Силабус освітнього компонента
Програма навчальної дисципліни

Математичні основи криптології

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
3

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 "Математичні основи криптології" є обов'язковою 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

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Математичний аналіз, Лінійна алгебра, Теорія ймовірностей і математична статистика, Дискретна математика, Інформатика, Програмування, Правове регулювання кібербезпеки.

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, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

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. http://kist.ntu.edu.ua/textPhD/tzi.pdf.
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

28.08.2024

Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024

Гарант ОП
Роман КОРОЛЬОВ