Шифри існують вже багато століть, але найбільшу популярність вони отримали тільки при появі інтернету та способів комунікації в ньому. На даний момент існує велика кількість сфер, де використовуються шифри, починаючи із захисту особистої інформації в інтернеті, закінчуючи армією та воєнними справами.

В даному випадку розглянемо лікарні. Часто у пацієнтів, які не можуть встати є потреба в спілкуванні, але родичі не можуть бути поряд не весь час. Але через те, що в лікарнях часто стоїть старе або дуже слабке обладнання на нього не можна поставити програми для спілкування в інтернеті. Саме для цього і був розроблений мій чат. Тому, що його можна запускати на будь-якому пристрої. Але з’являється проблема – зловмисники можуть потрапити до лікарні, та перехоплювати повідомлення. Саме для цього і були розроблені алгоритми шифрування.

Основна ціль цієї роботи – створити та порівняти алгоритми шифрування на прикладі чату.

Сам чат був написаний за допомогою мови програмування python 3.7.4, та за допомогою бібліотеки . Що дозволяє запускати програму на будь-яких пристроях, та потребує малу потужність від клієнта. Програма – кросплатформена, тому що код на мові програмування python можна відкомпілювати під будь-яку систему.

Для реалізації цієї задачі буде порівняно роботу табличних шифрів, блочних шифрів, та шифру, який не піддається дешифруванню.

Також в цій роботі буде створений власний шифр, який в собі поєднує ідею блочних шифрів та реалізацію найвідомішого табличного шифру – шифру Віженера.

На прикладі розробленої програми розглянемо та проаналізуємо вже відомі алгоритми шифрування даних, та порівняємо їх з одним новим алгоритмом.

Для виконання цієї задачі необхідно:

1. Охарактеризувати та розглянути вже відомі алгоритми шифрування.
2. Охарактеризувати та створити новий алгоритм шифрування.
3. Створити тести для деяких алгоритмів.
4. Порахувати асимптотику роботи алгоритмів та протестувати їх в реальних умовах.
5. Порівняти роботу алгоритмів шифрування.
6. Знайти оптимальний варіант для шифрування даних.
7. Охарактеризувати, в яких умовах краще використовувати які алгоритми.

Дане дослідження може бути застосоване при розробці програм, вхідні дані якої – рядок символів, та потрібно його зашифрувати чи дешифрувати.