Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
О ПРАКТИЧЕСКОЙ РАБОТЕ № 1
по дисциплине «Криптографические методы защиты информации»
Подстановочные шифры

Студент гр. 211
А. М. Павленко
«9» декабря 2022 г.

Руководитель
Заведующий кафедрой информационной безопасности киберфизических систем
канд. техн. наук, доцент
_____О.О. Евсютин
«___» _____ 2022 г.

Москва 2022

СОДЕРЖАНИЕ

1 Задание на практическую работу

Целью работы является Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к простым подстановочным шифрам.

В рамках практической работы необходимо выполнить следующее:

1. Написать программную реализацию следующих шифров:
   - шифр простой замены
   - аффинный шифр
   - аффинный рекуррентный шифр
2. Изучить методы криптоанализа моноалфавитных подстановочных шифров с использованием дополнительных источников
3. Провести криптоанализ данных шифров
4. Подготовить отчет о выполнении работы Программа должна обладать следующей функциональностью для каждого из реализованных в ней шифров:
   1) принимать на вход произвольную последовательность символов, вводимую пользователем в качестве открытого текста или шифротекста
   2) принимать на вход секретный ключ вида, соответствующего конкретному шифру
   3) осуществлять зашифрование или расшифрование введенного текста по выбору пользователя

2 Краткая теоретическая часть

2.1 Описание шифров

Простейшим примером подстановочного шифра является шифр простой замены.

Математически данный шифр может быть описан на языке подстановок.

Каждой букве алфавита A мощностью m ставится в соответствие число из диапазона $1 \dots m$ – другими словами, все символы алфавита нумеруются.

Множество возможных ключей шифра простой замены является симметрической группой степени m, то есть группой подстановок длины m является формула (1.1):

$$K = S(A) = S_m, \tag{1.1}$$

где K – множество возможных ключей;

A – алфавит;

m – мощность алфавита;

S_m – симметрическая группа степени m.

Открытый текст обозначим $x = (x_1, \dots, x_l)$, где $x_i \in A$, $i = \overline{1, l}$, соответствующий шифротекст – $y = (y_1, \dots, y_l)$.

Зашифрование открытого текста $x = (x_1, \dots, x_l)$ на ключе $k \in K$ может быть записано как (1.2):

$$E_k(x) = \big(k(x_1), \dots, k(x_l)\big), \tag{1.2}$$

где $E_k(x)$ – процесс зашифрования открытого текста x по ключу k;

k – ключ;

x – открытый текст.

Расшифрование шифротекста $y = (y_1, \dots, y_l)$ на том же ключе может быть записано как (1.3):

$$D_k(y) = \big(k^{-1}(y_1), \dots, k^{-1}(y_l)\big), \tag{1.3}$$

где $D_k(y)$ – процесс зашифрования шифротекста y по ключу k^{-1};

$k^{-1} \in K$ – подстановка, обратная k;

y – шифротекст.

Проще говоря, при зашифровании каждый символ текста заменяется на другой символ с помощью ключевой подстановки.

Известным частным случаем шифра простой замены является шифр Цезаря, названный так по имени использовавшего его всю жизнь древнеримского полководца. Данный шифр основан на использовании одного-единственного ключа – подстановки, полученной циклическим сдвигом элементов второй строки относительно первой на три позиции влево.

Другим частным случаем шифра простой замены является аффинный шифр, основанный на так называемом аффинном преобразовании. Данный шифр реализует замену символов открытого текста с использованием операций в кольце классов вычетов. Символы алфавита A мощностью m представляются элементами кольца классов вычетов $\mathbb{Z}_m$.

В качестве ключа аффинного шифра выступает пара значений $k = (\alpha, \beta),\ \alpha \in \mathbb{Z}_m^*,$ $\beta \in \mathbb{Z}_m$ соответственно ключевое пространство имеет вид $K = \mathbb{Z}_m^* \times \mathbb{Z}_m$

Открытый текст и шифротекст обозначим соответственно $x = (x_1, \dots, x_l)$ и $y = (y_1, \dots, y_l),$ где $x_i \in \mathbb{Z}_m,\ y_i \in \mathbb{Z}_m,\ i = \overline{1, l}.$

Зашифрование отдельного символа открытого текста осуществляется по формуле (1.4):

$$y_i = \alpha x_i + \beta, \tag{1.4}$$

где y_i – символ шифротекста, порядка i;

α, β – пара значений ключа;

x_i – символ открытого текста, порядка i;

$i = \overline{1, l}$, l это длина текста.

А вот расшифрование — по формуле (1.5):

$$x_i = (y_i - \beta) * \alpha^{-1}, \tag{1.5}$$

где y_i – символ шифротекста, порядка i;

α^{-1} – обратный элемент α

α, β – пара значений ключа;

x_i – символ открытого текста, порядка i;

$i = \overline{1, l}$, l это длина текста.

Усилением аффинного шифра является аффинный рекуррентный шифр, когда для каждого символа открытого текста вычисляется новое ключевое значение на основе предыдущего. Для этого необходимо задать две ключевые пары $k_1 = (\alpha_1, \beta_1)$, $k_2 = (\alpha_2, \beta_2)$ и тогда ключевая пара для произвольного символа преобразуемой последовательности будет иметь вид (1.6):

$$k_i = (\alpha_{i-1} * \alpha_{i-2}, \beta_{i-1} + \beta_{i-2}), \tag{1.6}$$

где k_i – номер ключа порядка i;

α, β – пара значений ключа;

$i = \overline{3, l}$, l это длина текста.

2.2 Методы криптоанализа шифров

Криптоанализ шифра простой замены

Криптоанализ шифра простой замены проводится с помощью частотного анализа.Он основан на том, что с точностью до обозначений частотные характеристики символов шифротекста и открытого текста одинаковы. Частотный анализ можно разделить на 3 этапа:

Первый этап. Считаем частоту встречаемости символов в шифротексте и записываем в порядке убывания все символы с вероятностью появления среди всех символов шифртекста.

Второй этап. Смотрим таблицу частот используемого алфавита (можно найти в Интернете) и приводим взаимно-однозначное соответствие символов с одинаковыми частотами в шифротексте и в используемом алфавите.

Третий этап. После чего, по получившемуся соответствию, меняем в шифротексте символы и получаем открытый текст.

Главным достоинством частотного криптоанализа является простота в реализации и быстрый взлом шифра. Главным минусом данного вида криптоанализа является то, что данный метод работает только на достаточно больших текстах (от 5000 символов в общем случае) и осмысленных последовательностях, так как основан на частоте использования конкретных символов в используемых алфавитах.

Криптоанализ аффинного шифра

Так как аффинный шифр является моноалфавитным шифром замены, то он обладает всеми уязвимостями этого класса шифров. Например, для случая использования латинского алфавита из 26 букв, число возможных a равно 13 вариантам. b может принимать 26 различных значений. Значит существует всего 338 возможных вариантов ключей для этого алфавита, что позволяет методом «грубой силы» подобрать ключи.

Также можно применить метод частотного криптоанализа, если текст достаточно большой. Чем больше размер текста, тем лучше и точнее работает этот метод. Метод основан на подсчете встречаемости каждой буквы в шифротексте и сравнении результатов с реальной встречаемостью букв в используемом алфавите. В данном случае частотный анализ можно разделить на 4 этапа:

Первый этап. Считаем частоту встречаемости символов в шифротексте и записываем в порядке убывания все символы с их вероятностью появления среди всех символов.

Второй этап. Смотрим таблицу частот используемого алфавита (можно найти в Интернете) и находим одинаковые частоты у некоторых символов шифротекста и символов алфавита.

Третий этап. По полученным на втором этапе символам строим уравнения, из которых находим всевозможные коэффициенты a, b исходного ключа.

Четвертый этап. Используя формулы расшифрования и полученные на третьем этапе значения ключа, проводим расшифрование шифротекста в открытый текст. Если на данном этапе мы получаем неверную последовательность символов в открытым тексте (если мы, например, знаем, что должны получить осознанный текст, а получаем не осознанный), то повторяем этапы 2–4 с другим символом шифротекста.

Данный метод криптоанализа достаточно прост в реализации, но имеет те же недостатки, что и при частотном криптоанализе шифра простой замены, но также еще главным недостатком является то, что необходимо перебирать все возможные значения коэффициентов ключа (данный недостаток может пропадать при достаточно большой длине шифротекста, так как мы можем рассчитывать значения ключа для нескольких элементов и брать пересечения).

Криптоанализ аффинного рекуррентного шифра

Аффинный рекуррентный шифр устойчив к частотному криптоанализу, так как один и тот же символ открытого текста может быть зашифрован в любой символ шифротекста за счет постоянной смены значений ключа. Данный шифр является устойчивым к криптоанализу и может быть взломан лишь методом “грубой силы”. Однако, имея ключ, но не имея информации о нем, возможно получение исходного текста путем многократного повторного шифрования. После многократного повторения шифрования (на некоторой итерации) шифротекст превратится в читаемую строку, что и будет начальной строкой

3 Примеры шифрования

Пример «ручного» шифрования путём простой замены:

Открытый текст(X) – СКРЫТЫЙ ТЕКСТ

Ключ указан в таблице 1

Таблица 1 – группа подстановок

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Я	А	Е	Ж	Й	Т	З	Х	С	У	Щ	И	Ш	Ы	Н	Л	Ф	Э	Ю	П	Д	Ч	К	Г	В	Ъ	Ц	О	Ё	Б	М	Ь	Р

Берем необходимый символ из первой строки таблицы и заменяем на соответствующий символ во второй строке.

E(С) = Ю

E(К) = И

E(Р) = Э

E(Ы) = Ё

E(Т) = П

E(Ы) = Ё

E(Й) = Щ

E(Т) = П

E(Е) = Т

E(К) = И

E(С) = Ю

E(Т) = П

В итоге получаем шифротекст(Y) – ЮИЭЁПЁЩ ПТИЮП

Пример «ручного» расшифрования путём простой замены:

Шифротекст (Y) – ЮИЭЁПЁЩ ПТИЮП

Ключ указан в таблице 2

Таблица 2 – группа подстановок

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Я	А	Е	Ж	Й	Т	З	Х	С	У	Щ	И	Ш	Ы	Н	Л	Ф	Э	Ю	П	Д	Ч	К	Г	В	Ъ	Ц	О	Ё	Б	М	Ь	Р

Берем необходимый символ из второй строки таблицы и заменяем на соответствующий символ в первой строке.

D(Ю) = С

D(И) = К

D(Э) = Р

D(Ё) = Ы

D(П) = Т

D(Ё) = Ы

D(Щ) = Й

D(П) = Т

D(Т) = Е

D(И) = К

D(Ю) = С

D(П) = С

В итоге получаем открытый текст(X) – СКРЫТЫЙ ТЕКСТ

Результат расшифрования совпадает с открытым текстом до шифрования, следовательно шифрование и расшифрование проведено правильно.

Пример «ручного» аффинного шифрования:

Открытый текст(X) – СКРЫТЫЙ ТЕКСТ

Пара ключей – 13 10

С помощью формулы 1.4, вычисляем из символа открытого текста, символ шифротекста, при a = 13 (является взаимно простым числом с длиной алфавита) и b = 10

y(С) = a * x + b = 13 * 18 + 10 = 244 mod 33 = 13 = М

y(К) = a * x + b = 13 * 11 + 10 = 153 mod 33 = 21 = Ф

y(Р) = a * x + b = 13 * 17 + 10 = 231 mod 33 = 0 = А

y(Ы) = a * x + b = 13 * 28 + 10 = 374 mod 33 = 11 = К

y(Т) = a * x + b = 13 * 19 + 10 = 257 mod 33 = 26 = Щ

y(Ы) = a * x + b = 13 * 28 + 10 = 374 mod 33 = 11 = К

y(Й) = a * x + b = 13 * 10 + 10 = 140 mod 33 = 8 = З

y(Т) = a * x + b = 13 * 19 + 10 = 257 mod 33 = 26 = Щ

y(Е) = a * x + b = 13 * 5 + 10 = 75 mod 33 = 9 = И

y(К) = a * x + b = 13 * 11 + 10 = 153 mod 33 = 21 = Ф

y(С) = a * x + b = 13 * 18 + 10 = 244 mod 33 = 13 = М

y(Т) = a * x + b = 13 * 19 + 10 = 247 mod 33 = 26 = Щ

В итоге получаем шифротекст(X) – МФАКЩКЗ ЩИФМЩ

Пример «ручного» аффинного расшифрования:

Шифротекст(Y) – МФАКЩКЗ ЩИФМЩ

Пара ключей – 13 10

С помощью формулы 1.5, вычисляем из символа шифротекста, символ открытого текста, при a = 13 (является взаимно простым числом с длиной алфавита) и b = 10

$$a^{-1} = 28$$

x(М) = (y – b) * a^{-1} = (13 - 10) * 28 = 84 mod 33 = 18 = С

x(Ф) = (y – b) * a^{-1} = (21 - 10) * 28 = 308 mod 33 = 11 = К

x(А) = (y – b) * a^{-1} = (0 - 10) * 28 = -280 mod 33 = 17 = Р

x(К) = (y – b) * a^{-1} = (11 - 10) * 28 = 28 = Ы

x(Щ) = (y – b) * a^{-1} = (26 - 10) * 28 = 448 mod 33 = 19 = Т

x(К) = (y – b) * a^{-1} = (11 - 10) * 28 = 28 = Ы

x(З) = (y – b) * a^{-1} = (8 - 10) * 28 = -56 mod 33 = 10 = Й

x(Щ) = (y – b) * a^{-1} = (26 - 10) * 28 = 448 mod 33 = 19 = Т

x(И) = (y – b) * a^{-1} = (9 - 10) * 28 = -28 mod 33 = 5 = Е

x(Ф) = (y – b) * a^{-1} = (21 - 10) * 28 = 308 mod 33 = 11 = К

x(М) = (y – b) * a^{-1} = (13 - 10) * 28 = 84 mod 33 = 18 = С

x(Щ) = (y – b) * a^{-1} = (26 - 10) * 28 = 448 mod 33 = 19 = Т

В итоге получаем открытый текст(X)– СКРЫТЫЙ ТЕКСТ

Результат расшифрования совпадает с открытым текстом до шифрования, следовательно шифрование и расшифрование проведено правильно.

Пример «ручного» аффинного рекуррентного шифрования:

Открытый текст(X) – СКРЫТЫЙ ТЕКСТ

Пара ключей – 13 10 и 15 5

С помощью формулы 1.4, при изменяющихся ключей по формуле 1.6, вычисляем из символа открытого текста, символ шифротекста, при a = 13 и a = 15(является взаимно простым числом с длиной алфавита) и b = 10 и b = 5

y(С) = a * x + b = 13 * 18 + 10 = 244 mod 33 = 13 = М

y(К) = a * x + b = 15 * 11 + 5 = 170 mod 33 = 15 = Е

y(Р) = a * x + b = 30 * 17 + 15 = 525 mod 33 = 30 = Э (a = 30, b = 15)

y(Ы) = a * x + b = 21 * 28 + 20 = 608 mod 33 = 14 = Н (a = 21, b = 20)

y(Т) = a * x + b = 3 * 19 + 2 = 59 mod 33 = 26 = Щ (a = 3, b = 2)

y(Ы) = a * x + b = 30 * 28 + 22 = 862 mod 33 = 4 = Д (a = 30, b = 22)

y(Й) = a * x + b = 24 * 10 + 24 = 264 mod 33 = 0 = А (a = 24, b = 24)

y(Т) = a * x + b = 27 * 19 + 13 = 526 mod 33 = 31 = Ю (a = 27, b = 13)

y(Е) = a * x + b = 21 * 5 + 4 = 109 mod 33 = 10 = Й (a = 21, b = 4)

y(К) = a * x + b = 6 * 11 + 17 = 83 mod 33 = 17 = Р (a = 6, b = 17)

y(С) = a * x + b = 27 * 18 + 21 = 507 mod 33 = 12 = Л (a = 27, b = 21)

y(Т) = a * x + b = 30 * 19 + 5 = 575 mod 33 = 14 = Н (a = 30, b = 5)

В итоге получаем шифротекст(X) – МЕЭНЩДА ЮЙРЛН

Пример «ручного» аффинного рекуррентного расшифрования:

Шифротекст(X) – МЕЭНЩДА ЮЙРЛН

Пара ключей – 13 10 и 15 5

С помощью формулы 1.5, при изменяющихся ключей по формуле 1.6, вычисляем из символа открытого текста, символ шифротекста, при a = 13 и a = 15(является взаимно простым числом с длиной алфавита) и b = 10 и b = 5

$$a^{-1} = 28 \quad a^{-1} = 15$$

x(М) = (y – b) * a^{-1} = (13 - 10) * 28 = 84 mod 33 = 18 = С

x(Е) = (y – b) * a^{-1} = (21 - 10) * 28 = 308 mod 33 = 11 = К

x(Э) = (y – b) * a^{-1} = (0 - 10) * 28 = -280 mod 33 = 17 = Р (a = 30, b = 15)

x(Н) = (y – b) * a^{-1} = (11 - 10) * 28 = 28 = Ы (a = 30, b = 15)

x(Щ) = (y – b) * a^{-1} = (26 - 10) * 28 = 448 mod 33 = 19 = Т (a = 30, b = 15)

x(Д) = (y – b) * a^{-1} = (11 - 10) * 28 = 28 = Ы (a = 30, b = 15)

x(А) = (y – b) * a^{-1} = (8 - 10) * 28 = -56 mod 33 = 10 = Й (a = 30, b = 15)

x(Ю) = (y – b) * a^{-1} = (26 - 10) * 28 = 448 mod 33 = 19 = Т (a = 30, b = 15)

x(Й) = (y – b) * a^{-1} = (9 - 10) * 28 = -28 mod 33 = 5 = Е (a = 30, b = 15)

x(Р) = (y – b) * a^{-1} = (21 - 10) * 28 = 308 mod 33 = 11 = К (a = 30, b = 15)

x(Л) = (y – b) * a^{-1} = (13 - 10) * 28 = 84 mod 33 = 18 = С (a = 30, b = 15)

x(Н) = (y – b) * a^{-1} = (26 - 10) * 28 = 448 mod 33 = 19 = Т (a = 30, b = 15)

В итоге получаем открытый текст(X)– СКРЫТЫЙ ТЕКСТ

4 Программная реализация шифров

Особенности программной реализации и примеры работы программы.

Программа реализована в виде множества файлов. Код для шифрования и дешифрования находится в файле EncryptCode.py. Код для криптоанализа находится в файле Analyse.py. Весь код написан на языке программирования Python. Программа принимает открытый текст для шифрования и шифротекст для расшифрования из файла input.txt формата текст. Результат записывается в файл output.txt формата текст. Ключ берется из файла key.txt.

Программа работает как с русским алфавитом, так и с английским. Алфавит выбирается пользователем. Шифруются только буквы, символы остаются без изменений. Аффинные шифры реализованы над классом вычетов. На рисунке 1.1 представлен результат работы программы для примера шифра простой замены из раздела 3:

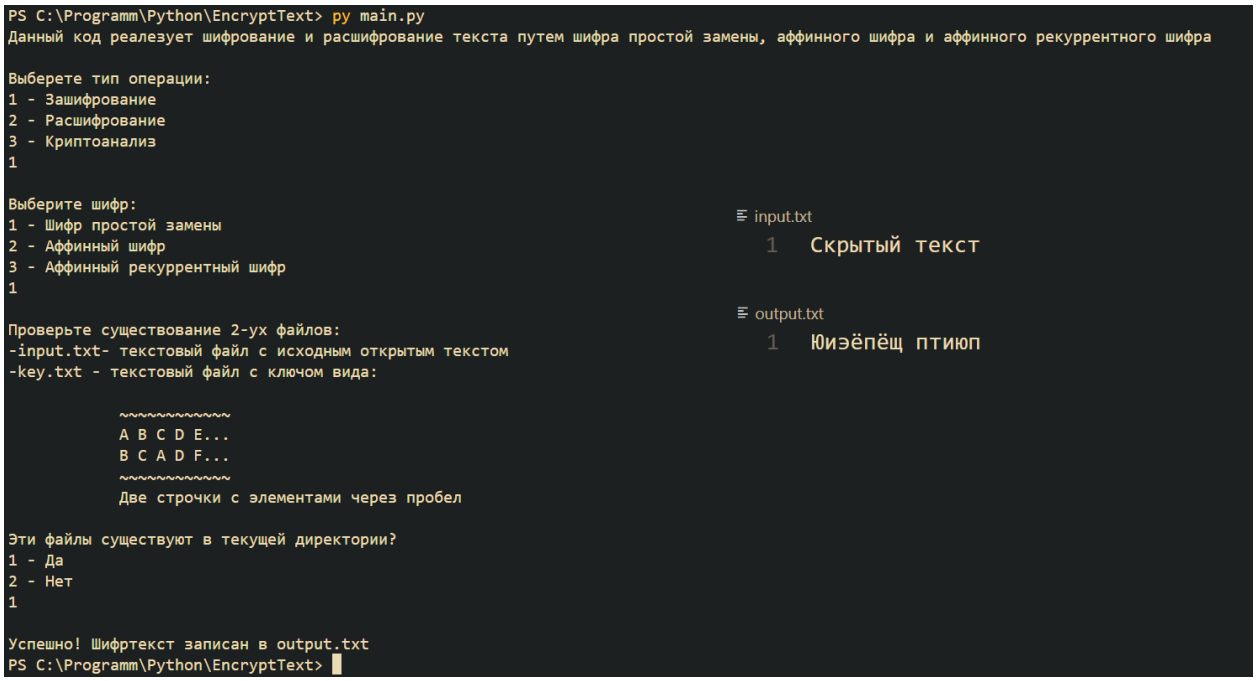

Рисунок 1.1 – результат шифрования для шифра простой замены

На рисунке 1.2 представлен результат расшифрования для примера шифра простой замены из раздела 3:

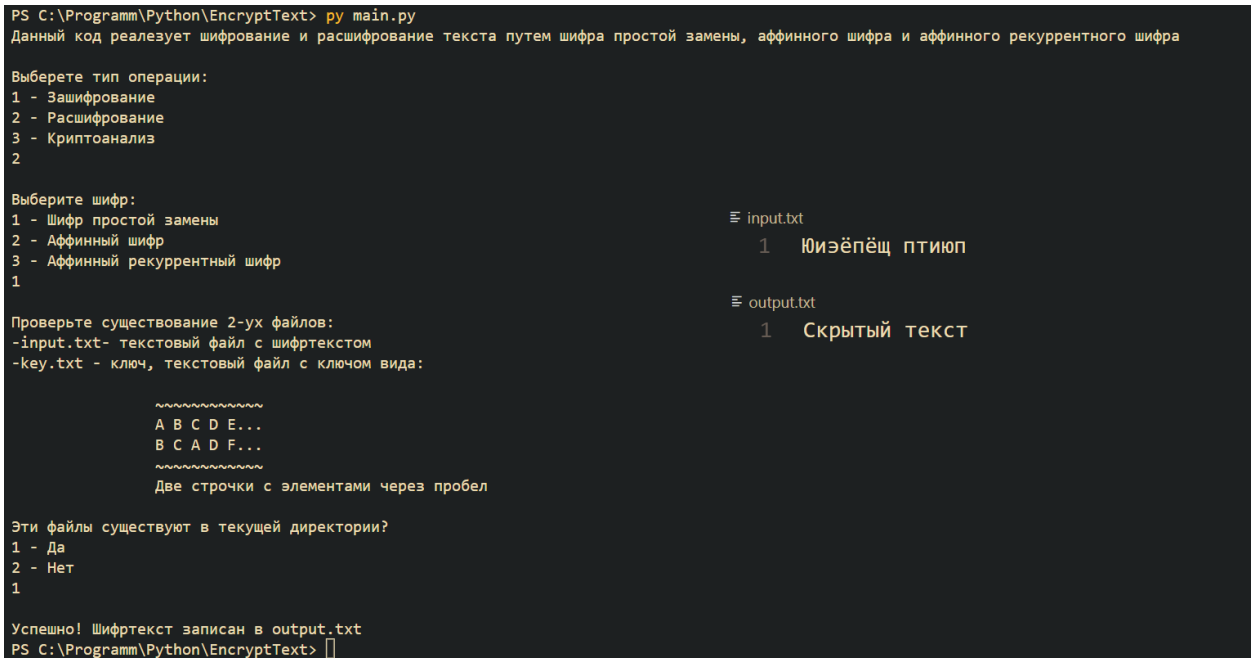

Рисунок 1.2 – результат расшифрования для шифра простой замены

Результаты шифрования и расшифрования программы, представленные на рисунках 1.1 и 1.2, совпадают с результатами “ручного” шифрования и расшифрования.

На рисунках 2.1 и 2.2 представлены результаты работ программы для примера аффинного шифра

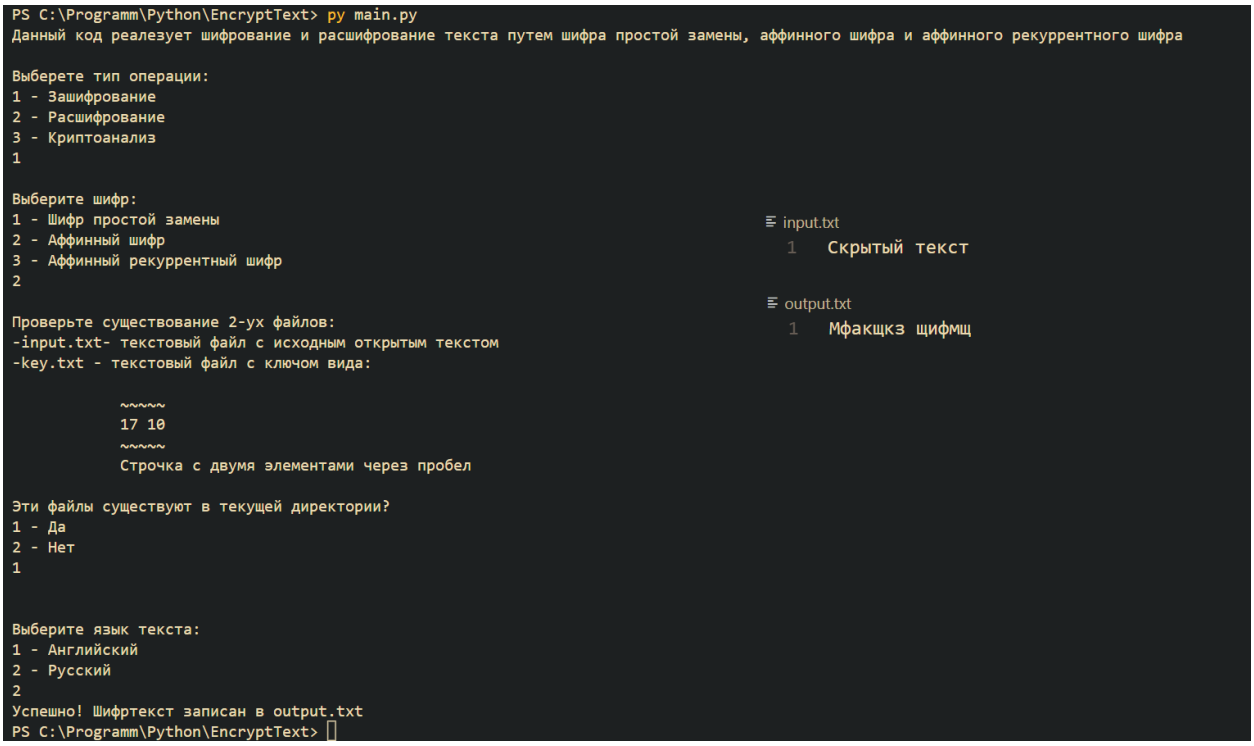

Рисунок 2.1 – результат шифрования аффинного шифра

```
PS C:\Programm\Python\EncryptText> py main.py
Данный код реализует шифрование и расшифрование текста путем шифра простой замены, аффинного шифра и аффинного рекуррентного шифра

Выберете тип операции:
1 - Зашифрование
2 - Расшифрование
3 - Криптоанализ
2

Выберите шифр:
1 - Шифр простой замены
2 - Аффинный шифр
3 - Аффинный рекуррентный шифр
2

Проверьте существование 2-ух файлов:
-input.txt- текстовый файл с шифртекстом
-key.txt - ключ, текстовый файл с ключом вида:

                ~~~~~
                17 10
                ~~~~~
                Строчка с двумя элементами через пробел

Эти файлы существуют в текущей директории?
1 - Да
2 - Нет
1


Выберите язык текста:
1 - Английский
2 - Русский
2
Успешно! Шифртекст записан в output.txt
PS C:\Programm\Python\EncryptText>
```

input.txt
1 Мфакщкз щифмщ

output.txt
1 Скрытый текст

Рисунок 2.2 – результат расшифрования аффинного шифра

На рисунках 3.1 и 3.2 представлены результаты работ программы для примера аффинного рекуррентного шифра

```
PS C:\Programm\Python\EncryptText> py main.py
Данный код реализует шифрование и расшифрование текста путем шифра простой замены, аффинного шифра и аффинного рекуррентного шифра

Выберете тип операции:
1 - Зашифрование
2 - Расшифрование
3 - Криптоанализ
1

Выберите шифр:
1 - Шифр простой замены
2 - Аффинный шифр
3 - Аффинный рекуррентный шифр
3

Проверьте существование 2-ух файлов:
-input.txt- текстовый файл с исходным открытым текстом
-key.txt - текстовый файл с ключом вида:

            ~~~~~
            17 10
            15 7
            ~~~~~
            Две строчки с двумя элементами через пробел

Эти файлы существуют в текущей директории?
1 - Да
2 - Нет
1


Выберите язык текста:
1 - Английский
2 - Русский
2
Успешно! Шифртекст записан в output.txt
PS C:\Programm\Python\EncryptText>
```

input.txt
1 Скрытый текст

output.txt
1 Мпкгаьх риыэс

Рисунок 3.1 – результат шифрования аффинного рекуррентного шифра

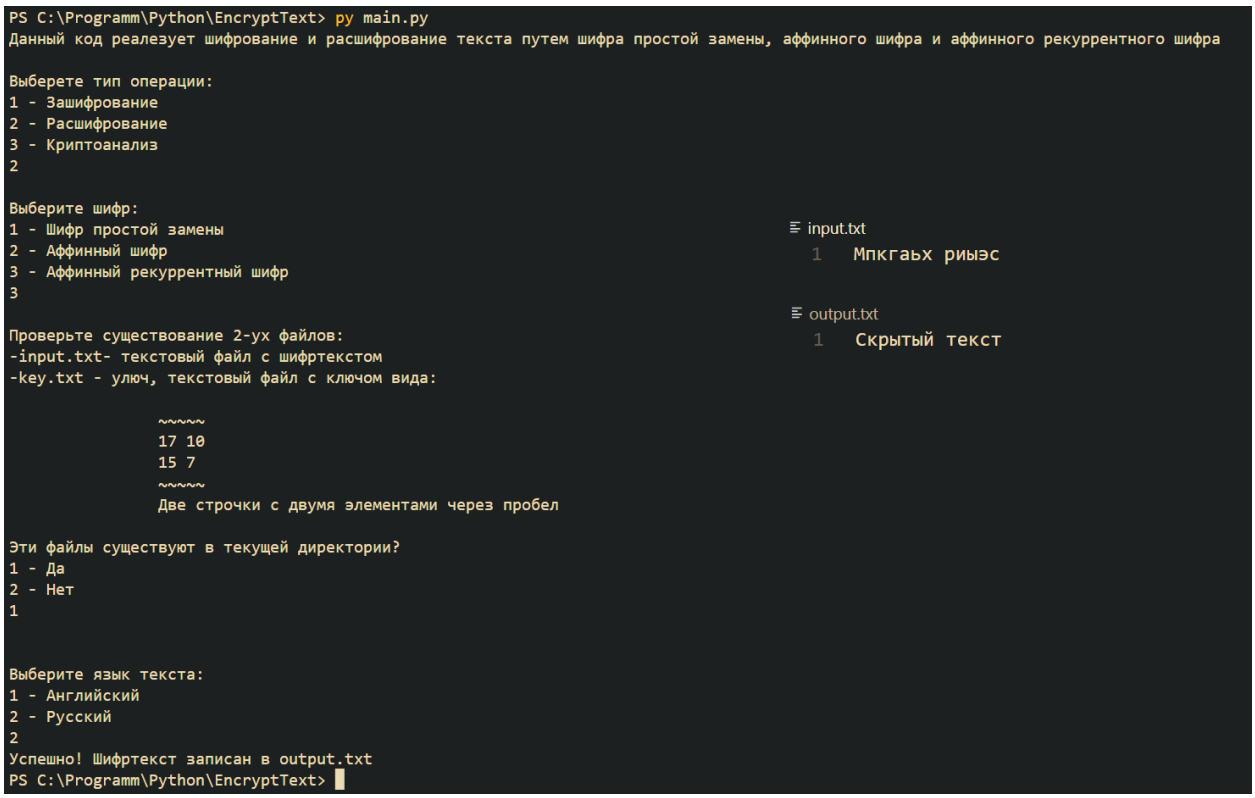

Рисунок 3.2 – результат расшифрования аффинного рекуррентного шифра

5 Примеры криптоанализа

Примеры криптоанализа исследуемых шифров с помощью методов, описанных в подразделе 2.2. Для примера была выбрано произведение Михаила Булгакова – Мастер и Маргарита

Криптоанализ шифра простой замены на рисунке 4:

```
output.txt
17  Такрт пабетеатры л порсаунай пвииьнанной вауекции (вмкопири жвенытры л
18
19
20
21  БЕРТГ ПАВЛЕЫ
22
23          ...Тек кто  тз, неконац?
24          – Ы – бертг той рисз,
25          бто лабно жобат
26          ьсе и лабно ролавчеат чсеяо.
27
28      Яата. «Эемрт»
29
```

Рисунок 4 – результат криптоанализа шифра простой замены

Криптоанализ аффинного шифра на рисунке 5:

```
PS C:\Programm\Python\EncryptText> py main.py
Данный код реалезует шифрование и расшифрование текста путем шифра простой замены, аффинного шифра и аффинного рекуррентного шифра

Выберете тип операции:
1 - Зашифрование
2 - Расшифрование
3 - Криптоанализ
3

Выберите для какого шифра выполнить криптоанализ:
1 - Шифр простой замены
2 - Аффинный шифр
2

Проверьте существование файлов:
-input.txt- текстовый файл с шифртекстом для частотного криптоанализа
Эти файлы существуют в текущей директории?
1 - Да
2 - Нет
1


Выберите язык шифртекста:
1 - Английский
2 - Русский
2

 {'О': 66281, 'А': 51763, 'Е': 48718, 'И': 41022, 'Н': 38426, 'Т': 36135, 'Л': 31477, 'С': 30417, 'Р': 28455, 'В': 28203, 'К': 21917, 'У': 1
 11428, 'З': 10645, 'Ь': 10638, 'Ы': 10367, 'Ч': 9520, 'Б': 9276, 'Й': 7021, 'Ж': 5394, 'Ш': 5227, 'Ю': 3166, 'Щ': 2122, 'Ц': 1990, 'Э': 183


Результат для a =  0 , и b =  15  =  Аааааа а Ааааааааа
Аааааа Аааа

Результат для a =  1 , и b =  0  =  Мастер и Маргарита
Михаил Афан
```

Рисунок 5 – результат криптоанализа аффинного шифра

6 Выводы о проделанной работе

Вывод: я выполнил практическую работу по подстановочным шифрам. В ходе выполнения работы я повторил свои знания по шифрам простой замены, аффинному и аффинному рекуррентному шифрам. Также я попрактиковался в ручном шифрование и сделал программную реализацию данных шифров, в том числе аффинный и аффинный рекуррентный. Из достоинств шифров стоит отметить: шифр простой замены – простота реализации, малое количество математических преобразований, удобен при малых открытых текстах; аффинный шифр – более устойчив к криптоанализу, чем шифр простой замены, достаточно прост в реализации, имеет малый ключ; аффинный рекуррентный шифр – устойчив к криптоанализу, когда злоумышленник не знает ключей.

Из недостатков шифров можно отметить: шифр простой замены – подвержен криптоанализу, прост к взлому, при больших последовательностях и малых ключах не имеет смысла; аффинный шифр – не устойчив к частотному криптоанализу; аффинный рекуррентный шифр – требует больших вычислительных мощностей.

Из проделанной работы можно сказать, что в случае, если открытый шифр был зашифрован с помощью подстановочного шифра, то с большой долей вероятности шифротекст может быть подвержен частотному криптоанализу при условии, что шифротекст (а соответственно и открытый текст) имеют большую длину.

Главными же ограничением выбранных методов криптоанализа можно считать ресурс времени (в случае перебора ключей и других методов «грубой» силы) и неточность первых результатов, в случае с частотным анализом приходилось перераспределять символы ключа 5 и более раз, так как на небольших длинах текстов частоты символов могут быть не совсем точными.

6 Список использованных источников

1. Булгаков. Мастер и Маргарита. Текст произведения. — Текст: электронный // интернет-библиотека: [сайт]. — URL: http://masterimargo.ru/book-download.html (дата обращения: 9.12.2022)
2. Классический криптоанализ. Статья. — Текст: электронный // habr.com [сайт]. — URL: https://habr.com/ru/post/271257/ (дата обращения: 9.12.2022)
3. Шифр подстановки. — Текст: электронный // ru.wikipedia.com: [сайт]. — URL: https://ru.wikipedia.org/wiki/Шифр_подстановки (дата обращения: 9.12.2022)
4. Аффинный шифр - Примеры шифрования и расшифрования. — Текст: электронный // chinapads.ru: [сайт]. — URL: https://chinapads.ru/c/s/affinnyiy_shifr_-_primeryi_shifrovaniya_i_rasshifrovaniya (дата обращения: 9.12.2022)
5. Аффинный и аффинный рекуррентный шифр. — Текст: электронный // helpstat.ru: [сайт]. — URL: https://helpstat.ru/affinnyj-i-affinnyj-rekurrentnyj-shifr/ (дата обращения: 9.12.2022)