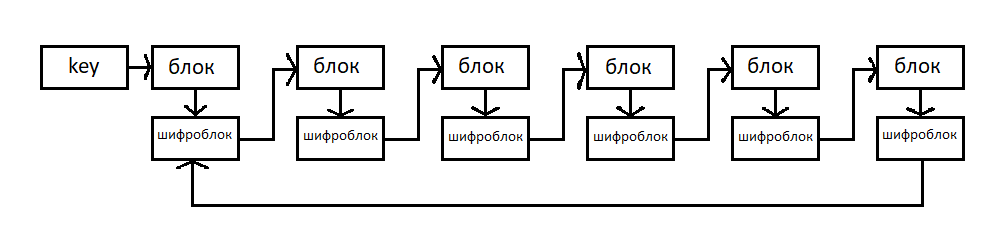
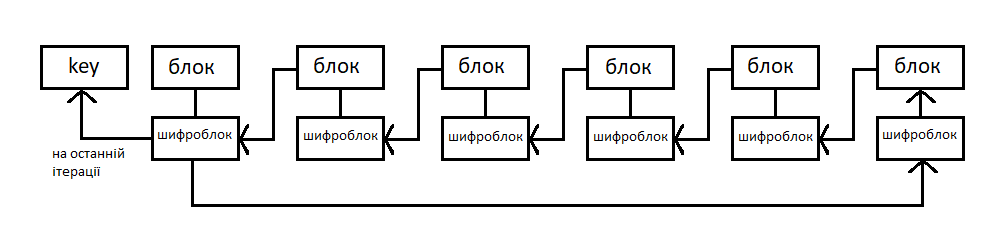
Мій шифр поєднує в собі ідею блочних шифрів, та шифр Віженера. Саме тому він біде стійкий до атак, які застосовуються до шифру Віженера. Працює мій шифр досить просто. Для початку формується алфавіт(в мене це латинські символи з до ). Потім зіставляється таблиця Віженера, але перед цим я формую псевдовипадкову послідовність чисел від 1 до 26, і перемішую алфавіт згідно із послідовністю. Після формування таблиці, алгоритм розбиває текст на блоки довжини ключа, та зашифровує текст використовуючи алгоритм Віженера для блоку, як відкритого тексту, і вектору ініціалізації, як для ключа. Коли алгоритм доходить до останнього блоку, він присвоює вектору ініціалізації значення зашифрованого останнього блоку, і далі повторює все с початку ще разів.



Дешифрування проходить за схожим алгоритмом. Шифротекст розбивається на блоки довжини ключа. Потім, використовуючи шифр Віженера, дешифрується шифротекст(блок), використовуючи ключ, як минулий блок. А на останній ітерації цей алгоритм використовує сам ключ, як ключ для дешифрації.



Щоб розшифрувати повідомлення зловмиснику потрібно знати довжину ключа, кількість проходів, та сам ключ. Бо якщо зловмисник буде знати лише ключ, то йому знадобиться багато часу, щоб підібрати кількість проходів. А якщо зловмисник знає лише кількість проходів, йому знадобиться підбирати ключ, що не є гарною ідеєю. Також людина, яка спробує вкрасти повідомлення не зможе дізнатися довжину ключа керуючись методом Касікі, тому що для цього йому буде потрібно знати довжину ключа та кількість проходів.

Цей алгоритм був реалізований на мові програмування python 3.7.4. Користувався я цією мовою програмування тому, що я хотів показати ці алгоритми на прикладі простого консольного чату. Чат був написаний використовуючи бібліотеку socket. Я використовував UDP протокол для зв’язку сервера із клієнтом.