2. Шифрування даних є дуже важливою складовою сьогодення, та використовується в багатьох сферах: авторизація на сайтах, відправленні повідомлень, воєнній сфері, тощо…

Основна ціль моєї роботи – знайти оптимальний алгоритм шифрування для відправки повідомлень великих розмірів за допомогою обладнання будь якої потужності. Це потрібно для обміну інформацією в таких закладах, як лікарні, соціальні центри, і тому подібні..., які не можуть собі дозволити використовувати високо потужну техніку.

3. Для порівняння різних шифрів був розроблений консольний чат, що має низькі вимоги до комп’ютера. Для шифрування даних використовуються табличні, блочні та потокові шифри.

4. Найвідомішим представником табличних шифрів є шифр Віженера. Він формує квадратну таблицю довжини кількості символів в алфавіті, і формує і-й символ шифротексту, як перетин і-го символу відкритого тексту та і-го символу ключа в цій таблиці. Цей шифр працює за лінійний час, але має величезний недолік – існує метод по взлому цього шифру.

5. Представником потокових шифрів є шифр Вєрнама. Для цього шифру доведена його абсолютна криптостійкість. Але в нього також є недолік, із-за якого його використовувати майже неможливо. Він присвоює різні числа в двійковому записі для кожного символу алфавіту, після чого формує випадкові числа, кількість яких дорівнює довжині тексту, і додає їх за модулем 2. Недоліком цього шифру є той факт, що для кожного повідомлення потрібні нові випадкові числа обом сторонам.

6. Блочний шифр – різновид симетрічного шифру оперуючий групами біт фіксованої довжини. Блочні шифри реалізуються шляхом багатократного застосування до блоків відкритого тексту деяких базових перетворень. До переваг блочних шифрів відносять схожість процедур шифрування та дешифрування, а також високу криптостійкість. Основними недоліками є маленька довжина ключа та ,відповідно, можливість його підбору.

7. Поєднавши ідеї блочних та табличних шифрів був розроблен шифр стійкий до атак методом Касіскі та до атак по масці. Принцип його роботи полягає в тому, що спочатку формується квадрат Віженера, перший ряд якого складається з будь-якої комбінації різних символів алфавіту, а кожний з наступних рядків є ціклічний зсув попереднього рядку на одну клітинку праворуч, де останній символ становиться на місце першого. Далі відкритий текст розбивається на блоки довжини ключа.

8. В першому раунді перший блок шифрується шифром Віженера, де вектором ініціалізації є ключ. Кожен з наступних блоків використовує вектор ініціалізації рівний минулому шифроблоку. А на всіх інших раундах для першого блоку вектором ініціалізації буде останній шифроблок. Це зроблено для того, щоб достигнути лавинного ефекту, і щоб зміна будь-якого символу призвела до зміни всього шифротексту.

9. Час роботи програми та надійність залежить від кількості раундів. Чим воно більше, тим надійніше шифрування і більше час роботи. Чим менше раундів, тим швидше працює шифр, але гірше шифруються дані.

10. Подивимось на порівняльну таблицю шифрів.

11. Шифр Віженера працює за лінійний час, але піддається дешифруванню. Шифр Вєрнама абсолютно криптостійкий, але для його праці потрібна генерація випадкових чисел, що не входить в концепт чату. Шифр DES працює за квадратний час, і є можливість підбору ключа.

12. Час роботи розробленого можна змінювати, змінюючи кількість раундів, тим самим збільшуючи або зменшуючи його криптостійкість та час праці.

13. Порівняльний аналіз залежності часу роботи програми від довжини відкритого тексту можна побачити на цьому графіку.

14. Отже для вирішення даного завдання не можна використовувати шифр Вєрнама через необхідність в генерації великої кількості випадкових чисел. Шифр Віженера не можна використовувати також через легке його дешифрування. Шифр DES краще використовувати на невеличких повідомлення, а на великих краще всього застосувати розроблений шифр.

15. Дякую за увагу.

#### Описание DES

Но для начала кратко опишем работу алгоритма. О DES сказано уже достаточно. Полное описание шифра можно найти на [Википедии](https://ru.wikipedia.org/wiki/DES). Однако для дальнейшего объяснения атаки нам потребуется ряд определений которые лучше ввести заранее.  
  
Итак, DES это блочный шифр, основанный на [сети Фейстеля](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F). Шифр имеет размер блока 64 бита и размер ключа 56 бит. Рассмотрим схему шифрования алгоритма DES.

Как видно из рисунка, при шифровании над текстом производятся следующие операции:

1. Начальная перестановка бит. На этом этапе биты входного блока перемешиваются в определенном порядке.
2. После этого перемешанные биты разбиваются на две половины, которые поступают на вход функции Фейстеля. Для стандартного DES сеть Фейстеля включает 16 раундов, но существуют и другие варианты алгоритма.
3. Два блока, полученных на последнем раунде преобразования объединяются и над полученным блоком производится еще одна перестановка.

Рассмотрим операции, выполняющиеся на этом этапе:

1. Входной блок проходит через функцию расширения E, которая преобразует 32-битный блок в блок длиной 48 бит.
2. Полученный блок складывается с раундовым ключом Ki.
3. Результат предыдущего шага разбивается на 8 блоков по 6 бит каждый.
4. Каждый из полученных блоков Bi проходит через функцию подстановки S-Boxi, которая заменяет 6-битную последовательность, 4-битным блоком.
5. Полученный в результате 32-битный блок проходит через перестановку P и возвращается в качестве результата функции f.