У шифрі Цезаря кожна літера зсувається на кілька позицій. Наприклад в шифрі Цезаря при зсуві на 2 символи праворуч A стане C, а X набуде значення Z. Шифр Віженера – поліалфавітний шифр, який складається з послідовності кількох шифрів Цезаря із різними зсувами. Для шифровки повідомлень може використовуватись таблиця алфавітів, чи як її ще називають – квадрат (таблиця) Віженера. Розмір (довжина сторони) таблиці Віженера дорівнює кількості символів в алфавіті. Таким чином застосовуючи шифр Віженера до латинського алфавіту вийде квадрат із стороною в 26 символів, тобто буде 26 різних шифрів Цезаря. На кожному етапі шифрування буде застосований окремий шифр Цезаря, засновуючись на літері ключового та секретного слів.

Працює шифр наступним чином. Людина, яка надсилає повідомлення записує ключове слово циклічно, доки довжина його не буде дорівнювати повідомленню. Після цього iй символ в шифротексті буде дорівнювати перетину iго символу в повідомленні та ключовому слові у таблиці.

Щоб розшифрувати текст потрібно у стовбці із iм символом ключа знайти iй символ шифротесту, тож iм символом повідомлення буде перший символ у рядку, який містить iй символ шифротесту.

///

Перейдемо до криптоаналізу. Шифр Віженера ховає частоти з’явлення символів в тексті, але деякі особливості залишаються. Головним недоліком цього шифру є те, що в нього повторюється ключ. Тому криптоаналіз шифру Віженера може бути побудований в два етапи. Потрібно підібрати довжину ключа. Це можна зробити беручі кожну другу літеру в тексті, потім кожну третю і.т.п. Коли розподіл літер буде сильно відрізнятися від рівномірного, тоді можна казати про довжину ключа. В другому етапі дешифрується велика кількість шифрів Цезаря [3].