План лабораторного заняття № 3
Тема № 2 “Криптографічні методи захисту інформації”

Навчальний час: 2 год.

Міжпредметні зв’язки: навчальна дисципліна “Захист інформації в інформаційних системах” взаємопов’язана з такими дисциплінами як “Економіко-математичне моделювання”, “Інформатика” та ін.

Мета і завдання лабораторного заняття: ознайомлення з найбільш простими методами шифрування.

Питання для перевірки базових знань за темою лабораторного заняття:

1. Що таке криптографія? Що таке шифр? У чому полягає мета шифрування?
2. Які основні вимоги висувають до шифру?
3. Що таке досконалий шифр?
4. Що таке криптографічна стійкість? Чим вона визначається?
5. У чому полягає суть шифрування за методом Цезаря?
6. Що таке частотний криптоаналіз?
7. Які переваги шифру Цезаря?
8. Які недоліки має шифр Цезаря?
9. Який шифр був побудований та вдосконалений на основі шифру Цезаря?

Завдання: автоматизувати процес шифрування тексту на основі шифру Цезаря. Перевірити правильність його виконання на прикладі довільного словосполучення. Оформити звіт.

Хід виконання лабораторної роботи:

Шифр Цезаря або шифр зсуву – це симетричний моноалфавітний алгоритм шифрування, в якому кожна буква відкритого тексту заміняється на ту, що віддалена від неї в алфавіті на сталу кількість позицій, яку задає власник шифру (т.зв. ключ). Римський імператор Юлій Цезар використовував для приватного листування шифр зсуву з ключем «3» – замість літери A підставляв D, замість B – E і так далі.

Приклад. Шифрування фрази «this is Caesar's code» за допомогою ключа k=3 (зсув на три літери, англійський алфавіт) дає такий зашифрований текст:

wklv lv Fdhvdu'v frgh

Для того, щоб одержувач повідомлення міг відновити вихідний текст, необхідно повідомити йому, що ключ k=3.

Недоліком шифру Цезаря, як і будь-якого моноалфавітного шифру, є вразливість до частотного криптоаналізу.

При автоматизації методу Цезаря врахувати, що:

Зауваження 1. Неалфавітні символи – знаки пунктуації, пробіли, цифри – не змінюються.

Зауваження 2. Урахувати, що при шифруванні тексту за допомогою шифру Цезаря алфавіт **зациклюється**, тобто літери в кінці алфавіту перетворюються в літери на початку алфавіту.

Якщо співставити кожному символу алфавіту його порядковий номер (починаючи нумерацію з 0), то шифрування та дешифрування можна виразити формулами модульної арифметики:

$$y = (x+k) \bmod n,$$

$$x = (y-k+n) \bmod n,$$

де x – символ відкритого (незашифрованного) тексту, y – символ вже зашифрованого тексту, n – потужність алфавіту (число літер в алфавіті), k – ключ; операція mod – ділення з остачею.

Рекомендована література до теми лабораторного заняття:

Основна та допоміжна література:

1. Харин Ю.С. Математические основы криптологии: учеб.пособ. / Ю.С.Харин, В.И.Берник, Г.В.Матвеев. – Мн.: БГУ, 1999. – 319 с.
2. Зима В. Безопасность глобальных сетевых технологий / В.Зима, А.Молдован, Н.Молдован. – СПб.: БХВ-Петербург, 2003. – 368 с.
3. Щербаков А. Прикладная криптография / А. Щербаков, А.Домашев. – М., 2003. – 404 с.
4. Пономаренко Н.Н. Защита информации в телекоммуникационных системах: учеб. пособ. / Н. Н. Пономаренко. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «Харьк.авиац.ин-т», 2015. – 40 с.
5. Алферов А.П. Основы криптографии: учеб. пособ. / А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин,
6. А.В.Черемушкин. – М.: Гелиос АРВ, 2002 – 480 с.
7. Басалова Г.В. Основы криптографии / Г.В. Басалова. – М.: Национальный Открытый Университет "ИНТУИТ", 2016. – 283 с. URL: https://www.twirpx.com/file/1907188/

Інтернет-ресурси:

https://books.ifmo.ru/file/pdf/56.pdf

http://booksshare.net/index.php?id1=4&category=cryptography&author=alferov-ap&book=2002

Обладнання заняття, ТЗН тощо: комп’ютери.

Завдання студентам на розв’язання вправ для підготовки до наступного лабораторного заняття.

Укладач:_____ Задорожна А. В., доцент кафедри цифрової економіки та бізнес-аналітики

(підпис) (ПІБ, посада, науковий ступінь, вчене звання)