Силабус освітнього компонента
Програма навчальної дисципліни

Прикладна криптологія

Шифр та назва спеціальності
123 – Комп’ютерна інженерія

Інститут
ННІ Комп'ютерних наук та інформаційних технологій

Освітня програма
Сучасне програмування, мобільні пристрої та комп'ютерні ігри

Кафедра
Комп’ютерна інженерія та програмування (326)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Вибіркова

Семестр
8

Мова викладання
Українська

Викладачі, розробники

Поворознюк Оксана Анатоліївна
Oksana.Povorozniuk@khpi.edu.ua
Кандидат технічних наук, доцент кафедри «КІП» НТУ «ХПІ»

Автор понад 80 наукових та науково-методичних праць. Провідний лектор з дисциплін: «Прикладна криптологія», «Управління інформаційною безпекою», «Основи наукових досліджень», «Computer architecture» та «Signal and Image Processing».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна спрямована на розгляд основних понять криптології, класичних криптосистем та методів їх криптоаналізу, вивчення основних алгоритмів симетричної та асиметричної криптографії, алгоритмів хешування та цифрового підпису, а також елементів криптографії на еліптичних кривих.

Мета та цілі дисципліни

Формування загальних принципів побудови систем криптографічного захисту інформації (систем шифрування) на основі використання сучасних алгоритмів симетричного й асиметричного шифрування для забезпечення конфіденційності даних в інформаційно-телекомунікаційній системі, отримання знань та навичок практичного застосування прийомів та методів криптографічного захисту інформації.

Формат занять

Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

ФК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.
ФК7. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема, з метою підвищення їх ефективності.

Результати навчання

ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж
ПРН8. Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей.
ПРН 11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредитів ECTS): лекції – 24 год., практичні заняття – 24 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно мати знання та практичні навички з наступних дисциплін: «Вища математика», «Алгебра програмування», «Програмування», «Теорія інформації та кодування».

Особливості дисципліни, методи та технології навчання

На лекційних заняттях викладання матеріалу здійснюється в усній формі із демонстрацією презентацій. Методи навчання: лекція-бесіда, лекція-візуалізація, навчальна дискусія, мозкова атака, кейс-метод, метод порівняння, метод узагальнення, метод конкретизації, метод відокремлення основного, обговорення, робота над помилками.
На практичних заняттях студенти виконують та демонструють індивідуальні завдання.
Під час самостійної роботи вдома студенти коректують свої індивідуальні завдання а також вивчають теми та питання, які не викладаються на лекційних заняттях.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Основні поняття та визначення. Класичні шифри та їх криптоаналіз
1.1 Вступ. Предмет курсу та його задачі. Структура, зміст дисципліни, його зв`язок з іншими дисциплінами та місце у підготовці інженера даного фаху.
1.2 Основні поняття криптології
1.3 Класичні алгоритми шифрування. Шифри Цезаря, Віженера, частоколу, Плейфера, криптосистема Хілла.
1.4 Основи криптоаналізу класичних шифрів. Частотний криптоаналіз, метод Казіскі та метод Фрідмана.
Тема 2. Симетричні криптографічні системи.
2.1 Потокові симетричні шифри. Шифр одноразового блокноту, потоковий шифр RC4, генератори псевдовипадкових послідовностей.
2.2 Блокові симетричні шифри. Алгоритм DES, алгоритм IDEA, удосконалений стандарт шифрування AES, національний стандарт шифрування ДСТУ 7624:2014. Режими роботи блокових симетричних шифрів
Тема 3. Асиметричні криптографічні системи.

3.1 Криптосистеми з відкритим ключем. Криптосистема Меркла-Хелмана, алгоритм шифрування RSA, алгоритм шифрування Ель-Гамаля, алгоритм обміну ключами Діффі-Хелмана
3.2 Криптографічні хеш-функції. Поняття та властивості хеш-функцій. Хеш-функція SHA-256, хеш-функція «Купина» (ДСТУ 7564:2014)
3.3 Цифровий підпис. Алгоритм цифрового підпису RSA, алгоритм цифрового підпису Ель-Гамаля, стандарт цифрового підпису DSS
3.4 Основи криптографії на еліптичних кривих. Операції над точками еліптичних кривих. Алгоритм Діффі-Хелмана на еліптичних кривих. Стандарт цифрового підпису ECDSS

Теми практичних занять

Тема 1. Класичні алгоритми шифрування (Цезаря, Віженера та частоколу).
Шифрування та дешифрування тексту використовуючи шифри Цезаря, Віженера та частоколу згідно з інд. завданням.
Тема 2. Класичні алгоритми шифрування (шифр Плейфера, криптосистема Хілла)
Шифрування та дешифрування тексту використовуючи шифр Плейфера та криптосистему Хілла згідно з інд. завданням.
Тема 3. Криптоаналіз класичних шифрів
Відновлення зашифрованого тексту за допомогою частотного криптоаналізу згідно з інд. завданням.
Тема 4. Симетричні криптографічні системи (алгоритм DES)
Здійснення S-перетворення повідомлення з використанням алгоритма DES згідно з інд. завданням
Тема 5. Симетричні криптографічні системи (алгоритм AES)
Знаходження наступного слова ключа в алгоритмі AES, якщо дано ключ попереднього раунду
Тема 6. Криптосистеми з відкритим ключем (криптосистема Меркла-Хелмана)
Шифрування та дешифрування тексту використовуючи криптосистему Меркла-Хелмана.
Тема 7. Криптосистеми з відкритим ключем (алгоритм шифрування RSA)
Шифрування та дешифрування тексту використовуючи алгоритм шифрування RSA.
Тема 8. Криптосистеми з відкритим ключем (алгоритм шифрування Ель-Гамаля)
Шифрування та дешифрування тексту використовуючи алгоритм шифрування Ель-Гамаля.
Тема 9. Криптосистеми з відкритим ключем (алгоритм обміну ключами Діффі-Хелмана)
Визначення спільного секретного ключа, обчисленого абонентами у криптосистемі Діффі-Хеллмана.
Тема 10. Криптографічні хеш-функції та цифровий підпис
Формування ЦП хеш-значення повідомлення.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

Самостійна робота

Опрацьовування лекційного матеріалу.
Підготовка до практичних занять та модульних контролів.
Самостійне вивчення тем та питань, які не викладаються на лекційних заняттях: багатоалфавітні шифри підстановки, криптографічна система Рабіна, методи зламу криптографічних систем, заснованих на дискретному логарифмуванні, атака методом інтерполяцій, атака методом скорочених диференціалів, атака “Квадрат” .

Література та навчальні матеріали

Основна література

1. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
https://learn.ztu.edu.ua/pluginfile.php/264055/mod_resource/content/1/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97_%D0%9D%D0%90%D0%92%D0%A7%D0%90%D0%9B%D0%AC

%D0%9D%D0%98%D0%99_%D0%9F%D0%9E%D0%A1%D0%86%D0%91%D0%9D%D0%98%D0%9A.pdf
2. Н.О. Щур. Прикладна криптологія. Методичні рекомендації до виконання лабораторних робіт. – Житомир: Державний університет «Житомирська політехніка», 2021. – 104 с. https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053471.pdf
3. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с. http://eir.zntu.edu.ua/bitstream/123456789/6528/1/B09754.pdf
4. Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. https://er.nau.edu.ua/handle/NAU/32583
5. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/70560
6. Поворознюк А.І., Поворознюк О.А. Управління інформаційною безпекою: методичні вказівки до виконання практичних занять Харків: НТУ «ХПІ» -2023. – 123 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/70559
7. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтак. Ужгород: В-во УжНУ «Говерла», 2020. 28 с. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/37067/1/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%BA%D0%B0%20%D0%9A%D0%BB%D0%B0%D1%81%D0%B8%D1%87%D0%BD%D1%96%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8.pdf
8. Системи захисту інформації. Криптографія [Текст] : навч. посіб. / уклад. Б. Д. Шепетюк ; Чернівец. нац. ун-т ім. Юрія Федьковича. - Чернівці : ЧНУ ім. Юрія Федьковича : Рута, 2021. - 75 с. http://e-cat.scilib.chnu.edu.ua/cgi/irbis64r_12/cgiirbis_64.exe
9. Прикладна криптологія [Текст] : лаб. практикум для здобувачів вищ. освіти ОС "Бакалавр" спец. 125 "Кібербезпека" / [уклад. А. В. Ільєнко] ; Нац. авіац. ун-т. - Київ : НАУ, 2022. – 57 с http://e-cat.scilib.chnu.edu.ua/cgi/irbis64r_12/cgiirbis_64.exe

Додаткова література.

10. Інформаційні технології. Методи захисту. Легковагова криптографія [Текст]. - Київ : УкрНДНЦ, [20--] . - (Національний стандарт України).ДСТУ ISO/IEC 29192-5:2018 (ISO/IEC 29192-5:2016, IDT). Хеш-функції. - Чинний від 2020-01-01. - 2019. - V, 18 с. : рис., табл. - Бібліогр.: с. 18.
11. Інформаційні технології. Методи захисту. Алгоритми шифрування [Текст]. - Київ : УкрНДНЦ, [20--] . - (Національний стандарт України). Ч. 4 : ДСТУ ISO/IEC 18033-4:2015. Потокові шифри (ISO/IEC 18033-4:2011, IDT). - Чинний від 2017-01-01. - 2081. - IV, 76 с. : рис., табл. - Бібліогр.: с. 74-75.
12. Когут Ю. І. Корпоративна безпека: практичний посібник. Консалтингова компанія «СІДКОН», 2021. – 460 с.

Інформаційні ресурси в інтернеті.

Тематичні бази даних https://ufn.ru/en/articles.
Закордонні електронні наукові інформаційні ресурси: European Library. Вільний доступ до ресурсів 47 Національних бібліотек Європи, Австралії, Білорусії, Великої Британії, Німеччини, бібліотека коледжу Лондонського університету.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:
модульні контролі - 20 балів; практичні заняття - 60 балів; екзамен - 20 балів.

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 22.04.2024	Завідувач кафедри Олександр ЗАКОВОРОТНИЙ
	Дата погодження, підпис 22.04.2024	Гарант ОП Олександр ЗАКОВОРОТНИЙ