

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное  
учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

---

КАФЕДРА №51

ОТЧЕТ ЗАЩИЩЕН С ОЦЕНКОЙ \_\_\_\_\_

ПРЕПОДАВАТЕЛЬ

ассистент

М.Н.Исаева

---

должность, уч. степень, звание

---

подпись, дата

---

инициалы, фамилия

**ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1**

**ИСТОРИЧЕСКИЕ ШИФРЫ. АФФИННЫЙ ШИФР.**

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ  
ИНФОРМАЦИИ

СТУДЕНТ ГР. № 5912

И.К. Лобач

---

номер группы

---

подпись, дата

---

инициалы, фамилия

Санкт-Петербург 2021

1 Цель работы: реализация подстановочного аффинного шифра в режимах шифрования и дешифрования, проведение частотного анализа, нахождение расстояния единственности и анализ криптостойкости алгоритма.

## 2 Описание работы

Подстановочный аффинный шифр реализуется следующим образом: каждой букве алфавита размера  $N$  с порядковым номером  $x$  ставится в соответствие новая буква с порядковым номером, вычисленным согласно функции шифрования  $E(x)$ :

$$E(x) = (ax + b) \bmod N$$

где  $E(x)$  – порядковый номер новой буквы, заменяющей старую в шифротексте,  $a, b$  – ключи шифра. Чтобы шифротекст возможно было расшифровать,  $a$  и  $N$  должны быть взаимнопростыми числами.

Для дешифрования каждой букве шифротекста с порядковым номером  $x$  ставится в соответствие буква, порядковый номер которой вычисляется согласно функции расшифрования  $D(x)$ :

$$D(x) = a^{-1}(x - b) \bmod N$$

где  $a^{-1}$  – обратное число к  $a$  по модулю  $N$ . Иначе говоря,  $1 \equiv aa^{-1} \bmod N$ .

## 3 Описание реализации

Исходный текст считывается из файла “In.txt”. Ключи  $a, b$  вводятся пользователем. Предусмотрена и псевдослучайная генерация ключей. Затем проверяется выполнение условия взаимной простоты мощности алфавита  $N$  и ключа  $a$ . Проверка осуществляется по алгоритму Евклида. В случае нарушения выполнения программа аварийно завершается.

Затем происходит посимвольное чтение файла. Каждый символ с ключами передается в функцию шифрования. Полученному номеру сопоставляется буква алфавита (по умолчанию в программе используется английский алфавит с  $N = 26$ ) и выводится в файл “Result.txt”. Знаки препинания, разделители и цифры не шифруются и сохраняются в шифротексте. Заглавные буквы шифруются в заглавные, строчные в строчные.

При чтении файла осуществляется подсчет количества букв для частотного анализа. Эти данные затем выводятся в виде гистограммы в отдельном файле.

Аналогично осуществляется процедура расшифрования.

#### 4 Пример работы программы

Продemonстрируем работу алгоритма.

При запуске программы пользователю предложено ввести два ключа (см.ниже).

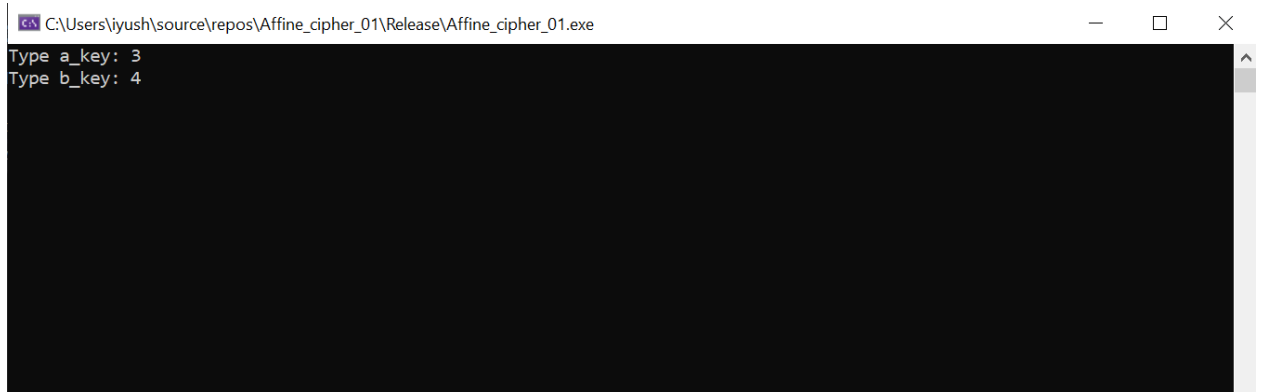


Рисунок 1 - Ввод ключей

Если ввести ключи, не удовлетворяющие условию, то программа завершит свое выполнение (см. ниже). В данном случае  $\text{НОД}(26,2) = 13 \neq 1$ , следовательно, ввод некорректный.

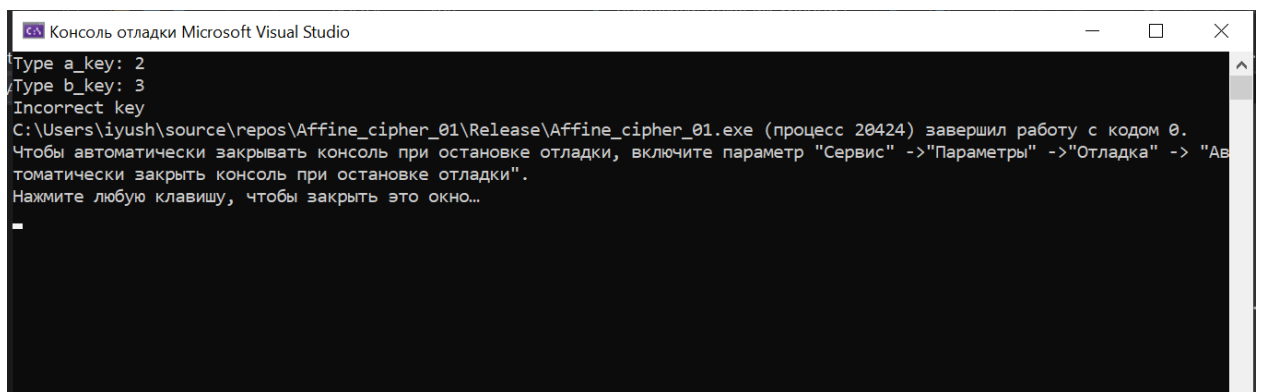


Рисунок 2 - Некорректный ввод ключей

Пусть файл с исходным текстом выглядит следующим образом (см. ниже).

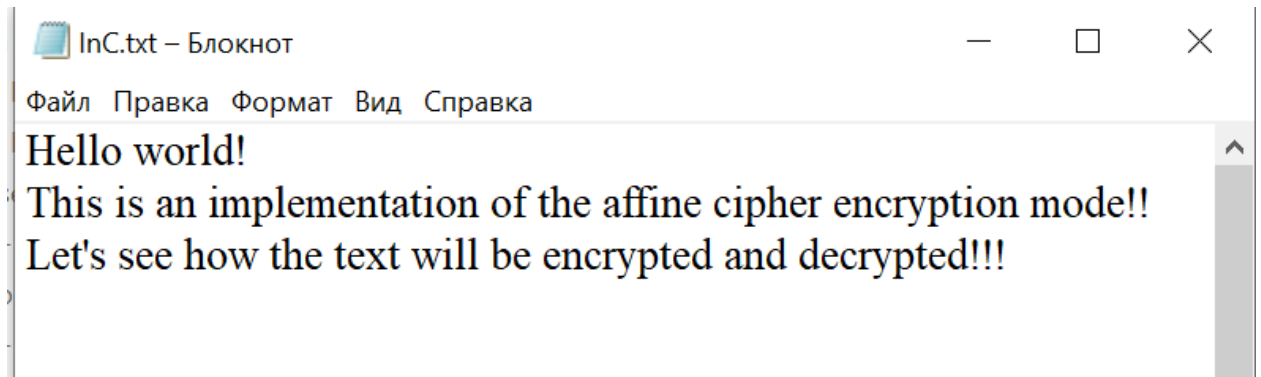


Рисунок 3 - Исходный текст

В файле "Out.txt" мы увидим следующее (см. ниже).

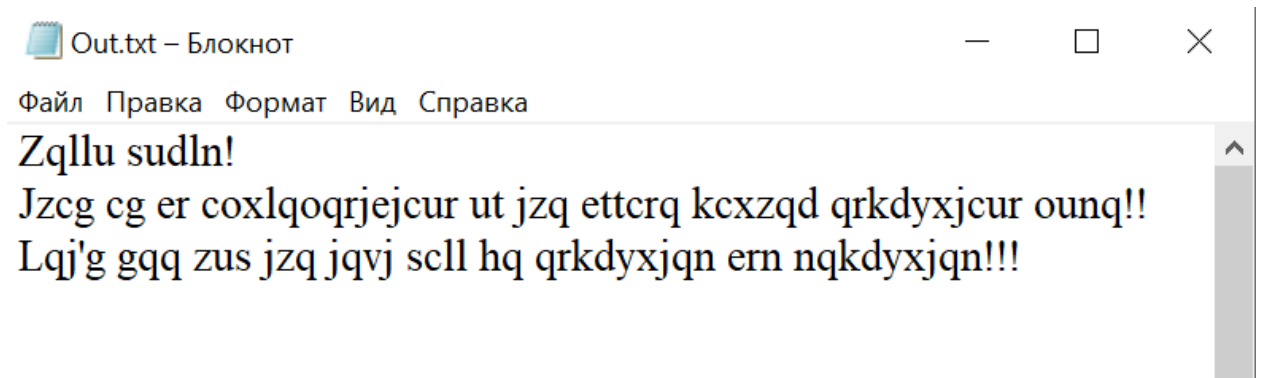


Рисунок 4 – Шифротекст

Если этот файл подать на вход функции расшифрования, то мы увидим следующее (см. ниже).

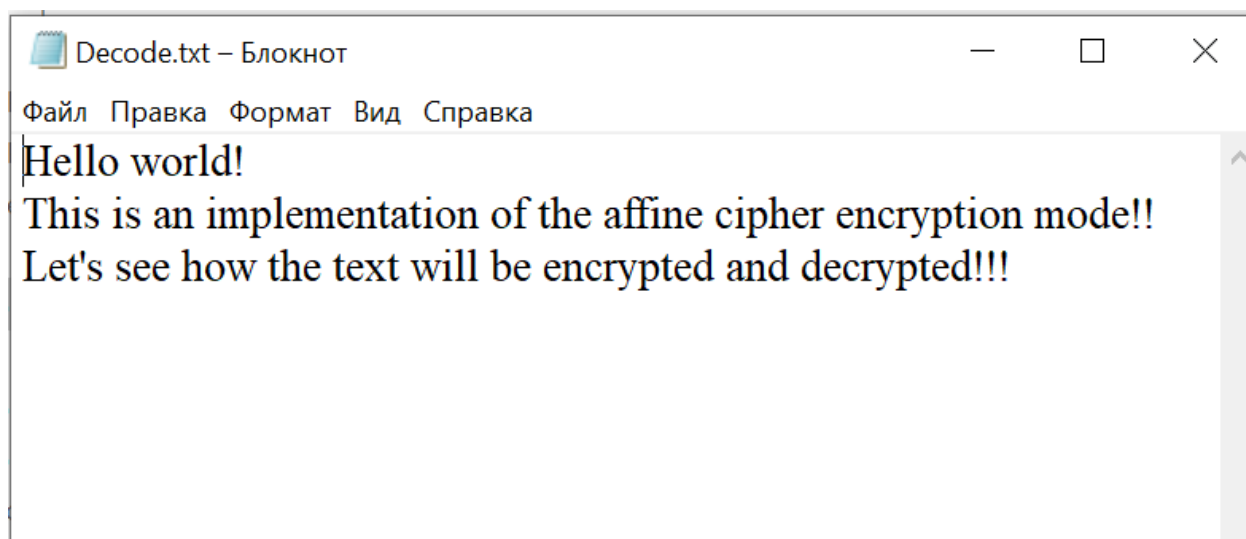


Рисунок 5 - Расшифрованный текст

Отсюда, можно сделать вывод о корректной реализации алгоритма, т.к. дешифрованный текст полностью совпадает с исходным.

## 5 Результаты исследования

Проведем частотный анализ исходного текста и шифротекста, построим гистограммы.

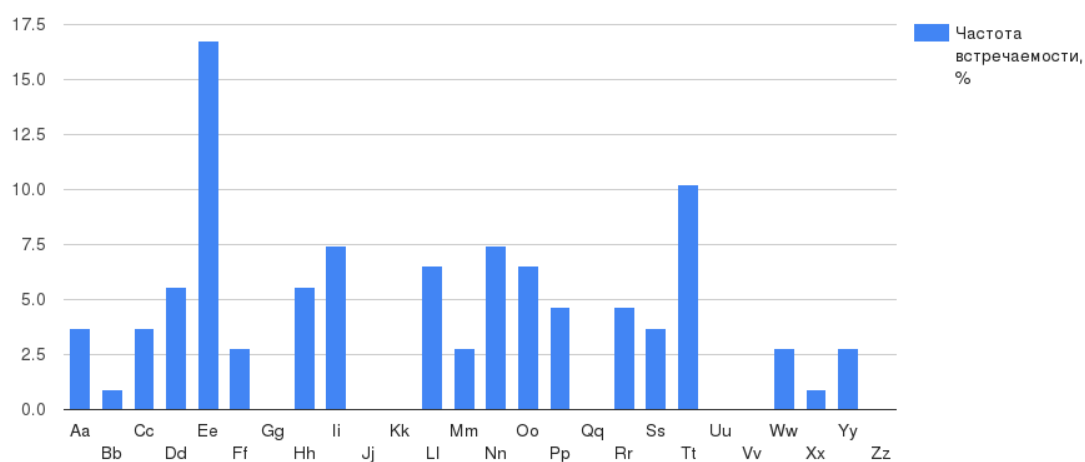


Рисунок 6 - Частотный анализ исходного текста

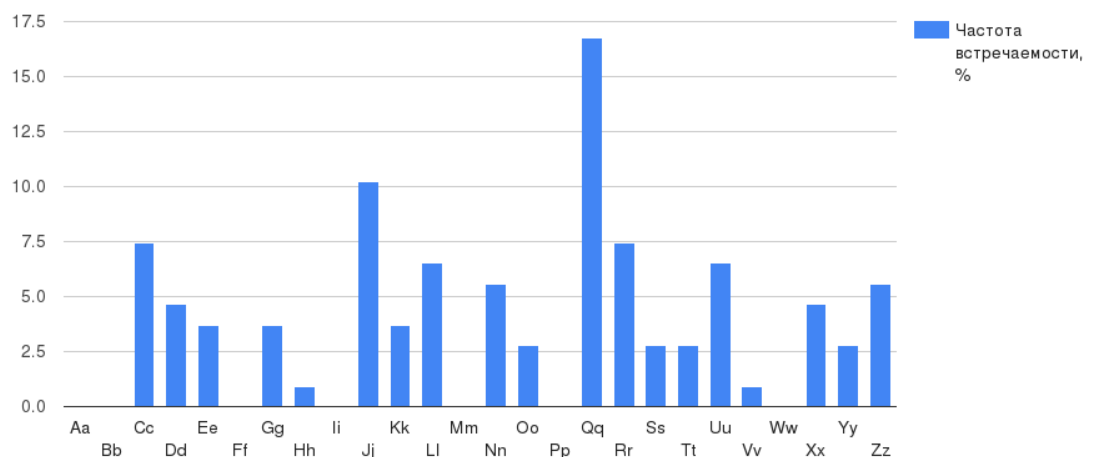


Рисунок 7 - Частотный анализ шифротекста

Расстояние единственности - это минимальная длина шифрованного текста, необходимого для однозначного восстановления истинного ключа шифра. Нахождение расстояния единственности  $L$  осуществляется по формуле:

$$L \geq \frac{\log_2 |K|}{D \log_2 N}$$

где  $|K|$  - количество ключей шифра,  $D$  - избыточность языка (для английского алфавита  $D \approx 0,68$ ).

Определим количество ключей: ключ  $a$  – всевозможные значения в интервале  $0, 1 \dots N - 1$ , взаимнопростых с  $N$ . Таких чисел, согласно функции Эйлера,  $\varphi(N) = \varphi(26) = 12$ . Ключ  $b$  принимает значения  $0, 1 \dots N - 1$ .

Отсюда,  $|K| = 12 * 26 = 312$  возможных ключей. Таким образом,  $L \geq 2,6$

6 Вывод:

В ходе выполнения работы реализовала подстановочный аффинный шифр в режимах шифрования и дешифрования, провела частотный анализ, определила расстояние единственности.

На основе данных исследований проведем анализ криптостойкости: ограниченное количество ключей (всего их 312) приводит к тому, что система крайне не криптостойка. Основная уязвимость шифра заключается в том, что криптоаналитик может выяснить (путём частотного анализа, полного

перебора, угадывания или каким-либо другим способом) соответствие между двумя любыми буквами исходного текста и шифротекста. Тогда ключ может быть найден путём решения простой системы уравнений. Кроме того, условие взаимной простоты  $N$  и  $a$  существенно уменьшает количество проверяемых ключей.

### **Используемые источники.**

1. А.А. Овчинников «Исторический шифры»
2. С.А. Сушко Практическая криптология, лекция 4
3. В.С. Пилиди «Криптография. Вводные главы»