План лабораторного заняття № 5
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 алгоритмом Евкліда.

Питання для перевірки базових знань за темою лабораторного заняття:

1. Опишіть суть алгоритму Евкліда.
2. На яких фактах заснований алгоритм Евкліда?
3. У яких випадках використовується алгоритм Евкліда?
4. Які кроки виконуються в алгоритмі Евкліда?
5. Які існують методи шифрування?
6. Назвіть переваги симетричного шифрування.
7. Які недоліки симетричного шифрування?
8. Як здійснюється шифрування та дешифрування повідомлення з використанням відкритого ключа?

Завдання: автоматизувати алгоритм Евкліда, що використовується при розв’язку багатьох криптографічних задач.

Хід виконання лабораторної роботи:

Алгоритм Евкліда використовується у багатьох задачах криптографії, у тому числі при формуванні секретного ключа в алгоритмі RSA, поширеному методі криптографії з відкритим ключем.

Найбільший спільний дільник (НСД) двох чисел a і b позначається як НСД(a, b) або(a, b). В англомовній літературі прийнято вживати позначення gcd(a, b).

НСД двох чисел – це найбільше число, що ділить обидва дані числа без остачі. Алгоритм Евкліда заснований на тому, що НСД не змінюється, якщо від більшого числа відняти менше. Наприклад, 21 є НСД чисел 252 та 105 (252 = 21 × 12; 105 = 21 × 5); оскільки 252 − 105 = 147, НСД 147 та 105 також 21. Оскільки більше з двох чисел постійно зменшується, повторне виконання цього кроку дає все менші числа, поки одне з них не дорівнюватиме нулю. Коли одне з чисел дорівнюватиме нулю, те, що залишилось, і є НСД. Обертаючи кроки алгоритму Евкліда у зворотний порядок, НСД можна виразити як лінійну комбінацію даних чисел помножених на цілі коефіцієнти, наприклад 21 = 5 × 105 + (−2) × 252.

Кожен дільник натурального числа a не може бути більшим самого числа a, тому число a має скінченне число дільників, які не перевищують a.

Серед дільників чисел a і b можуть бути однакові, тобто спільні дільники. Очевидно, їх кількість так само є скінченною. Найбільшим спільним дільником двох натуральних чисел називається найбільше натуральне число, на яке ділиться кожне з цих чисел без залишку. З даного означення випливає, що для того, щоб знайти НСД двох чисел a і b, на першому кроці, необхідно знайти всі додатні дільники числа a і всі додатні дільники числа b. Далі, необхідно вибрати всі числа, що входять в обидві множини, та визначити найбільше серед них. Воно і буде найбільшим спільним дільником.

Алгоритм Евкліда полягає у повторенні таких кроків:

1. Для визначення НСД використаємо дві змінні r_1 і r_2. Це дозволяє запам’ятовувати змінні, що змінюються, протягом всього процесу. Нехай вони мають початкові значення a і b.

На кожному кроці потрібно обчислити залишок від ділення r_1 на r_2 і зберігаємо результат у вигляді змінної r (тобто знаходять цілу частину та залишок r).

2. Потім замінюємо r_1 на r_2 і r_2 на r і продовжити виконувати кроки до тих пір, доки r не стане рівним нулю. Отже, НСД (a,b) знайдено і він дорівнює r_1.

За допомогою побудованої програми знайти:

1) Найбільший спільний дільник чисел 26325 та 42315;
2) Найбільший спільний дільник чисел 391951 та 161063;
3) Найбільший спільний дільник чисел 221867 та 301971;
4) Найбільший спільний дільник чисел 2004687 та 5127506.

Результати оформити у вигляді звіту.

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, 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.

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)