Силабус освітнього компонента
Програма навчальної дисципліни

Основи криптології

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп`ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Вибіркова

Семестр
5

Мова викладання
Українська

Викладачі, розробники

Мілов Олександр Володимирович

oleksandr.milov@khpi.edu.ua
Доктор технічних наук, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж» , «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «Методологія наукової та педагогічної діяльності в науках кіберзахисту» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Основи криптології " є вибірковою навчальною дисципліною. Вивчення дисципліни дає уявлення про основні математичні методи та підходи, що застосовуються для забезпечення криптографічного захисту інформації в процесі зберігання та передачі інформації, представленої в двійкових кодах. Дисципліна присвячена вивченню математичних основ криптології та криптографічного аналізу, що застосовуються до захисту інформації в інформаційних системах. Дисципліна розкриває поняття шифрів, симетричної та асиметричної криптографії, електронного підпису, гешування та інші математичні об'єкти криптографії. Вивчаються відповідні криптографічні стандарти, що застосовуються сьогодні в захисті інформації в Україні та за кордоном.

Мета та цілі дисципліни

Ознайомлення з математичними основами криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних

моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК 1. Здатність учитися й оволодівати сучасними знаннями.
ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
ЗК 5. Здатність проведення досліджень на відповідному рівні.
ЗК 7. Здатність до пошуку, оброблення й аналізу інформації з різноманітних джерел.
ЗК 8. Знання і розуміння предметної області та розуміння професійної діяльності.
ЗК 10. Навички у використанні інформаційних і комунікаційних технологій.
СК 1. Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.
СК 2. Здатність виконувати завдання, сформульовані у математичній формі.
СК 3. Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проєктування, керування, прогнозування, прийняття рішень.
СК 5. Здатність розробляти алгоритми та структури даних, програмні засоби та програмну документацію.
СК 6. Здатність проєктувати бази даних, інформаційні системи та ресурси.
СК 7. Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, із використанням стандартних офісних додатків.
СК 14. Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.
СК 18. Здатність обирати та застосовувати математичні моделі та методи для статистичного та інтелектуального аналізу даних в умовах невизначеності.

Результати навчання

РН 1. Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.
РН 6. Володіти основними методами розробки дискретних і неперервних математичних моделей об'єктів та процесів, аналітичного дослідження цих моделей на предмет існування та єдиності їх розв'язку.
РН 8. Поєднувати методи математичного та комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень.
РН 10. Володіти методиками вибору раціональних методів та алгоритмів розв'язання математичних задач оптимізації, дослідження операцій, оптимального керування і прийняття рішень, аналізу даних.
РН 13. Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики.
РН 14. Виявляти здатність до самонавчання та продовження професійного розвитку.
РН 24. Вміти застосовувати існуючі та розробляти нові алгоритми і програмні засоби обробки даних вимірювань та спостережень, текстів, сигналів та зображень.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 30 год., лабораторні роботи – 30 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

«Математичний аналіз», «Лінійна алгебра», «Теорія ймовірностей», «Дискретні структури і структури даних», «Алгоритмізація та програмування».

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи..

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ. Цілі та завдання навчальної дисципліни «Математичні основи криптології ».
Місце дисципліни у навчальному процесі. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.
Тема 2. Основні поняття криптології.
Основні поняття криптології та криптоаналізу: криптографічне перетворення інформації, відправник та одержувач інформації, канал зв'язку, відкрите повідомлення, криптографічний ключ, процеси шифрування та розшифрування, криптограма, криптографічна система, противник та його атаки. Методи криптографічного захисту інформації та роль криптографії у забезпеченні безпеки інформації. Основні завдання криптографії: забезпечення встановленого режиму доступу інформації, забезпечення цілісності інформації, аутентифікація автора повідомлення.
Тема 3. Модульна арифметика.
Арифметика цілих чисел. Множина цілих чисел: бінарні операції, розподіл цілих чисел, два обмеження, граф рівняння поділу.Теорія подільності. Властивості. Всі подільники. Найбільший спільний дільник. Алгоритм Евкліда. Розширений алгоритм Евкліда. Лінійні діофантові рівняння. Частне рішення. Загальні рішення. Модульна арифметика. Операції по модулю.
Система відрахувань: Zn. Порівняння. Система відрахувань. Кругова система позначень. Операції в Zn. Властивості. Інверсії. Адитивна інверсія. Мультиплікативна інверсія. Додавання і множення таблиць. Різні множини для додавання і множення.
Тема 4. Матриці.
Визначення. Операції і рівняння. Рівність. Складання і віднімання. Множення. Скалярний множення. Детермінант. Інверсії. Адитивна інверсія. Мультиплікативна інверсія. Матриці відрахувань. Порівняння. Лінійне рівняння. Лінійні рівняння з одним невідомим, що містять порівняння. Система лінійних рівнянь, що містять порівняння.
Тема 5. Прості шифри.
Категорії простих шифрів. Шифри підстановки. Моноалфавітні шифри. Адитивний шифр. Шифр зсуву. Шифр Цезаря. Мультиплікативні шифри. Моноалфавітни шифр підстановки. Багатоалфавітні шифри. Автоключевий шифр. Шифр Плейфера. Шифр Віженера. Шифр Хілла. Одноразовий блокнот. Роторний шифр. Машина "Енігма". Кодова книга - довідник шифрів. Шифри перестановки. Шифри перестановки без використання ключа. Ключові шифри перестановки. Об'єднання двох підходів. Ключі. Використання матриць. Шифри с подвійною перестановкою.
Тема 6. Алгебраїчні структури.
Групи. Поле. Поля GF(2n). Поліноми. Операції. Модуль. Додавання. Множення. Множення, що використовує комп'ютер. Використання генератора. Інверсії. Адитивні інверсії. Мультиплікативні інверсії. Додавання і віднімання. Множення і ділення.
Тема 7. Сучасні блокові шифри.
Підстановка, або транспозиція. Блокові шифри як групові математичні перестановки. Повнорозмірні ключові шифри. Шифри ключа часткового розміру. Шифри без ключа. Компоненти сучасного блокового шифру. S-блоки. Циклічний зсув. Заміна. Розбиття і об'єднання. Складові шифри. Розсіювання і перемішування. Раунди. Два класу складових шифрів. Мережа Файстеля.
Тема 8. DES.
Загальні положення. Структура DES. Початкові і кінцеві перестановки. Раунди. Функція DES. Генерація ключів. Видалення бітів перевірки. Зсув вліво. Перестановка стиснення. Аналіз DES. S-блоки. P-блоки. Число раундів. Слабкості DES. Слабкість в ключі шифру. Багаторазове

застосування DES. Дворазовий DES. Триразовий DES. Триразовий DES з двома ключами. Триразовий DES з трьома ключами.

Тема 9. Стандарт щифрування за ГОСТ 28147-89.

Принципи побудови алгоритму шифрування. Основний крок та базові цикли криптоперетворень за ГОСТ 28147-89. Режими та схеми роботи режимів шифрування за ГОСТ 28147-89.

Тема 10. Шифр AES.

Критерії. Безпека. Вартість. Реалізація. Раунди. Одиниці даних. Біт. Байт. Слово. Блок. Матриця станів. Структура кожного раунду. Підстановка. SubBytes. InvSubBytes. Перетворення з використанням поля GF. Нелінійність. Перестановка. ShiftRows. InvShiftRows. Змішування. MixColumns. InvMixColumns. Додавання ключів. AddRoundKey. Розширення ключів в AES-128. RotWord. SubWord. RoundConstants. Алгоритм. Розширення ключа в AES-192 і AES-256. Аналіз розширення ключа.

Тема 11. Шифр “Калина -256”.

Структура алгоритму шифрування. Режими та схеми роботи режимів шифрування за “Калина - 256”. Показники безпекаи, оперативності. Вартість. Реалізація. Раунди.

Тема 12. Прості числа.

Визначення. Взаємно прості числа. Кількість простих чисел. Число простих чисел. Число простих чисел, менших n. Перевірка на просте число. Решето Ератосфена. Phi-функція Ейлера. Мала теорема Ферма. Перша версія. Друга версія. Додатки. Теорема Ейлера. Перша версія. Друга версія. Додатки. Генерація простих чисел. Прості числа Мерсенна. Прості числа Ферма. Випробування простоти чисел. Детерміновані алгоритми. Алгоритм теорії подільності. AKS-алгоритм. Імовірнісні алгоритми. Тест Ферма. Випробування квадратним коренем. Тест Міллера-Рабіна. Ініціалізація. Рекомендовані тести простоти чисел. Розкладання на множники. Основна теорема арифметики. Найбільший спільний дільник. Найменше спільне кратне. Методи розкладання на множники. Метод перевірки розподілом. Метод Ферма. Метод Полларда. PB (Rho) - метод Полларда. Більш ефективні методи. Квадратичне решето. Решето поля чисел. Інші проблеми. Китайська теорема про залишки.

Тема 13. Квадратичне порівняння з модулем.

Квадратичне порівняння з модулем у вигляді простого числа. Квадратичні відрахування і невирахування. Критерій Ейлера. Рішення квадратичного порівняння з модулем у вигляді простого числа. Квадратичне порівняння по складеному модулю. Складність.

Піднесення до ступеню і логарифми. Швидке піднесення в ступінь. Логарифм. Повний перебір. Дискретний логарифм. Рішення модульного логарифма з використанням дискретних логарифмів.

Тема 14. Криптографічні геш-функції.

Цілісність повідомлення. Функції гешування та цілісність даних. Вимоги до функцій гешування. Випадкова модель Oracle. Ітеративна геш-функція (схема Меркеля-Дамгарда). Дайджест повідомлення (MD). Алгоритм безпечного гешування (SHA).

Геш-функції, засновані на блочних шифрах (схема Рабіна, схема Міагучі-Пренеля. SHA-512. Whirlpool. Геш-алгоритм “Купина-256”.

Тема 15. Криптографічна система RSA.

Вступ. Ключі. Загальна ідея. Оригінальний текст / зашифрований текст. Шифрування / дешифрування. Потреба в обох криптосистемах. "Лазівка" в односторонньої функції. Функції. Ранцева криптосистема. Визначення. Суперзбільшення кортежу. Секретна зв'язок з використанням ранця. Генерація ключів. Шифрація. Дешифрація. Лазівка. Криптографічний система RSA. Введення. Процедура. Дві алгебраїчні структури. Генерація ключів. Шифрування. Дешифрування. Деякі тривіальні приклади.

Тема 16. Криптосистемы Рабина и Эль-Гамаля. Алгоритм Диффи-Хеллмана.

Процедура. Генерація ключів. Шифрування. Дешифрування. Безпека криптографічної системи Рабина. Криптографічна система Ель-Гамаля. Процедура. Генерація ключів. Шифрування. Дешифрування. Аналіз безпеки криптосистеми Ель-Гамаля. Атаки малого модуля. Атака знання вихідного тексту. Алгоритм Диффи-Хеллмана.

Тема 17. Криптосистеми на основі методу еліптичних кривих.

Рівняння еліптичної кривої. Сингулярні та несингулярні криві. Операції з точками. Використання еліптичних кривих у криптографії. Еліптичні криві в дійсних числах. Абелева група. Група і поле. Еліптичні криві в GF(p). Знаходження інверсії. Знаходження точок на кривій. Складання двох точок. Множення точки на константу. Еліптичні криві в GF. Криптографія еліптичної кривої, що моделює криптосистему Ель-Гамаля. Генерація загальнодоступних і приватних ключів.

Шифрування. Дешифрування. Порівняння. Безпека методу з використанням еліптичної кривої. Розмір модуля.

Тема 18. Цифровий підпис.

Концепція цифрового підпису. Процес цифрового підпису. Служби безпеки, забезпечені цифровим підписом. Атаки цифрових підписів. Схеми цифрового підпису (RSA, Ель-Гамаль, Шнора, DSS, еліптичної кривої). Програми цифрового підпису.

Тема 19. Псевдовипадкові числа у криптографії.

Переваги та перспективи використання потокових систем шифрування. Використання випадкових чисел (випадковість, непередбачуваність). Джерела випадкових чисел. Генератори псевдовипадкових чисел: циклічне шифрування, режим зворотного зв'язку після виходу, генератор псевдовипадкових чисел ANSI X9.17, генератор BBS, лінійно-конгруентний метод, метод Фібоначі з затримкою. Перевірка якості роботи генератора псевдовипадкових чисел. Послідовності максимальної довжини. Аналіз псевдовипадкових послідовностей.

Тема 20. Криптоаналіз.

Принципи Керкгоффса. Криптоаналіз. Загальні методи криптоаналізу: метод грубої сили, компроміси час-простір, веселкові таблиці, атаки слайдів, криптоаналіз хеш-функцій, криптоаналіз генераторів випадкових чисел. Лінійний криптоаналіз. Загальний огляд. Алгоритми Мацуї. Лінійні вирази для S-боксів. Лема Мацуї про нагромадження. Шифр Easy1 Лінійні вирази та відновлення ключів. Лінійний криптоаналіз DES. Множинні лінійні наближення. Знаходження лінійних виразів. Код лінійного криптоаналізу. Диференціальний криптоаналіз. Загальлний огляд. Позначення. Диференціали S-Box. Поєднання характеристик S-Box. Виведення ключа. Код диференціального криптоаналізу. Диференціальний криптоаналіз шифрів Фейстеля. Диференціально-лінійний криптоаналіз. Умовні характеристики. Диференціали вищого порядку. Усічені диференціали. Неможливі диференціали. Атака бумеранга. Інтерполяційна атака. Атака пов'язаних ключів.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Знайомство с оболонкою виконання лабораторних робіт з криптології. Інструменти підготовки інформації для виконання лабораторних робіт.
Тема 2. Дослідження сучасних блочних симетричних шифрів та режимів шифрування.
Тема 3. Шифрування та дешифрування у шифрах підстановки та перестановки. Шифрування та дешифрування у роторних машинах «Енігма».
Тема 4. Дослідження сучасних блочних симетричних шифрів та режимів шифрування. Дослідження сучасних асиметричних криптосистем шифрування.
Тема 5. Виконання криптографічних перетворювань у DES. Генерація ключей у DES.
Тема 6. Виконання криптографічних перетворювань у AES. Генерація ключей у AES.
Тема 7. Генерування та дослідження геш-функцій.
Тема 8. Генерація ключів в системі RSA. Шифрування та дешифрування. Використання та дослідження криптосистем Рабина, Ель-Гамаля та алгоритма Диффі Хеллмана.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт та іспиту.

.

Література та навчальні матеріали

Основна література:

1. Євсеєв С. П. Кібербезпека: Криптографія з Python: навчальний посібник. – Львів “Новий світ-2000”, 2021. – 120 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

2. Євсеєв С. П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів “Новий світ-2000”, 2020. – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
3. Євсеєв С. П. Кібербезпека: сучасні технології захисту. / Євсеєв С. П, Остапов С. Е., Король О. Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678 с.
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
4. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
5. Євсеєв С. П. Кібербезпека: основи кодування та криптографії/ С. П. Євсеєв, О. В. Мілов, С. Е. Остапов, О. В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Додаткова література :

6. Євсеєв С. П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів “Новий світ-2000”, 2020. – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Бобало Ю. Я., Горбатий І. В. (ред.) Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с. – ISBN 978-966-941-339-0
http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- іспит: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.

Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	Дата погодження, підпис 28.08.2023 р.		Завідувач кафедри Сергій ЄВСЕЄВ
	Дата погодження, підпис 31.08.2023 р.		Гарант ОП Олена АХІЄЗЕР