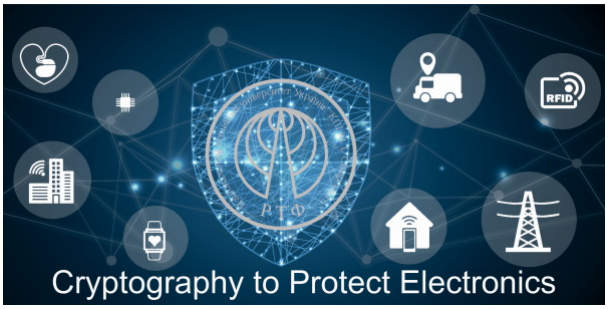
Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра прикладної радіоелектроніки

[RE-92] ТЕХНІЧНИЙ ЗАХИСТ В ІНФОРМАЦІЙНИХ СИСТЕМАХ



Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Другий (магістерський)
Галузь знань	17 - Електроніка, автоматизація та електронні комунікації
Спеціальність	172 - Електронні комунікації та радіотехніка
Освітня програма	Всі ОП
Статус дисципліни	Вибіркова (Ф-каталог)
Форма здобуття вищої освіти	Очна
Рік підготовки, семестр	Доступно для вибору починаючи з 1-го курсу, весняний семестр
Обсяг дисципліни	4 кред. (Лекц. 18 год, Практ. год, Лаб. 36 год, СРС. год)
Семестровий контроль/контрольні заходи	Залік
Розклад занять	https://rozklad.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лекц.: Навроцький Д. О., Лаб.: Навроцький Д. О.,
Розміщення курсу	

Програма навчальної дисципліни

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

Чому це цікаво/треба вивчати?

Корисна інформація, завжди становить цінність, яку необхідно оберігати. На цьому курсі вивчимо основи криптографії для захисту каналів зв’язку і для захисту даних у сховищах.

Чому можна навчитися (результати навчання)?

- Навчитись основам симетричної і асиметричної криптографії.
- Навчитись використовувати існуючі шифратори для захисту різних програм/пристроїв.
- Навчитись створювати власні шифратори.

Як можна користуватися набутими знаннями і уміннями (компетентності)?

- Набуті знання дозволять використовувати існуючі шифратори, наприклад, AES256, RSA для захисту даних на комп’ютері і у мікроконтролері.
- Використовувати криптографію для захисту каналу зв’язку між різними пристроями.

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

Бажане володіння мовами програмування низького і високого рівня.

Такими як C/C++, C#, Python.

Але, можна навчитись програмуванню і під час проходження курсу.

Бажано вміти програмувати мікроконтролери, типу Arduino, STM32, ESP32/8266

3. Зміст навчальної дисципліни

Тема 1. "Вступ до захисту даних. Цілі криптографії і стеганографії"

Тема 2. "Основи криптографії. Симетрична, асиметрична, гібридна, квантова криптографії"

Тема 3. "Криптографічні примітиви, функції перетворення"

Тема 4. "Незвідні та примітивні поліноми, Абелеві групи, поля, кільця, побудова S-Box (таблиця замін)"

Тема 5. "Потокові шифри"

Тема 6. "Блокові шифри"

Тема 7. "Режими шифрування"

Тема 8. "Порівняння AES подібних шифрів"

Тема 9. "Генератори псевдо-випадкових послідовностей"

Тема 10. "Цифровий підпис. Геш-функції".

Тема 11. "Аналіз шифрограми. Тести NIST STS, цифрова ентропія, тести Diehard"

Тема 12. "RSA шифри"

Тема 13. "Розробка власного шифру"

Тема 14. "Криптологія. Вразливості алгоритму і реалізації"

4. Навчальні матеріали та ресурси

Інформаційні ресурси:

1. Тести NIST STS [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

2. Тести Dieharder [Електронний ресурс]. – Режим

доступу: https://webhome.phy.duke.edu/~rgb/General/dieharder.php

3. І. Н. Войцехівська. Криптографія// Енциклопедія історії України : у 10 т. / редкол.: В. А. Смолій (голова) та ін. ; Інститут історії України НАН України. — К. : Наукова думка, 2009. — Т. 5 : Кон — Кю. — С. 390. — 560 с. : іл. — ISBN 978-966-00-0855-4.

4. О. В. Гомонай. Криптографія // Енциклопедія сучасної України : у 30 т. / ред. кол. І. М. Дзюба [та ін.] ; НАН України, НТШ. — К. : Інститут енциклопедичних досліджень НАН України, 2001–2020. — ISBN 944-02-3354-X.

5. Криптографія // Літературознавча енциклопедія : у 2 т. / авт.-уклад. Ю. І. Ковалів. — Київ : ВЦ «Академія», 2007. — Т. 1 : А — Л. — С. 532.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лабораторні роботи:

1. Створення форми авторизації для користувача (поле для вводу логіна і пароля);
2. Шифрування чисел за допомогою операції XOR (вона ж “складання за модулем 2”);
3. Шифрування тексту, одноразовим ключем, коли довжина тексту і ключа однакові.;
4. Шифрування файлу одноразовим ключем, коли довжина файлу значно більша за довжину ключа;
5. Створення цифрового підпису, використання HASH-функції;
6. Розширення ключа шифрування, створення “гами” довільної довжини. Стандарт PBKDF2.
7. Розрахунок інформаційної ентропії, аналіз шифрограми;
8. Режими симетричного блочного шифрування AES, 3DES;
9. Асиметричне шифрування RSA;
10. Розробка власного потокового шифру;
11. Стеганографія;
12. Криптологія.

6. Самостійна робота студента

Домашня контрольна робота:

1. Розрахувати власну таблицю замін (S-Box) за вказаним незвідним поліномом і утворюючим елементом. Таблиця містить 256 унікальних елементів (числа від 0 до 255), розмір таблиці 16x16. Приклад S-Box для AES.
2. Написати власний AES подібний шифратор з використанням таблиці замін і таблиці підстановок.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Максимум практичних занять, мінімум теорії (тільки необхідне)

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

...

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

9. Додаткова інформація з дисципліни (освітнього компонента)

Приклади екзаменаційних запитань:

1. Що таке семерична криптографія?
2. Що таке асиметрична криптографія?
3. Коли використовують відкритий ключ шифрування?
4. Коли використовують секретний ключ шифрування?
5. Що таке інформаційна ентропія?
6. Що таке гамування?
7. Що таке шифрограма?
8. Коли використовують блочні шифри?
9. Коли використовують потокові шифри?
10. Основні криптографічні примітиви?
11. Які популярні стандарти шифрування?
12. Чим відрізняється практична від теоретичної криптостійкості шифру?
13. Що таке вразливість реалізації шифру?
14. Які бувають режими шифрування?
15. …

Опис матеріально-технічного та інформаційного забезпечення дисципліни

IDE Visual Studio для Python, C#

STM32CubeIDE або IDE Arduino (Atmel Studio) для C/C++

Використовуємо в лабораторних роботах комп’ютер, плати STM32F4Discovery або Arduino Uno (пишемо код під ATMega328 або STM32F401), в залежності від рівня підготовки групи.

Робочу програму навчальної дисципліни (силабус):
Складено Навроцький Д. О.;
Ухвалено кафедрою ПРЕ (протокол № 06/2023 від 22.06.2023)
Погоджено методичною комісією факультету/ННІ (протокол № 06-2023 від 29.06.2023)