План лабораторного заняття № 6
Тема № 3 "Безпека в інформаційних мережах"

Навчальний час: 4 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 розширеним методом Евкліда.

Питання для перевірки базових знань за темою лабораторного заняття:

1. У чому полягає суть розширеного методу Евкліда? Для чого він використовується?
2. Які види ключів використовуються при асиметричному шифруванні?
3. Опишіть алгоритм шифрування за допомогою асиметричного методу.
4. Яку криптографічну стійкість дають асиметричні методи шифрування?
5. Який з методів шифрування – симетричний чи асиметричний – дає більшу швидкість?
6. Який з методів шифрування – симетричний чи асиметричний – забезпечує більшу криптографічну стійкість?
7. До якої криптографії належить алгоритм RSA?
8. Які переваги асиметричного методу шифрування?
9. Які недоліки має асиметричний метод шифрування?

Завдання: автоматизувати розширений алгоритм Евкліда. Перевірити правильність його виконання. Обчислити:

1) Нехай a та b – натуральні числа. Знайти НСД(a, b), не використовуючи при обчисленнях операцій множення та ділення.
2) Нехай a та b – натуральні числа. Знайти НСК(a, b).
3) Нехай a та b – цілі числа. Знайти НСД(a, b), не використовуючи при обчисленнях операцій множення та ділення.
4) Нехай a та b – цілі числа. Знайти НСК(a, b), не використовуючи при обчисленнях операцій множення та ділення.
5) Нехай a та b – цілі числа. Обчислити трійку чисел (d, a, b) за допомогою розширеної моделі Евкліда.
6) Нехай a та b – натуральні числа. Подати НСД(a, b) у вигляді лінійної комбінації a та b.
7) Нехай a та b – цілі числа. Подати НОД(m, n) у вигляді лінійної комбінації m та n.
8) Нехай a та b – цілі числа. Перевірити, чи a та b є взаємно простими.

Оформити звіт.

Хід виконання лабораторної роботи:

Нехай a і b - натуральні числа, а d - їх найбільший більший загальний дільник. Розширений алгоритм Евкліда підраховує не лише d, а й два цілих числа x і y, таких, що: ax + by = d. Тобто він знаходить коефіцієнти, за допомогою яких НСД двох чисел виражається через самі ці числа. Алгоритм Евкліда складається з послідовності розподілів із залишком. Найбільший спільний множник являє собою останній ненульовий залишок в цій послідовності.

Дано два цілих числа a і b. Нам часто треба знайти інші два цілих числа s і t, такі, які s×a + t×b = НСД (a, b).

Розширений алгоритм Евкліда може обчислити НСД (a, b) і в той же самий час обчислити значення s і t. Тут розширений алгоритм Евкліда використовує ті ж самі кроки, що й простий алгоритм Евкліда. Однак в кожному кроці ми застосовуємо три групи обчислень замість однієї. Алгоритм використовує три набори змінних: r, s і t.

На кожному кроці змінні r_1, r_2 і r використовуються так само, як в алгоритмі Евкліда. Змінним r_1 і r_2 присвоюються початкові значення a і b відповідно. Змінним s_1 і s_2 присвоюються початкові значення 1 і 0 відповідно. Змінним t_1 і t_2 присвоюються початкові значення 0 і 1 відповідно.

Обчислення r, s і t однакові, але з однією відмінністю. Хоча r – залишок від ділення r_1 на r_2, але такої відповідності в інших двох групах обчислень немає. Є тільки одне приватне q, яке обчислюється як r_1/r_2 і використовується для інших двох обчислень.

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
http://e-maxx.ru/algo/export_extended_euclid_algorithm

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)