Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Факультет программной инженерии и компьютерной техники

Информационная безопасность

Лабораторная работа №1

Основы шифрования данных

Вариант 4

Студент: Мокров Семён Андреевич

P34121

Преподаватель: Маркина Татьяна Анатольевна

Санкт-Петербург 2023

Оглавление

Цель работы

Изучение основных принципов шифрования
информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.

Задание

Реализовать в программе шифрование и дешифрацию файла с использованием квадрата Полибия, обеспечив его случайное заполнение.

Листинг разработанной программы

main.py

```
from utils.io import input_from_file, input_alphabed, input_mode,
input_matrix, input_matrix_from_file, Mode, \
    print_result, output_result, input_save_matrix, output_matrix, print_matrix
from utils.utils import configure_matrix, convert_matrix_to_string

mode = input_mode()
alphabed = input_alphabed()

if mode == Mode.CR:
    if not input_matrix():
        matrix = configure_matrix(alphabed)
    else:
        matrix = input_matrix_from_file(alphabed)
else:
    matrix = input_matrix_from_file(alphabed)

# Поиск координат символа в квадрате Полибия
def find_idx_in_matrix(char):
    for i in range(len(matrix)):
        for j in range(len(matrix[i])):
            if matrix[i][j] == char:
                return [i, j]

    raise ValueError("Некорректная матрица (не содержит весь алфавит)")

# Циклический сдвиг строки
def cyclic_shift(value, mode="STRAIGHT"):
    value = list(value)

    if mode != "REVERSE":
        value = value[::-1]

    last_char = value.pop()
    value.append(last_char)
```

```
    return value if mode == "REVERSE" else value[::-1]

# Получение индексов в квадрате Полибия в виде x и y координат
def get_indexes_from_matrix(value):
    x_idxs = []
    y_idxs = []

    for char in value:
        i, j = find_idx_in_matrix(char)
        x_idxs.append(i)
        y_idxs.append(j)

    return x_idxs, y_idxs

# Получение индексов в квадрате Полибия по строке
def get_indexes_by_str(value):
    x_idxs, y_idxs = get_indexes_from_matrix(value)

    result = ""

    for char in x_idxs:
        result += str(char)

    for char in y_idxs:
        result += str(char)

    return list(result)

# Получение строки по индексам в квадрате Полибия
def get_str_by_indexes(indexes):
    result = ""

    for i in range(len(indexes) // 2):
        result += matrix[int(indexes[i * 2])][int(indexes[i * 2 + 1])]

    return result
```

```
# Получение индексов из зашифрованной строки
def get_res_indx(value):
    source_indexes = ""

    x_indx, y_indx = get_indexes_from_matrix(value)
    for i in range(len(value)):
        source_indexes += str(x_indx[i]) + str(y_indx[i])

    source_indexes = cyclic_shift(source_indexes, "REVERSE")
    x_res_indx = source_indexes[0:len(source_indexes) // 2]
    y_res_indx = source_indexes[len(source_indexes) // 2:]

    return x_res_indx, y_res_indx

# Функция шифрования
def crypto(source):
    source_indexes = get_indexes_by_str(source)
    source_indexes = cyclic_shift(source_indexes)
    return get_str_by_indexes(source_indexes)

# Функция дешифрования
def decrypto(source):
    x_res_indx, y_res_indx = get_res_indx(source)

    result_indx = ""

    for i in range(len(x_res_indx)):
        result_indx += str(x_res_indx[i]) + str(y_res_indx[i])

    return get_str_by_indexes(result_indx)


if mode == Mode.CR:
    string_for_crypto = input_from_file()

    result = crypto(string_for_crypto)
```

```
    if input_save_matrix():
        output_matrix(convert_matrix_to_string(matrix))
else:
    string_for_decrypto = input_from_file()
    result = decrypto(string_for_decrypto)

output_result(result)

print_result(result)
print_matrix(matrix)
```

utils.py

```
from math import ceil
from random import randint


# Расчет размера квадрата Полибия
def count_matrix_size(alphabed):
    size = ceil(len(alphabed) ** 0.5)
    assert size == len(alphabed) ** 0.5, "Некорректный алфавит"
    return size


# Получение изначальной матрицы
def get_default_matrix(matrix_size):
    matrix = [''] * matrix_size
    for i in range(matrix_size):
        matrix[i] = [''] * matrix_size
    return matrix


# Создание квадрата полибия по заданному алфавиту
def configure_matrix(alphabed):
    # Ищем размер итогового квадрата
    matrix_size = count_matrix_size(alphabed)
```

```
    # Инициализируем квадрат
    matrix = get_default_matrix(matrix_size)

    current_alphabed = list(alphabed)

    # Заполняем матрицу случайными символами из алфавита
    for i in range(matrix_size):
        for j in range(matrix_size):
            if len(current_alphabed) > 0:
                current_idx = randint(0, len(current_alphabed) - 1)
                current_symbol = current_alphabed[current_idx]
                matrix[i][j] = current_symbol
                del current_alphabed[current_idx]

    return matrix


# Конвертирование квадрата Полибия в строку
def convert_matrix_to_string(matrix):
    result = ""

    for i in range(len(matrix)):
        for j in range(len(list(matrix[i]))):
            result += matrix[i][j]
        if len(matrix) - 1 != i:
            result += "\n"

    return result
```

Исходный код

Исходный код расположен в репозитории:
https://github.com/semwett0301/information-security

Результаты работы программы

Русский алфавит

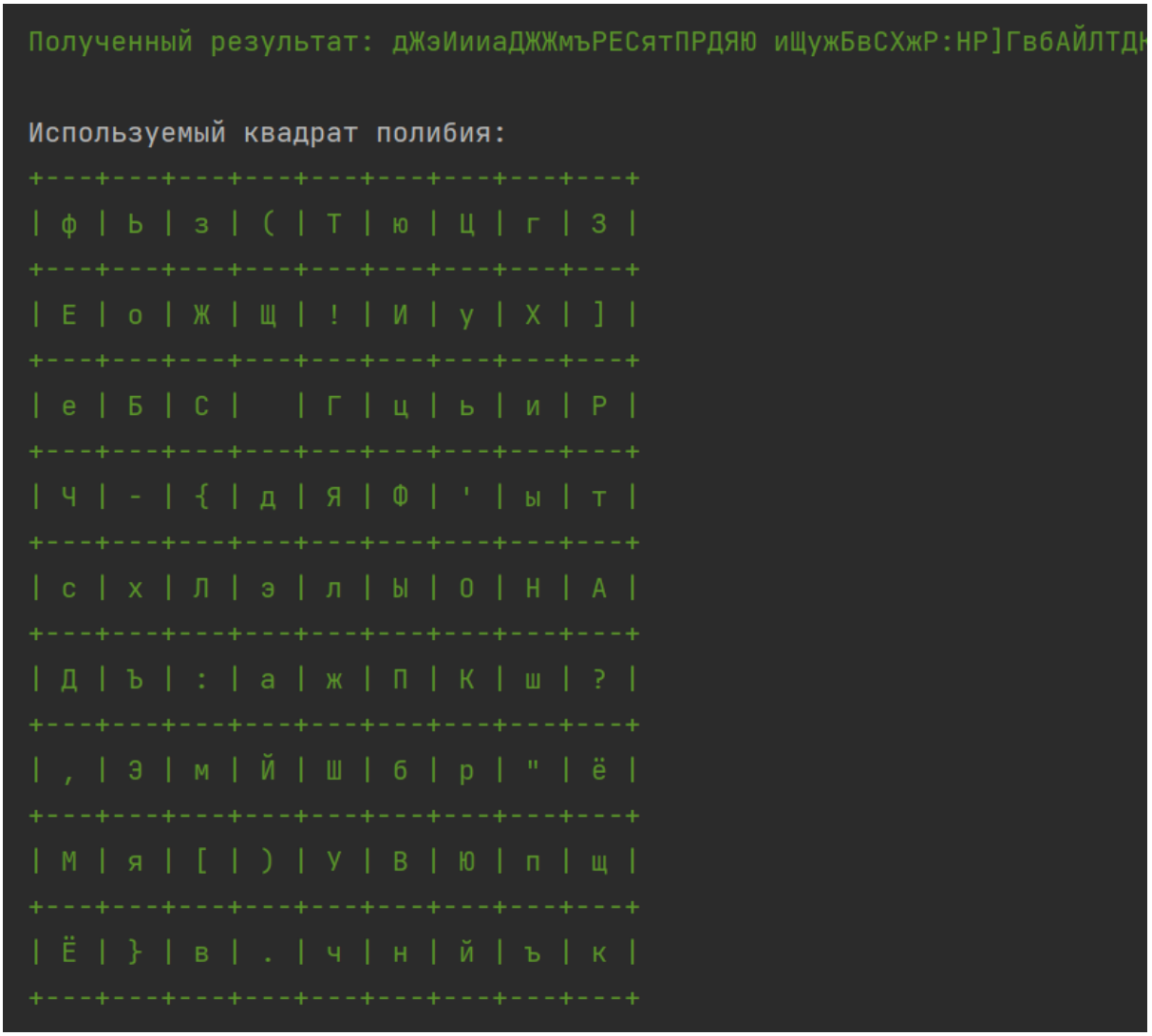
Шифровка

Исходный текст: Что это? я падаю! у меня ноги подкашиваются, - подумал он и упал на спину. Он раскрыл глаза, надеясь увидать, чем кончилась борьба французов с артиллеристами, и желая знать, убит или нет рыжий артиллерист, взяты или спасены пушки. Но он ничего не видал. Над ним не было ничего уже, кроме неба, - высокого неба, не ясного, но все-таки неизмеримо высокого, с тихо ползущими по нем серыми облаками. Как тихо, спокойно и торжественно, совсем не так, как я бежал, - подумал князь Андрей, - не так, как мы бежали, кричали и дрались, совсем не так, как с озлобленными и испуганными лицами тащили друг у друга банник француз и артиллерист, - совсем не так ползут облака по этому высокому бесконечному небу. Как же я не видал прежде этого высокого неба? И как я счастлив, что узнал его наконец. Да! все пустое, все обман, кроме этого бесконечного неба. Ничего, ничего нет, кроме его. Но и того даже нет, ничего нет, кроме тишины, успокоения. И слава Богу!..

Результат: дЖэИииаДЖЖмъРЕСятПРДЯЮ
иЩужБвСХжР:НР]ГвбАЙЛТДКРаиЛБвФ{мвм}кГжСЭмбебвЕ]ГцЙГЛмэК
ьСцГшен{му СЛР ьФРцЙГЛмэмЁ){ГСНжР{я?РГЖ]РРеЖвР
жвЫ{вмвьЯЖввЬБ:мйуСвбм{.х}ЬРьКРСУ}Ьм}РЛд?СвеммЭРЯ]ЕуГ
ГЖясХьСяРьГъ'СуЫнмвПв{хмН]]}С у:эвкуГ]Лмв ?мнв[мПО
иЩужРъзГ.мй РСФйР?ь{мПЛмйРжСС'жГъГ]Лмв
?мнвЛЕхШР.мССНЕ?.мГСКСФ[Л
ЭзЖ'Е:бкРебвЕСцЙГЛмэм{хчьРСФвясЩБШ?:яГ-ЭРЯ]уЖмА]Р}ЭРь]ц?цС[
вР
жимаСэЕЖ.х}ЬРьПБР?иГнэЛйР-БЗжСЬР?]СвПЖчСяэЖмчСубйРЭмГ-ЬьГ

}вкЕЖвбвЛвЬмввЬР мйуСе]ГЖС-Ь ПСв'РРеЖв'РЭм
цР'БН]ЖвщБГЫнСЕокЗЩт]-ыдФэЙеЪФХ)яты[ФЁЕ-ыЩмЯ-а)"ЯФдгВЙ'а
ЙЗ"эУ{ЧФдЬЦ'идй(с
}жУЧЙЪраЧЙПмЖЧдёУс"З{МыЯТ-{ай(бщыНФЗ'УЮдёУс"З(С])У)гЧю)Ю
щ)ыЩИФУгШД{)Яд)дш
ДФУЩшся'с(йЖ(Да(ЩиЬ}яФюЧФ(ЕЪя(Ъ{ф]т)Д[е"Б{М]ХЕЧтяЩяЛё[)яФ
зЧЦ[)Иэ.идЙ.ъо(г]уЪытусЗеПЕЧЖф
Дтт(..ЩДэс-ыЩмЯтЬьта,,-Ф(.Ётт{)ДэН(йУЯ))'ЯМ,ЧЖф
Дтт(..(Жхжюшиыыг"ФшиЯВ{).ъНдр)Й'"даПщЧЙПмыдёУс"З(ЩЬезФ(..яЛё
-жтдяд}ь{М]ЖЙДЗИТЪьФюЙ'тЯ(ЩД{)Яы,э(тХЩиЬ}яФютФтт-ЧэЗНеЯ}'
цЯЧяФтИюд(эе(ЮЗЕ(е(И
ДтЭед}яФф}ДЫХШДадпся(шсяФЗ(йЖ(гЩыЩ)}ядЯ(ДЁФУгШДЁтЭетпВ
М'г]ЕшЩФЧэ -ХШд

Вывод программы:



Дешифровка

Исходный текст: дЖэИииаДЖЖмъРЕСятПРДЯЮ иЩужБвСХжР:НР]ГвбАЙЛТДКРаиЛБвФ{мвм}кГжСЭмбебвЕ]ГцЙГЛмэК ьСцГшен{му СЛР ьФРцЙГЛмэмЁ){ГСНжР{я?РГЖ]РРеЖвР жвЫ{вмвьЯЖввЬБ:мйуСвбм{.х}ЬРьКРСУ}Ьм}РЛд?СвеммЭРЯ]ЕуГ ГЖясХьСяРьГь'СуЫнмвПв{хмН]]}С у:эвкуГ]Лмв ?мнв[мПО иЩужРъзГ.мй РСФйР?ь{мПЛмйРжСС'жГъГ]Лмв ?мнвЛЕхШР.мССНЕ?.мГСКСФ[Л ЭзЖ'Е:бкРебвЕСцЙГЛмэм{хчьРСФвясЩБШ?:яГ-ЭРЯ]уЖмА]Р}ЭРь]ц?цС[вР жимаСэЕЖ.х}ЬРьПБР?иГнэЛйР-БЗжСЬР?]СвПЖчСяэЖмчСубйРЭмГ-ЬьГ

}вкЕЖвбвЛвЬмввЬР мйуСе]ГЖС-Ь ПСв'РРеЖв'РЭм
цР'БН]ЖвщБГЫнСЕокЗЩт]-ыдФэЙеЪФХ)яты[ФЁЕ-ыЩмЯ-а)"ЯФдгВЙ'а
ЙЗ"эУ{ЧФдЬЦ'идй(с
}жУЧЙЪраЧЙПмЖЧдёУс"З{МыЯТ-{ай(бщыНФЗ'УЮдёУс"З(С])У)гЧю)Ю
щ)ыЩИФУгШД{)Яд)дш
ДФУЩшся'с(йЖ(Да(ЩиЬ}яФюЧФ(ЕЪя(Ъ{ф]т)Д[е"Б{М]ХЕЧтяЩяЛё[)яФ
зЧЦ[)Иэ.идЙ.ъо(г]уЪытусЗеПЕЧЖф
Дтт(..ЩДэс-ыЩмЯтЬьта,,-Ф(.Ётт{)ДэН(йУЯ))'ЯМ,ЧЖф
Дтт(..(Жхжюшиыыг"ФшиЯВ{).ъНдр)Й'"даПщЧЙПмыдёУс"З(ЩЬезФ(..яЛё
-жтдяд}ь{М]ЖЙДЗИТЪьФюЙ'тЯ(ЩД{)Яы,э(тХЩиЬ}яФютФтт-ЧэЗНеЯ}'
цЯЧяФтИюд(эе(ЮЗЕ(е(И
ДтЭед}яФф}ДЫХЩДадпся(шсяФЗ(йЖ(гЩыЩ)}ядЯ(ДЁФУгШДЁтЭетпВ
М'г]ЕшЩФЧэ -ХШд

Результат: Что это? я падаю! у меня ноги подкашиваются, - подумал он и упал на спину. Он раскрыл глаза, надеясь увидать, чем кончилась борьба французов с артиллеристами, и желая знать, убит или нет рыжий артиллерист, взяты или спасены пушки. Но он ничего не видал. Над ним не было ничего уже, кроме неба, - высокого неба, не ясного, но все-таки неизмеримо высокого, с тихо ползущими по нем серыми облаками. Как тихо, спокойно и торжественно, совсем не так, как я бежал, - подумал князь Андрей, - не так, как мы бежали, кричали и дрались, совсем не так, как с озлобленными и испуганными лицами тащили друг у друга банник француз и артиллерист, - совсем не так ползут облака по этому высокому бесконечному небу. Как же я не видал прежде этого высокого неба? И как я счастлив, что узнал его наконец. Да! все пустое, все обман, кроме этого бесконечного неба. Ничего, ничего нет, кроме его. Но и того даже нет, ничего нет, кроме тишины, успокоения. И слава Богу!..

Вывод программы:

```
Полученный результат: Что это? я падаю! у меня ноги подкашиваются, -

Используемый квадрат полибия:
+---+---+---+---+---+---+---+---+---+---+
| ф | Ь | з | ( | Т | ю | Ц | г | З |
+---+---+---+---+---+---+---+---+---+---+
| Е | о | Ж | Щ | ! | И | у | Х | ] |
+---+---+---+---+---+---+---+---+---+---+
| е | Б | С |   | Г | ц | ь | и | Р |
+---+---+---+---+---+---+---+---+---+---+
| Ч | - | { | д | Я | Ф | ' | ы | т |
+---+---+---+---+---+---+---+---+---+---+
| с | х | Л | э | л | Ы | О | Н | А |
+---+---+---+---+---+---+---+---+---+---+
| Д | Ъ | : | а | ж | П | К | ш | ? |
+---+---+---+---+---+---+---+---+---+---+
| , | Э | м | Й | Ш | б | р | " | ё |
+---+---+---+---+---+---+---+---+---+---+
| М | я | [ | ) | У | В | Ю | п | щ |
+---+---+---+---+---+---+---+---+---+---+
| Ё | } | в | . | ч | н | й | ъ | к |
+---+---+---+---+---+---+---+---+---+---+
```

Английский алфавит

Шифровка

Исходный текст: With the last morsel of bread Tom King wiped his plate clean of the last particle of flour gravy and chewed the resulting mouthful in a slow and meditative way. When he arose from the table, he was oppressed by the feeling that he was distinctly hungry. Yet he alone had eaten. The two children in the other room had been sent early to bed in order that in sleep they might forget they had gone supperless. His wife had touched nothing, and had sat silently and watched him with solicitous eyes. She was a thin, worn woman of the working-class, though signs of an earlier prettiness were not wanting in

her face. The flour for the gravy she had borrowed from the neighbour across the hall The last two ha'pennies had gone to buy the bread.

Результат: ot &qd(R:q.qYECd(eV zEfJlE(eqM.qtqEsl!HOqSq.uervEZe&(CtqxI gORF&xe&CSsEZ EP)zqw&.&&&E:Sq:(tqwNlfqwSWY.SCv &qqeV Z(& dEJHV(&yVUqN(&E.&faq)fqMqBSgO!fe&tqs&x:sfalq&Shq!f SNCg.rK Z(g.ql &&Hg(.Q &&ZCJ&.jNx.S J OqZCRQ&CktgzEZfa.).Of(&MCwH&CV(Ht.ScPISf.q'qwSCtgNRU sM.qtqRUgLOdW kQ&ogSSE&ExOxY H&D Kqk(whgOgfKqTqE&q.uqI &erv.&falI:(CKs &fegpuEiDStqZqE&qd(BSZNnOSZCJ& SY&tqYECYhtH")hQ)zHhXLscFunw:JBFRXVH,MHhhPXtRayzPgt,rtaywkH HTshPTmvUhQUtjmh)"LwkmJUMUPa:"HhHwTHtTFhPZbcBPaBJGPHsYtHt cYntwhHw)RFyV?Fmn!sQhHw,VBdHMgsPPZPPjGgmhhPgH)TiBd"chHnHa YtP,sUHdLtwhUB,JtHFuhhVMgtHFwsVVB:o-PRHFwUPwsVQHsVhUVwkB dBMBjg?FMsaVHsmF!hBzQUiBiPs PaB)hUPTMwiMHhhPTdU?z)HtHUBmnBgwhL-Q)GgyVBwLPVhanUhUBLt TJHHt,rtLtHtayBHBd"LTTsZitHtih,rwLPBhPwbHH")hZPwonQBwsVVtPYFh PXLD

Вывод программы:

```
Полученный результат: ot &qd(R:q.qYECd(eV zEfJlE(eqM.qtqEsl!HOqSq.u

Используемый квадрат полибия:
+---+---+---+---+---+---+---+---+
| q | e | K |   | f | l | . | E |
+---+---+---+---+---+---+---+---+
| O | c | i | P | g | z | J | L |
+---+---+---+---+---+---+---+---+
| x | Q | u | F | U | j | : | r |
+---+---+---+---+---+---+---+---+
| ( | H | m | B | t | " | R | w |
+---+---+---+---+---+---+---+---+
| & | V | y | h | n | ? | k | Z |
+---+---+---+---+---+---+---+---+
| N | , | Y | A | v | b | p | X |
+---+---+---+---+---+---+---+---+
| S | o | I | s | ' | W | D | G |
+---+---+---+---+---+---+---+---+
| C | T | ! | ) | M | - | d | a |
+---+---+---+---+---+---+---+---+
```

Дешифровка

Исходный текст: ot &qd(R:q.qYECd(eV zEfJlE(eqM.qtqEsl!HOqSq.uervEZe&(CtqxI gORF&xe&CSsEZ EP)zqw&.&&&E:Sq:(tqwNlfqwSWY.SCv &qqeV Z(& dEJHV(&yVUqN(&E.&faq)fqMqBSgO!fe&tqs&x:sfalq&Shq!f SNCg.rK Z(g.ql &&Hg(.Q &&ZCJ&.jNx.S J OqZCRQ&CktgzEZfa.).Of(&MCwH&CV(Ht.ScPISf.q'qwSCtgNRU sM.qtqRUgLOdW kQ&ogSSE&ExOxY H&D Kqk(whgOgfKqTqE&q.uqI &erv.&fallI:(CKs &fegpuEiDStqZqE&qd(BSZNnOSZCJ& SY&tqYECYhtH")hQ)zHhXLscFunw:JBFRXVH,MHhhPXtRayzPgt,rtaywkH HTshPTmvUhQUtjmh)"LwkmJUMUPa:"HhHwTHtTFhPZbcBPaBJGPHsYtHt cYntwhHw)RFyV?Fmn!sQhHw,VBdHMgsPPZPPjGgmhhPgH)TiBd"chHnHa

YtP,sUHdLtwhUB,JtHFuhhVMgtHFwsVVB:o-PRHFwUPwsVQHsVhUVwkB
dBMBjg?FMsaVHsmF!hBzQUiBiPs
PaB)hUPTMwiMHhhPTdU?z)HtHUBmnBgwhL-Q)GgyVBwLPVhanUhUBLt
TJHHt,rtLtHtayBHBd"LTTsZitHtih,rwLPBhPwbHH")hZPwonQBwsVVtPYFh
PXLD

Результат: With the last morsel of bread Tom King wiped his plate clean of the last particle of flour gravy and chewed the resulting mouthful in a slow and meditative way. When he arose from the table, he was oppressed by the feeling that he was distinctly hungry. Yet he alone had eaten. The two children in the other room had been sent early to bed in order that in sleep they might forget they had gone supperless. His wife had touched nothing, and had sat silently and watched him with solicitous eyes. She was a thin, worn woman of the working-class, though signs of an earlier prettiness were not wanting in her face. The flour for the gravy she had borrowed from the neighbour across the hall The last two ha'pennies had gone to buy the bread.

Вывод программы:

```
Полученный результат: With the last morsel of bread

Используемый квадрат полибия:
+---+---+---+---+---+---+---+---+
| q | e | K |   | f | l | . | E |
+---+---+---+---+---+---+---+---+
| O | c | i | P | g | z | J | L |
+---+---+---+---+---+---+---+---+
| x | Q | u | F | U | j | : | r |
+---+---+---+---+---+---+---+---+
| ( | H | m | B | t | " | R | w |
+---+---+---+---+---+---+---+---+
| & | V | y | h | n | ? | k | Z |
+---+---+---+---+---+---+---+---+
| N | , | Y | A | v | b | p | X |
+---+---+---+---+---+---+---+---+
| S | o | I | s | ' | W | D | G |
+---+---+---+---+---+---+---+---+
| C | T | ! | ) | M | - | d | a |
+---+---+---+---+---+---+---+---+
```

Вывод

В данной лабораторной работе я:

- Получил навыки программной реализации алгоритма шифрования с использованием квадрата Полибия на ЯП Python
- Ознакомился с алгоритмом шифрования с использованием Квадрата Полибия
- Ознакомился с несколькими реализациями данного метода шифрования
- Выяснил, что у реализованного мною метода есть два ограничения – алфавит должен состоять из уникальных символов и его длина должна быть квадратом целого числа