НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
Факультет прикладної математики
Кафедра прикладної математики

Звіт
з лабораторної роботи № 5
із дисципліни «Криптографічні методи захисту інформації»
на тему
*Криптографічні алгоритми Діффі-Хеллмана та Ель-Гамаля*

Виконав:
студент групи КМ-ХХ
*Іваненко І. І.*

Керівник:
*ст. викладач Бай Ю. П.*

Київ — 20__

# ЗМІСТ

***Мета роботи:*** розробити асиметричні криптосистеми на основі алгоритмів Діффі-Хеллмана та Ель-Гамаля.

## Постановка завдань

1. Скласти програму, яка дозволяє здійснити обмін ключами за алгоритмом Діффі-Хеллмана. Перевірити роботу програми на контрольному прикладі. В якості ВІДПРАВНИКА здійснити обмін ключами з ОДЕРЖУВАЧЕМ, згенерувати спільний ключ. Навести скріншоти детального виконання алгоритму для контрольного прикладу та власного завдання.

1.*а*. Контрольний приклад (Протокол Діффі-Хеллмана)

$g = 5, \quad p = 23, \quad a = 6, \quad b = 15,$

*public key* $\{g, p\} = \{5, 23\}$

*Alice's private key* $\{a\} = \{6\}$

*Bob's private key* $\{b\} = \{15\}$

$\boldsymbol{K = 2}$

1.*б*. Виконати дії ВІДПРАВНИКА та ОДЕРЖУВАЧА, згенерувати спільний ключ *К*, заповнити *Таблицю 1*. Результати також записати в гугл-таблицю Завдання ЛР 5.

2. Скласти програму, яка дозволяє виконувати шифрування та розшифрування за алгоритмом Ель-Гамаля. Перевірити роботу програми на контрольних прикладах. Навести скріншоти детального виконання алгоритму для контрольних прикладів (*а, б*) та власного завдання (*в*).

2.*а*. Контрольний приклад 1 (Схема Ель-Гамаля)

2.*б*. Контрольний приклад 2 (ElGamal encryption)

2.*в*. Виконати дії ВІДПРАВНИКА: використовуючи заданий відкритий ключ, зашифрувати День свого народження, записаний у форматі *"ddmm"*, або інше число в діапазоні від 101 до 3112. Результати шифрування **для двох різних випадкових чисел $k_1$ і $k_2$** записати в Завдання ЛР 5. Розшифрувати одержані криптотексти. Заповнити *Таблиці 2, 3*.

*Увага! Як визначити М ?*

*01 січня* $\rightarrow M = 101 \ldots$ 4 *липня* $\rightarrow M = 407 \ldots$ *31 грудня* $\rightarrow M = 3112$ .

## Математичне підґрунтя і опис алгоритму Діффі-Хеллмана

……

## Математичне підґрунтя і опис алгоритму Ель-Гамаля

……

## Контрольний приклад до алгоритма Діффі-Хеллмана

Протокол Діффі-Хеллмана

Виконати приклад. Додати скріншот, що містить усі проміжні результати.

## Завдання 1. Обмін ключами за алгоритмом Діффі-Хеллмана

*Таблиця 1.*

| $f(x) = g^x \bmod p$ |
|---|

| | ***Alice (Відправник)*** | | | ***Bob (Одержувач)*** | |
|---|---|---|---|---|---|
| 1 | Обирає і публікує прості числа *g, p (частини відкритого ключа)* | {3,17} | | | |
| 2 | Обирає секретний ключ ***a*** | **4** | | Обирає секретний ключ ***b*** | **6** |
| 3 | Обчислює і публікує $A=g^a \bmod p$ | A=13 | | Обчислює і публікує $B = g^b \bmod p$ | B=15 |
| 4 | Обчислює $K=B^a \bmod p$ | **16** | | Обчислює $K=A^b \bmod p$ | **16** |

## Контрольні приклади до алгоритма Ель-Гамаля

2.*а*.

2.*б*.

## Завдання 2. Шифрування і розшифрування за алгоритмом Ель-Гамаля

*Таблиця 2 (Шифрування 1).*

| | ***Alice*** (ВІДПРАВНИК) | | | ***Bob*** (ОДЕРЖУВАЧ) | |
|---|---|---|---|---|---|
| | | | 1 | Обирає прості числа $g$, $p$ *(g - генератор, p - модуль)* | $g = 2$<br>$p = 2357$ |
| | | | 2 | Обирає секретний ключ ***x*** | **1751** |
| | | | 3 | Обчислює $y=g^x \bmod p$ | $y = 1185$ |
| | | | 4 | Публікує відкритий ключ $\{p, g, y\}$ | 2357, 2, 1751 |
| 5 | Одержує відкритий ключ $\{p, g, y\}$ | 2357, 2, 1751 | | | |
| 6 | Обирає текст для шифрування $M$ | 2035 | | | |
| 7 | Обирає випадкове ціле число $k$: $k < p - 2$ | 1520 | | | |
| 8 | Обчислює $a = g^k \bmod p$ та $b = (y^k \cdot M) \bmod p$ | $a = 1430$<br>$b = 697$ | | | |
| 9 | Надсилає одержувачу шифротекст $(a; b)$. | 1430, 697 | | | |
| | | | 10 | Використовуючи секретний ключ ***x***, розшифровує отриманий шифротекст:<br>$M' = (a^{p-1-x} \cdot b) \bmod p$ | $M' = 2035$ |

*Таблиця 3 (Шифрування 2).*

| | ***Alice*** (ВІДПРАВНИК) | | | ***Bob*** (ОДЕРЖУВАЧ) | |
|---|---|---|---|---|---|
| | | | 1 | Обирає прості числа *g, p* *(g - генератор, p - модуль)* | *g* = 2 *p* = 2357 |
| | | | 2 | Обирає секретний ключ ***x*** | **1751** |
| | | | 3 | Обчислює $y=g^x \bmod p$ | *y* = 1185 |
| | | | 4 | Публікує відкритий ключ {*p, g, y*} | 2357, 2, 1751 |
| 5 | Одержує відкритий ключ {*p, g, y*} | 2357, 2, 1751 | | | |
| 6 | Обирає текст для шифрування *M* | 2035 | | | |
| 7 | Обирає випадкове ціле число *k*: $k < p - 2$ | | | | |
| 8 | Обчислює $a = g^k \bmod p$ та $b = (y^k \cdot M) \bmod p$ | | | | |
| 9 | Надсилає одержувачу шифротекст *(a; b).* | | | | |
| | | | 10 | Використовуючи секретний ключ ***x***, розшифровує отриманий шифротекст: $M' = (a^{p-1-x}) \cdot b) \bmod p$ | M′ = 2035 |

## Список літератури

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Диалектика, 2003. – 610 с.

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.

4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: «Вильямс», 2001. – 672 с.

5. Menezes A.J., Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, Inc., 1997. – 795 p.

**Додаток 1**

# Скріншоти виконання обчислень