доступу: http://moodle.kntu.kr.ua/course/view.php?id=650