Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Системного програмування і спеціалізованих комп'ютерних систем

Комп'ютерна криптографія

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*123 Комп'ютерна інженерія*
Освітня програма	*ОПП Системне програмування і спеціалізовані комп'ютерні системи*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*5 курс, весняний семестр*
Обсяг дисципліни	*5 кредитів (150 годин)*
Семестровий контроль/ контрольні заходи	*Екзамен/ ДКР*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: к.т.н, с.н.с. Тесленко Олександр Кирилович,akirill766@ukr.net teslenko@scs.kpi.ua* *Лабораторні : к.т.н, с.н.с. Тесленко Олександр Кирилович*
Розміщення курсу	Лекції, лабораторні -на кафедральній системі дистанційного навчання https://scs-kpi.pp.ua/.

Програма навчальної дисципліни

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

Предмет дисципліни. Вивчення кредитного модуля «Комп'ютерна криптографія» дозволяє сформувати у студентів компетенції, необхідні для розв'язання практичних задач професійної діяльності, пов'язаної з розробленням та використанням засобів комп'ютерної криптографії в інформаційних технологіях

Метою кредитного модуля є формування у студентів здатностей:

– Створювати засоби комп'ютерної криптографії для інформаційних технологій.

– Застосовувати засоби комп'ютерної криптографії для забезпечення розподілу доступу до інформації,

– Застосовувати засоби комп'ютерної криптографії для ідентифікації суб'єктів та об'єктів в інформаційних технологіях

Згідно з вимогами навчальної дисципліни студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

знання:

-– Структури секретної системи Клода Шенона, визначення теоретичної секретності;

– Суть блочних симетричних криптографічних перетворень, основні рівні крипто аналізу;

– Вимоги до блочних симетричних криптографічних перетворень;

– Типові апаратно та програмно реалізовані операції комп'ютерних систем, які застосовуються в криптографічних перетвореннях;

– Поширені в Україні та світі стандарти блочних симетричних криптографічних перетворень, їх режими;

– Суть асиметричних криптографічних перетворень з відкритим ключем;

– Класичні алгоритми асиметричних криптографічних перетворень з відкритим ключем;
– Основи електронного цифрового підпису

уміння:

- – Аналізувати криптографічні перетворення на виконання вимог теоретичної секретності;
– Застосовувати типові операції комп'ютерних систем для апаратної або програмної реалізації криптографічних перетворень;
– Застосовувати у відповідності до практичних задач режими блочних симетричних криптографічних перетворень;
– Створювати закритий канал у відкритій комп'ютерній мережі;
– Виконувати послідовність дій при застосуванні стандарту України по електронному цифровому підпису

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

Кредитний модуль «Комп'ютерна криптографія» базується на кредитних модулях «Архітектура комп'ютерів», «Комп'ютерні мережі», "Захист інформації в комп'ютерних системах""

3. Зміст навчальної дисципліни

Тема 1. Предмет дисципліни.

Тема 2. Основи теорії секретних систем К.Шенона.

Тема 3. Алгебра секретних систем.

Тема 4. Стандартні алгоритми симетричних криптографічних перетворень.

Тема 5. Засади практичної криптостійкості в асиметричних криптографічних перетвореннях з відкритим ключем.

Тема 6. Математичні основи алгоритмів шифрування з відкритими ключами

Тема 7. Класичні алгоритми асиметричних криптографічних перетворень.

Тема 8. Цифровий електронний підпис.

Тема 9. Криптографічні протоколи.

4. Навчальні матеріали та ресурси

Базова література

1. Задірака В., Олексюк О. Комп'ютерна криптологія. Підручник. Київ 2002.
2. Сапсай Т.Г., Тарасенко В.П., Тесленко О.К. Методичні особливості вивчення поняття і обчислення параметрів теоретичної секретності в комп'ютерній криптографії // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2017, №1 (133), с. 91-98.
3. Вербіцький О.В. Вступ до криптології. Львів. 1998

Додаткова література

4. ДСТУ 7624:2014 «Калина» . [Електронний ресурс] http://www.dstszi.gov.ua/dstszi/control/ua/publish/printable article? art id=48387.
5. ДСТУ ISO 10118-2:2003. Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції з використовуванням n-бітового блокового шифру[Електронний ресурс]https://dnaop.com/html/41034/doc-%D0%94%D0%A1%D0%A2%D0%A3_ISO_10118-2_2003

6. ДСТУ 4145 – 2002.Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка [Електронний ресурс] https://itender-online.ru/wp-content/uploads/2017/09/dstu-4145-2002-1.pdf
7. Стандарт блочних криптографічних перетворень США, AES. [Електронний ресурс] http://www.enlight.ru/crypto/algorithms/rijndael/rijndael00.htm»

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчальна дисципліна охоплює 36 годин лекцій та 36 годин лабораторних занять, а також виконання модульної контрольної роботи

Лекційні заняття

1 Тема 1. Предмет дисципліни.

Лекція 1.1. Перелік проблем, які вирішуються засобами комп'ютерної криптографії в сучасних інформаційних системах. . Коротка історична справка з криптографії. Основні етапи розвитку комп'ютерної криптографії. Терміни і визначення в області криптографічного захисту інформації. Симетричні та асиметричні криптографічні перетворення.

Завдання на СРС: Алгоритми шифрування Цезаря та Віженера..

2 Тема 2. Основи теорії секретних систем К.Шенона.

Лекція 2.1. Структура секретної системи. Визначення криптографічних перетворень в комп'ютерній криптографії на основі секретної системи по К.Шенону. Теорема про теоретичну секретність.

Лекція 2.2. Аналіз властивостей криптографічних перетворень при забезпеченні теоретичної секретності. Аналіз практичного забезпечення теоретичної секретності. Визначення практичної секретності.

Завдання на СРС: Обчислення апостеріорних ймовірностей початкових повідомлень та ключів.

3 Тема 3. Алгебра секретних систем.

Лекція 3.1. Поняття криптографічного алгоритму. Блочні та потокові криптографічні алгоритми.. Поняття перемішування та розсіювання в блочних криптографічних алгоритмах. Цикли Фейстеля.

Лекція 3.2. Поняття ненадійності ключів блочного алгоритму шифрування.

Визначення рівнів крипто аналізу по характеру інформації, доступної крипто аналітику. Силовий алгоритм атаки на ключ. Поняття лінійного та диференційного крипто аналізу

Завдання на СРС Аналіз систем команд сучасних ЕОМ для використання в криптографічних перетвореннях

4 Тема 4 Стандарти блочних симетричних криптографічних перетворень

Лекція 4.1. Основні параметри стандарту DES. Алгоритми шифрування та розшифрування. Формування раундових ключів. Потрійний DES та йому подібні.

Лекція 4.2. Основні параметри стандарту ГОСТ 28147-89. Алгоритми шифрування та розшифрування. Довгостроковий ключ. Порівняльна характеристика DES та ГОСТ 28147-89 .

Лекція 4.3. Основні параметри стандарту AES. Алгоритми шифрування та розшифрування. Формування раундових ключів.

Лекція 4.4. Основні параметри стандарту КАЛИНА. Алгоритми шифрування та розшифрування. Формування раундових ключів. Порівняльна характеристика AES та КАЛИНи.

5 Тема 5. Засади практичної криптостійкості в асиметричних криптографічних перетвореннях з відкритим ключем.

Лекція 5.1.Поняття масового алгоритму (масових функцій, масових задач). Оцінки складності алгоритмів, складність задач. Поняття експоненційної складності та поліноміальної складності.

Лекція 5.2 Приведення задач. Класи складності N та NP. Теза Едмонта. Поняття NP – повних задач. Ідеї Діффі та Хелмена. Поняття односторонніх функцій.

6 Тема 6. Математичні основи алгоритмів шифрування з відкритими ключами

Лекція 6.1. Основи теорії кінцевих груп. Теорема Лагранжа та її наслідки. Алгоритм піднесення до степеню в кінцевих групах. Проблеми дискретного логарифму.

Лекція 6.2. Основи теорії кінцевих полів. Адитивна та мультиплікативна операції в полях GF(p) та GF(pn)

Завдання на СРС: Прості числа. Генерування та перевірка на простоту.

7 Тема 7. Класичні алгоритми асиметричних криптографічних перетворень.

Лекція 7.1. Алгоритм шифрування Ель-Гамаля та його математичне обґрунтування. Алгоритм шифрування RSA та його математичне обґрунтування. Особливості програмної реалізації алгоритмів Ель-Гамаля та RSA.. Оцінки швидкодії алгоритмів.. Порівняльна характеристика симетричних алгоритмів та алгоритмів шифрування з відкритим ключем.

Тема 8. Цифровий електронний підпис.

Лекція 8.1. Визначення електронного підпису і його ролі в сучасних інформаційних технологіях. Перелік вимог до електронного підпису. Математичні основи електронного підпису. Визначення функції хешування та вимоги до неї. Стандарти алгоритмів обчислення хеш значень для цифрового підпису.

Лекція 8.2. Еліптичні криві в кінцевих полях. Групи точок еліптичних кривих. Операції додавання та подвоєння точок. Особливості та причини використання криптографічних перетворень на еліптичних кривих.

Лекція 8.3. Електронний цифровий підпис по ДСТУ 4145-2002. Процедура вироблення та перевірки електронного підпису по ДСТУ 4145-2002.. Послідовність дій при використанні ДСТУ 4145-2002

Тема 9. Криптографічні протоколи.

Визначення криптографічного протоколу. Перелік вимог до криптографічного протоколу. Протокол Діффі-Хелмена. Забезпечення «передавання» секретних ключів по відкритій мережі. Аналіз атак на криптографічні протоколи. Протоколи з нульовим розголошенням.

Завдання на СРС: Організація роздачі карт по мережі

Лабораторні заняття

Основне завдання циклу лабораторних робіт: набуття практичного досвіду проектування та дослідження криптографічних перетворень.

Дослідження апостеріорних ймовірностей криптограм в залежності від властивостей функції шифрування, довжини ключа та розподілу апріорних ймовірностей початкових повідомлень та ключів.

Дослідження властивостей стандартних блочних симетричних криптографічних перетворень.

Дослідження криптографічно стійких програмних генераторів випадкових послідовностей

Самостійна робота студентів

Назва теми, що виноситься на самостійне опрацювання

Тема 1. Предмет дисципліни.

Алгоритми шифрування Цезаря та Віженера

Тема 2. Основи теорії секретних систем К.Шеннона.

Обчислення апостеріорних ймовірностей початкових повідомлень та ключів

Тема 3. Алгебра секретних систем.

Аналіз систем команд сучасних ЕОМ для використання в криптографічних перетвореннях

Тема 6. Математичні основи алгоритмів шифрування з відкритими ключами

Прості числа. Генерування та перевірка на простоту

Тема 9. Криптографічні протоколи.

Організація роздачі карт по мережі

Політика та контроль

6. Політика навчальної дисципліни (освітнього компонента)

- Правила відвідування *занять – обов'язкове (як лекцій, так і лабораторних);*
- Правила виконання лабораторних робіт при дистанційному навчанні – рішення і відповіді на запитання присилаються студентами по електронній пошті.
- ***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. Усі письмові роботи перевіряються на наявність плагіату. Списування під час контрольних робіт чи завдань заборонені (в т. ч. із використанням мобільних пристроїв).*
- ***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.
- ***Інклюзивне навчання.*** *Засвоєння знань та умінь в ході вивчення дисципліни бути доступним для більшості осіб з особливими освітніми потребами, окрім здобувачів з серйозними вадами зору, які не дозволяють виконувати завдання за допомогою персональних комп'ютерів, ноутбуків та/або інших технічних засобів.*
- ***Навчання іноземною мовою.*** *У ході виконання завдань студентам може бути рекомендовано звернутися до англомовних джерел.*
- ***Процедура оскарження результатів контрольних заходів оцінювання.*** *Студент може підняти будь-яке питання, яке стосується процедури контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право аргументовано оскаржити результати контрольних заходів, пояснивши з яким критерієм не погоджуються відповідно до оціночного.*
- ***Неформальна/інформальна освіта.***
- *Порядок визнання результатів навчання, набутих у неформальній/інформальній освіті здобувачами, які навчаються в КПІ ім. Ігоря Сікорського, регулюється «Положенням про визнання в КПІ ім.Ігоря Сікорського результатів навчання, набутих у неформальній/інформальній освіті» (*https://osvita.kpi.ua/sites/default/files/downloads/%D0%9D%D0%B5%D1%84%D0%BE%D1%80%D0%BC_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.pdf*) та наказом «Про особливості визнання результатів навчання в умовах правового режиму воєнного стану» (https://document.kpi.ua/files/2022_НОН-164.pdf)*

7. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Семестровий контроль проводиться у вигляді екзамену. Для оцінювання результатів навчання застосовується 100-бальна рейтингова система та університетська шкала.

Поточний контроль: фронтальні опитування, участь у роботі семінарів, доповідання,

електронне звітування виконаних лабораторних робіт, МКР.

Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану

виконання вимог силабусу.

Семестровий контроль: екзамен – два теоретичні запитання і одне практичне

Рейтингова система оцінки успішності студентів кредитного модуля " Комп'ютерна криптографія ".

Рейтинг студента з дисципліни складається з балів, що він отримує за:

1) виконання та захист 3 лабораторних робіт;
2) виконання контрольної роботи;
3) відповідь на екзамені.

Система рейтингових (вагових) балів та критерії оцінювання

1. Лабораторні роботи

Ваговий бал – 16. Максимальна кількість балів за всі лабораторні роботи дорівнює 16бали х 3 = 48 балів.

По кожній лабораторній роботі студент одержує 16 балів при умові якісного вчасного виконання.

На першу та другу лабораторні роботи виділяється по 5 тижнів, на третю – 6 тижнів

Не вчасне виконання зменшує кількість отриманих балів пропорційно затримці, але не менше ніж 8 балів.

Позначимо R1 – кількість балів, які студент одержав на протязі семестру за виконання лабораторних робіт

.

Контрольна робота

Максимальна кількість балів за контрольну роботу дорівнює 12 балів.

Критерії оцінювання.

a) Відповідь правильна та прокоментована r2 = 12 балів
b) Відповідь правильна, але не прокоментована r2 = 10 балів
c) Відповідь не правильна, але коментар вказує на механічну помилку (наприклад, помилку в обчисленнях) r2 =8 балів
d) Відповідь не правильна, але коментар вказує на не значну логічну помилку – 6 балів
e) 0 балів в інших випадках.

Позначимо R2 – кількість балів, які отримав студент за виконання контрольної роботи.

Сума вагових балів контрольних заходів протягом семестру складає:

RC = 48 + 12 = 60 балів.

Екзаменаційна складова шкали дорівнює 40% від R.

Таким чином, рейтингова шкала з дисципліни складає R = RC + RE = 100 балів.

Стартовий рейтинг студента rC = R1+R2

Необхідною умовою допуску до екзамену є стартовий рейтинг (rC) не менше 40 % від RC, тобто 24 бали. В іншому разі студент повинен виконати додаткову роботу та підвищити свій рейтинг.

Екзаменаційний білет складається з 2 питань – одного теоретичного і одного практичного.

Максимальна кількість балів за теоретичне питання – 30, за практичне - 10.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

8. Додаткова інформація з дисципліни (освітнього компонента)

Під час навчання та для взаємодії зі студентами використовуються сучасні інформаційно-комунікаційні та мережеві технології для вирішення навчальних завдань.

Робочу програму навчальної дисципліни (силабус):

Складено доцентом кафедри СПіСКС., к.т.н., с.н.с Тесленком О.К..

Ухвалено кафедрою СПСКС (протокол №6 від 03.01.24)

Погоджено Методичною комісією ФПМ (протокол №11 від 12.06.2024)