Лабораторний практикум
з дисципліни “Основи криптографії” для студентів 4-го курсу спеціальності
“Інженерія програмного забезпечення”

Лабораторний практикум складається з 16 робіт і має кілька рівнів складності.
Студент може обирати будь-яку кількість робіт, виконувати їх в будь-якому порядку (за винятком випадків, коли для виконання певної роботи неохідно виконати попередню/попередні).
Задача студента — набрати максимально можливу кількість балів. У навчальному плані на лабораторний практикум відводиться 50 балів (20 в першому модулі + 30 — в другому). Звісно, можна набрати й більше/менше балів, виконавши більшу/меншу кількість лабораторних робіт.
Лабораторні роботи будуть оцінюватися так, як подано в таблиці. Звісно, якщо робота виконана не повністю, або якщо виконано полегшений варіант — повна кількість балів не нараховується.
Можливий варіант дистанційного захисту лабораторної роботи, коли студент, зробивши роботу, знімає скрин-каст протоколу дій, робить архів зі звітом та кодом, і відправляє це викладачу (попередньо домовившись про такий спосіб захисту!).
Найкращі лабораторні роботи III рівня (їх скрін-касти) буде викладено на каналі кафедри програмного забезпечення в YouTube:
https://www.youtube.com/channel/UCvvfjUiMrv0oIOZVRrw1e-g

Таблиця: Оцінювання лабораторних робіт з курсу “Основи криптографії”

ЛР№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
К-сть балів	4	4	4	6	6	4	4	4	4	8	10/6	8	10	10	10	10
	- лабораторні роботи I рівня;															
	- лабораторні роботи II рівня;															
	- лабораторні роботи III рівня.															

Лабораторні роботи I рівня — прості роботи, в яких необхідно розробити програмне забезпечення, що використовує класичні криптоалгоритми (шифр Цезаря, спрощені потокові шифри, спрощений RSA).
Лабораторні роботи II рівня вимагають більш ретельної роботи та написання більших об’ємів коду.
Лабораторні роботи III рівня — досить серйозні криптографічні застосування, які продемонструють студенту, що їх виконав, можливості сучасного криптографічного програмного забезпечення та принципів його розробки.

ЗАУВАЖЕННЯ: В усіх лабораторних роботах висуваються вимоги до правил написання коду, наприклад, *C++ Programming Style Guideline* або аналогічного для обраної Вами мови програмування. Змінні типу Form1, Procedure1, a1,b2,c3 не допускаються, і код буде відхилений. Крім цього, код повинен супроводжуватися коментарями, які давали би повне розуміння про функції тієї чи іншої процедури/функції/класу/об’єкту тощо. Код без коментарів також буде відхилятися.

Лектор С.Е.Остапов