План лабораторного заняття № 1
Тема № 1 "Загальні аспекти 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 операціями, що використовуються у криптографії.

Питання для перевірки базових знань за темою лабораторного заняття:

1. Для чого призначена операція XOR?
2. У якому випадку результат виконання операції над двома змінними буде істинним? Операції над трьома змінними?
3. Що таке шифр?

Завдання:

1. На основі мови програмування Java створити програму для автоматизації операції суми по модулю два (так звану «**xor**»). Програма повинна виконувати такі дії:
   А) переводити два числа з десяткової системи числення в іншу (двійкову) систему числення.
   Б) Виконувати операцію суми по модулю два (або «**xor**»).
   В) Результат обчислень перевести з двійкової системи числення в десяткову.
   Г) Вивести результат обчислень у десятковій системі числення на екран монітора.

Хід виконання лабораторної роботи:

1) На першому етапі передбачити переведення двох чисел з десяткової в двійкову систему числення. Для цього використати такий алгоритм перетворення числа X з десяткової системи числення в іншу систему числення Y:
   Для цього припустимо, що R – рядок цифр, що містить результат переводу числа X в систему числення з основою Y. Ініціалізувати R порожнім рядком.
   Знайти цілу частину N від ділення X на Y та залишок L.
   Замінити X на N. Додати в рядок R нову цифру L.
   Якщо X>0, то перейти на крок 2. Інакше перейти на крок 5.
   Записати цифри рядка R у зворотному порядку. Число переведено з десяткової системи X в систему числення Y.
   Приклад. Перевести число 78 у двійкову систему числення.
   R=""

78:2=39	0 у залишку	R="0"	X=39
39:2=19	1 у залишку	R="01"	X=19
19:2=9	1 у залишку	R="011"	X=9
9:2=4	1 у залишку	R="0111"	X=4
4:2=2	0 у залишку	R="01110"	X=2
2:2=1	0 у залишку	R="011100"	X=1
1:2=0	1 у залишку	R="0111001"	X=0

   Записуємо R у зворотному порядку: R=1001110.
   Тоді число 78 у двійковій системі числення буде мати вигляд: $78_{10}=1001110_2$.

2) Після цього виконати обчислення на основі такого правила (табл. 1):

Таблиця 1

Правило обчислення суми по модулю два

1-й біт	2-й біт	Сума
0	0	0
1	0	1
0	1	1
1	1	0

3) На третьому етапі передбачити переведення кінцевого результату у десяткову систему числення.

4) Для цього використати такий алгоритм перетворення числа з системи числення Y в десяткову систему числення X:

Спочатку потрібно подати число X у вигляді рядку цифр R. Нехай число цифр у рядку R дорівнює n. Далі нумерують цифри справа наліво, починаючи з нуля і завершуючи n-1.

Тоді число X у десятковій системі числення буде мати вигляд:

$X_{10} = a_{n-1}Y^{n-1} + a_{n-2}Y^{n-2} + \ldots + a_2Y^2 + a_1Y^1 + a_0Y^0$.

2. Перевірити правильність виконання програми для таких операцій:
   1) 115 xor 18
   2) 78 xor 43
   3) 189 xor 274.

Додаткові завдання для студентів: опрацювання теоретичного матеріалу теми, написати план-конспект заняття за вибраною темою із використанням демонстраційного матеріалу.
Форми контролю знань – презентація виконаних завдань, перевірка коду програми, обговорення виконаних завдань.

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.

Укладач:_____ Задорожна А. В., доцент кафедри цифрової економіки та бізнес-аналітики
(підпис) (ПІБ, посада, науковий ступінь, вчене звання)