# ЛАБОРАТОРНА РОБОТА 1

**ШИФРИ ЗАМІНИ**

**Мета роботи:** вивчити теоретичні основи побудови шифрів заміни, провести зашифрування відкритого і розшифрування шифрованого повідомлення. Усвідомити сильні і слабкі сторони шифрів заміни.

## **Короткі теоретичні відомості**

Шифри заміни (підстановки) – це алгоритми шифрування, при якому кожен знак вихідного тексту заміняється шифропозначенням – одним, або декількома знаками деякого набору символів (алфавіту).

Шифри заміни поділяються на моноалфавітні та поліалфавітні. У моноалфавітних шифрах підстановки літера (або символ) у початковому тексті завжди змінюється на ту саму літеру (або символ) у зашифрованому тексті незалежно від її позиції в тексті. Очевидні слабкі сторони шифрів моноалфавітної підстаноівки – у шифрованому тексті зберігаються всі частотні характеристики відкритого тексту, усі сполучення і повторення.

Найпростіший моноалфавітний шифр підстановки — адитивний шифр, його іноді називають шифром зсуву, а іноді — шифром Цезаря, але термін “адитивний шифр” краще показує його математичний сенс. Зашифрування текстових повідомлень за допомогою адитивних шифрів підстановки здійснюється за допомогою формули:

*довжина алфавіту***; *М* –** *відкритий текст***; С-** *шифртекст*;

***K –*** *ключ (ціле число в* ***)***

Розшифрування здійснюється відповідно за формулою:

Зашифрування текстових повідомлень за допомогою *мультипліктивних* шифрів заміни здійснюється за формулою:

а розшифрування відповідно за формулою:

**Хід роботи**

**2.** За допомогою афінного алгоритму шифрування та даних ключів (таблиця 1) зашифрувати своє прізвище.

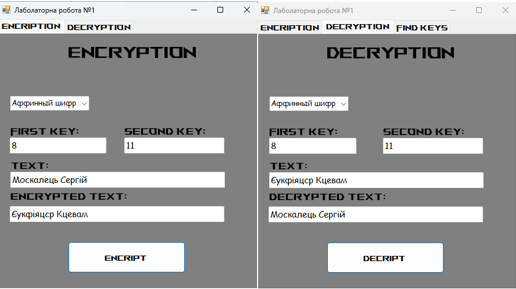


Рисунок 1.1 – Зашифроване повідомлення, розшифроване повідомлення

1. Розшифруйте шифртекст, отриманий за допомогою афінного алгоритму шифрування (ключі шифру відомі).

Таблиця 1

|  |  |  |  |
| --- | --- | --- | --- |
| Варіант | К1 | К2 | Шифтекст |
| 3 | 8 | 11 | КУЛ |

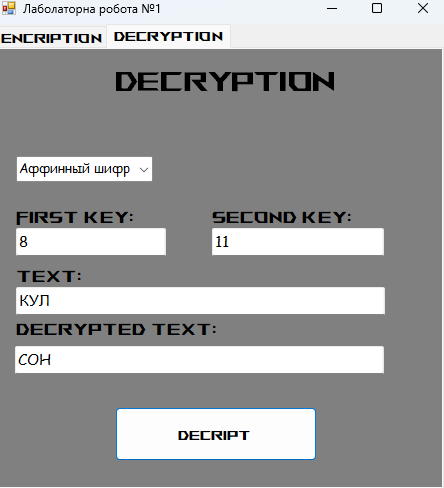


Рисунок 1.2 – розшифрований шифртекст

1. Відома пара відкритий текст-шифртекст (біграми). Відновіть ключі та запишіть формули, за якими відбувається шифрування і розшифрування.

Таблиця 2

|  |  |  |
| --- | --- | --- |
| Варіант | Відкритий текст | Шифртекст |
| 3 | Ло | ВЖ |

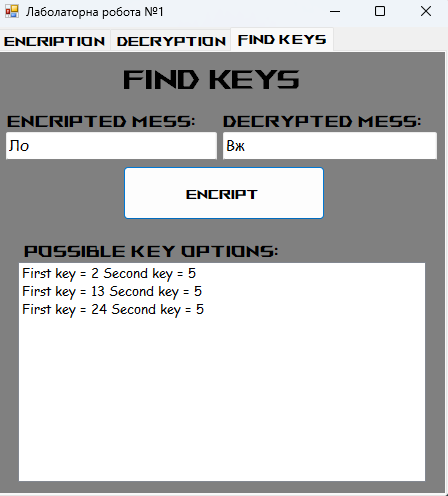


Рисунок 1.3 – пошук ключів

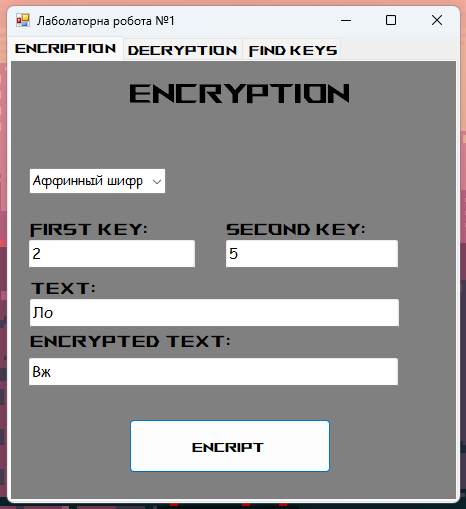


Рисунок 1.4 – перевірка ключів

1. За допомогою шифру Віженера та ключового слова зашифруйте фразу з книги Л. Керрола « Аліса в країні чудес».

Таблиця 3

|  |  |  |
| --- | --- | --- |
|  | **Фраза для шифрування** | Ключ |
| 3 | Чого варта книжка без малюнків та розмов | Шифр |

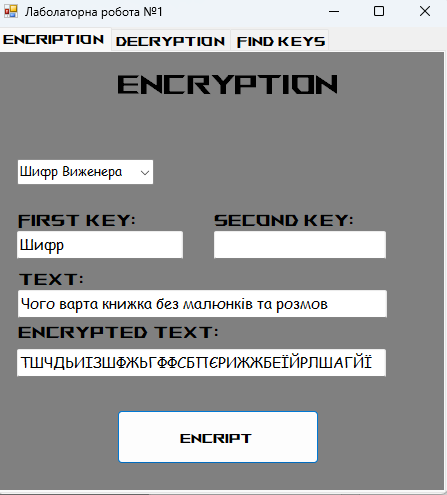


Рисунок 1.5 – Шифр Віженера зашифроване повідомлення

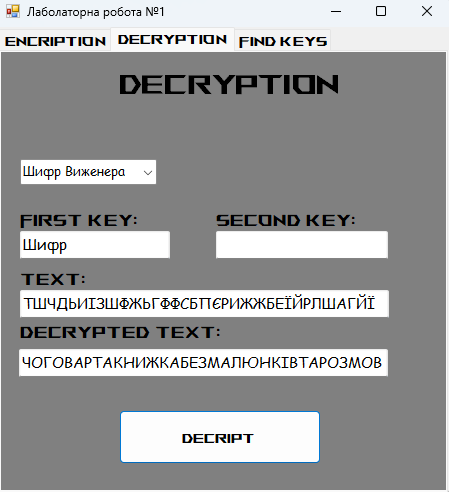


Рисунок 1.6 – Шифр Віженера розшифроване повідомлення

1. Зашифруйте фразу з попереднього завдання за допомогою шифру Плейфера.

Таблиця 4

|  |  |  |
| --- | --- | --- |
|  | **Фраза для шифрування** | Ключ |
| 3 | Чого варта книжка без малюнків та розмов | Шифр |



Рисунок 1.7 – Шифр Плейфера зашифроване повідомлення

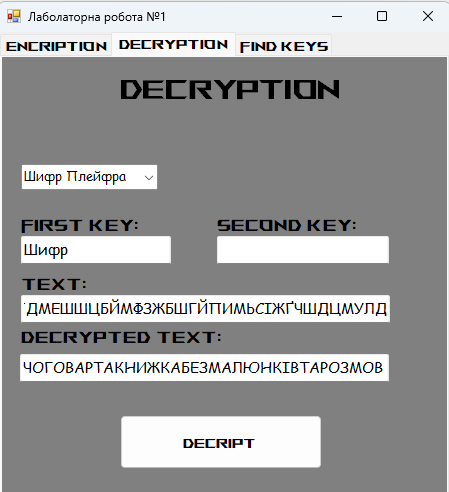


Рисунок 1.7 – Шифр Плейфера розшифроване повідомлення

**Висновок**

На даній лаболаторній роботі ми вивчили теоретичні основи побудови шифрів заміни, провесли зашифрування відкритого і розшифрування шифрованого повідомлення. Усвідомили сильні і слабкі сторони шифрів заміни.