НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра прикладної математики

Звіт

з лабораторної роботи №*2*

з дисципліни «Криптографічні методи захисту інформації»

на тему:

*Розробка криптосистем на основі шифру Віженера та шифру з використанням двійкового гамування*

|  |  |
| --- | --- |
| Виконав(-ла): | Керівник: |
| студент(ка) групи КМ-01 | *ст. викладач Бай Ю. П.* |
| *Іваненко І. І.* |  |

Київ — 2022

ЗМІСТ

[ЗАВДАННЯ 2](#_Toc96528890)

[Основні теоретичні відомості з шифру Віженера 3](#_Toc96528891)

[Завдання з шифру Віженера 3](#_Toc96528892)

[Основні теоретичні відомості з шифру двійкового гамування 4](#_Toc96528893)

[Завдання з шифру двійкового гамування 4](#_Toc96528894)

[Список літератури 5](#_Toc96528895)

[Додаток 1 6](#_Toc96528896)

[Додаток 2 7](#_Toc96528897)

# ЗАВДАННЯ

***Мета роботи:*** розробити криптосистеми на основі шифрів Віженера та двійкового гамування.

1. Обрати початковий текст англійською, українською або російською мовою довжиною від 8 до 20 символів, та ключове слово від 3 до 8 символів. Зашифрувати текст, користуючись шифром Віженера. Алфавіт, криптотекст та ключ записати в [Таблицю\_3](https://docs.google.com/spreadsheets/d/1Fqu6vkzaJYX1mQPbSPU4A1CSVkOK_MHggPLZTmA6gzA/edit?usp=sharing) в СВІЙ РЯДОК у стовпчики AF, AG, AH. Перед шифруванням пробіли з початкового тексту необхідно видалити. (*1 бал*).

2. Користуючись наданим ключем, розшифрувати отриманий криптотекст за алгоритмом Віженера (завдання дивитись в [Таблиці\_3](https://docs.google.com/spreadsheets/d/1Fqu6vkzaJYX1mQPbSPU4A1CSVkOK_MHggPLZTmA6gzA/edit?usp=sharing) у рядку НАД СВОЇМ). Відповідь записати в рядок НАД СВОЇМ у стовпчик AI. (*1 бал*)

3. Написати програмний код для шифрування - розшифрування за шифром Віженера. Продемонструвати роботу створеної програми на контрольних прикладах. (*2 бали*)

4. Обрати початковий текст англійською, українською або російською мовою довжиною від 8 до 15 символів (ім'я відомої особистості, відома назва пісні чи групи, комп'ютерна гра, тощо). Записати символи початкового тексту у двійковому вигляді, користуючись кодовою таблицею сp866.

5. Згенерувати ключ - псевдовипадкову гамму, довжина якої дорівнює або більша довжини початкового тексту. Записати ключ у двійковому вигляді в [Таблицю\_4](https://docs.google.com/spreadsheets/d/1TzJmWgV5XCRY0FRKcvfvVlcJ3Yhk3TgyJc02ud0XWRo/edit?usp=sharing) в СВІЙ рядок, стовпчик AG. Значення ключа повинно бути унікальним в стовпчику AG. (*1 бал*)

6. **Шифрування:** для початкового тексту та згенерованого ключа виконати побітово операцію XOR. Отриманий криптотекст у двійковому вигляді записати в [Таблицю\_4](https://docs.google.com/spreadsheets/d/1TzJmWgV5XCRY0FRKcvfvVlcJ3Yhk3TgyJc02ud0XWRo/edit?usp=sharing) в СВІЙ рядок, стовпчик AH. (*1 бал*)

7. **Розшифрування** (завдання дивитись в [Таблиці\_4](https://docs.google.com/spreadsheets/d/1TzJmWgV5XCRY0FRKcvfvVlcJ3Yhk3TgyJc02ud0XWRo/edit?usp=sharing) у рядку НАД СВОЇМ): користуючись наданим ключем, розшифрувати отриманий криптотекст за алгоритмом XOR. Відповідь записати в рядок НАД СВОЇМ: у стовпчик AI - у двійковому вигляді, у стовпчик AJ - у вигляді тексту згідно з таблицею cp866. (2 *бали*)

8. Написати програмний код для шифрування - розшифрування за шифром двійкового гамування. Продемонструвати роботу створеної програми на прикладах. (*1 бал*)

9. Оформити звіт. (*1 бал*)

# Основні теоретичні відомості з шифру Віженера

# Завдання з шифру Віженера

# Основні теоретичні відомості з шифру двійкового гамування

# Завдання з шифру двійкового гамування

# 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. Сингх С. Книга шифров. Тайная история шифров и их расшифровки, Пер. с англ. – М.: «Астрель», 2007. – 447 с.

# Додаток 1

Текст програми, що реалізує криптосистему Віженера

# Додаток 2

Текст програми, що реалізує криптосистему з використанням двійкового гамування