

Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЁТ
к лабораторной работе №2
на тему

ЭЛЕМЕНТЫ КРИПТОГРАФИИ

Выполнил: студент гр. 253503
Тимошевич К.С.

Проверил: ассистент кафедры
информатики Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

1 Постановка задачи.....	3
2 Ход выполнения программы.....	4
Заключение.....	8
Список использованных источников.....	9

1 ПОСТАНОВКА ЗАДАЧИ

В данной лабораторной работе требуется реализовать программу для шифрования и дешифрования текстовых файлов с использованием двух алгоритмов: шифра Цезаря и шифра Виженера. Основной целью является создание инструмента, позволяющего шифровать текстовую информацию и расшифровывать её обратно, обеспечивая корректную работу с символами русского и английского алфавитов. При этом необходимо учитывать особенности работы с регистром букв, то есть заглавные и строчные символы должны обрабатываться отдельно, сохраняя структуру исходного текста. Также важно, чтобы программа сохраняла исходное форматирование, включая пробелы, знаки препинания и другие символы, не подвергая их изменению в процессе шифрования и дешифрования.

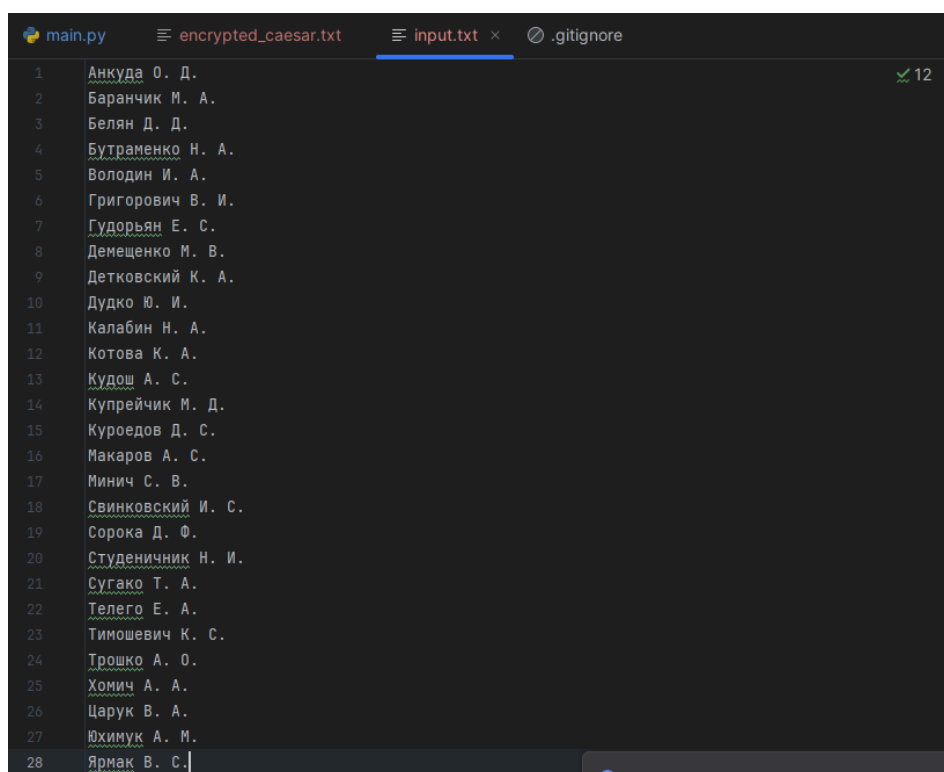
Шифр Цезаря предполагает сдвиг букв на заданное количество позиций в алфавите, поэтому пользователь должен иметь возможность выбрать необходимый сдвиг [1]. В свою очередь, шифр Виженера является более сложным методом, использующим ключевое слово, на основе которого осуществляется посимвольное шифрование, поэтому программа должна корректно применять данный метод для зашифровки и дешифровки текстовых данных [2]. Так как алфавиты русского и английского языков различаются по длине и составу, алгоритмы должны учитывать особенности каждого языка и корректно обрабатывать символы в зависимости от используемого алфавита.

Программа должна работать с текстовыми файлами, то есть входные данные считываются из файлов, после чего производится шифрование или дешифрование, а результат записывается в новый файл. Это позволит автоматизировать процесс обработки больших объемов текста и упростит взаимодействие с программой. Таким образом, итоговый программный продукт должен быть универсальным инструментом для работы с двумя видами классических методов шифрования, обеспечивая обработку данных и удобство использования.

2 ХОД ВЫПОЛНЕНИЯ РАБОТЫ

Для реализации лабораторной работы была разработана программа на языке *Python*, позволяющая выполнять шифрование и дешифрование текстовых файлов с использованием двух алгоритмов: шифра Цезаря и шифра Виженера. Исходные данные представляют собой текстовый файл с открытым текстом, который подвергается обработке указанными методами.

Программа реализована в виде набора функций, каждая из которых выполняет свою задачу. Для работы с шифром Цезаря используются функции *caesar_encrypt* и *caesar_decrypt*, которые выполняют посимвольный сдвиг символов на заданное количество позиций в пределах алфавита. Реализация поддерживает как русский, так и английский языки, что позволяет обрабатывать текст с учетом особенностей каждого алфавита. Для обработки файлов предусмотрены функции *encrypt_file_caesar* и *decrypt_file_caesar*, которые считывают данные из исходного файла, выполняют шифрование или дешифрование и сохраняют результат в новый файл. Исходный текст до обработки представлен на рисунке 2.1.



```
main.py  encrypted_caesar.txt  input.txt x  .gitignore
1  Анкуда О. Д.
2  Баранчик М. А.
3  Белян Д. Д.
4  Бутраменко Н. А.
5  Володин И. А.
6  Григорович В. И.
7  Гудорьян Е. С.
8  Демещенко М. В.
9  Детковский К. А.
10  Дудко Ю. И.
11  Калабин Н. А.
12  Котова К. А.
13  Кудош А. С.
14  Купрейчик М. Д.
15  Куроедов Д. С.
16  Макаров А. С.
17  Минич С. В.
18  Свинковский И. С.
19  Сорока Д. Ф.
20  Студеничник Н. И.
21  Сугако Т. А.
22  Телего Е. А.
23  Тимошевич К. С.
24  Трошко А. О.
25  Хомич А. А.
26  Царук В. А.
27  Юхинук А. М.
28  Ярмач В. С.]
```

Рисунок 2.1 – Исходный текстовый файл перед шифрованием

После успешного шифрования методом Цезаря формируется новый файл, содержащий зашифрованный текст. Результат выполнения программы представлен на рисунке 2.2.

```

1  Грнцжг С. Ж.
2  Ддугрьлн П. Г.]
3  Дзовр Ж. Ж.
4  Дцхуглзрнс Р. Г.
5  Есосжлр Л. Г.
6  Еулёсусель Е. Л.
7  Ецжсуявр З. Ф.
8  Жэлзърнс П. Е.
9  Жэхнсефнлм Н. Г.
10 Жцжнс Б. Л.
11 Нгогдлр Р. Г.
12 Нсхсег Н. Г.
13 Нцжсы Г. Ф.
14 Нцтузмьлн П. Ж.
15 Нцусэжсе Ж. Ф.
16 Пгнгусе Г. Ф.
17 Плрль Ф. Е.
18 Фелрнсефнлм Л. Ф.
19 Фсуснг Ж. Ч.
20 Фхцжзърлрлн Р. Л.
21 Фцёгнс Х. Г.
22 Хзозёс З. Г.
23 Хлпсызель Н. Ф.
24 Хусынс Г. С.
25 Щспль Г. Г.
26 Цгущн Е. Г.
27 Бшлпцн Г. П.
28 Вупгн Е. Ф.

```

Рисунок 2.2 – Текст после шифрования шифром Цезаря

Для проверки корректности алгоритма выполняется обратная операция – дешифрование. Функция *caesar_decrypt* применяет тот же алгоритм, но с обратным сдвигом, что позволяет восстановить исходное содержимое файла. Результаты расшифровки отображены на рисунке 2.3.

```

main.py  decrypted_caesar.txt x  decrypted_vigenere.txt  encrypted_caesar.txt
1  Анкуда О. Д.
2  Баранчик М. А.
3  Белян Д. Д.
4  Бутраменко Н. А.
5  Володин И. А.
6  Григорович В. И.
7  Гудорьян Е. С.
8  Демещенко М. В.
9  Детковский К. А.
10 Дудко Ю. И.
11 Калабин Н. А.
12 Котова К. А.
13 Кудош А. С.
14 Купрейчик М. Д.
15 Куроедов Д. С.
16 Макаров А. С.
17 Минич С. В.
18 Свинковский И. С.
19 Сорока Д. Ф.
20 Студеничник Н. И.
21 Сугако Т. А.
22 Телого Е. А.
23 Тимошевич К. С.
24 Трошко А. О.
25 Хомич А. А.
26 Царук В. А.
27 Юхинук А. М.
28 Ярмак В. С.

```

Рисунок 2.3 – Текст после дешифрования шифром Цезаря

Аналогично, для шифра Виженера были реализованы функции *vigenere_encrypt* и *vigenere_decrypt*, которые выполняют шифрование с

использованием ключевого слова. Для работы с файлами разработаны функции *encrypt_file_vigenere* и *decrypt_file_vigenere*. На рисунке 2.4 представлен файл после шифрования методом Виженера.

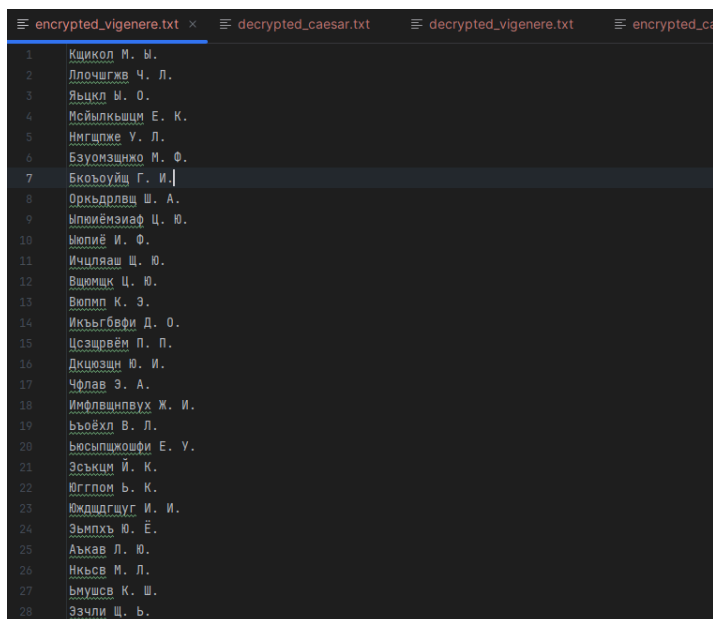


Рисунок 2.4 – Текст после шифрования шифром Виженера

После выполнения дешифрования с использованием метода Виженера текст должен восстановиться в исходный вид. Результаты обработки продемонстрированы на рисунке 2.5.

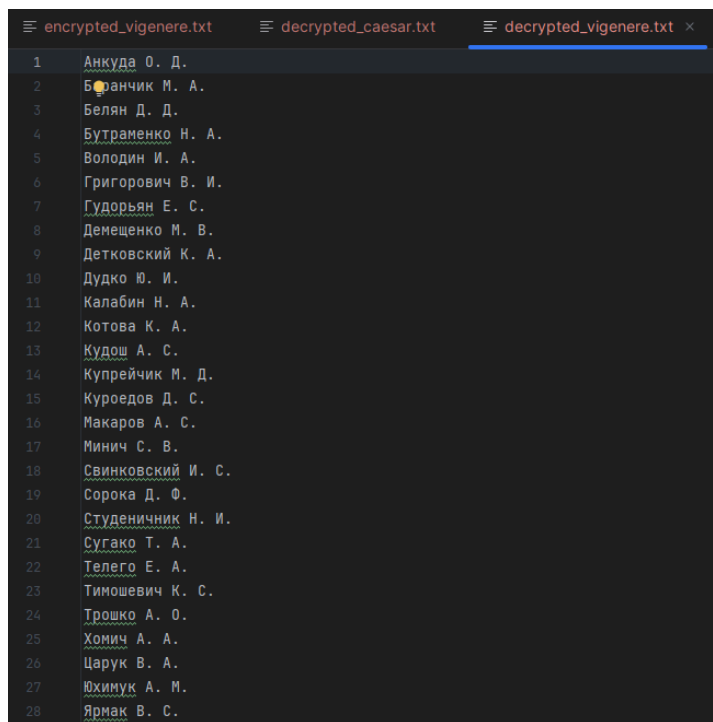


Рисунок 2.5 – Текст после дешифрования шифром Виженера

Для проверки корректности работы алгоритмов была проведена дополнительная валидация с использованием сторонних интернет-сервисов шифрования и дешифрования. Полученные результаты сравнивались с выходными данными программы. Проверка соответствия зашифрованных и расшифрованных данных подтверждает корректную работу алгоритмов. Итоговые результаты тестирования на внешнем сервисе приведены на рисунках 2.6 и 2.7.

ROT3
Грнцжг С. Ж. Дгугрълн П. Г. Дзовр Ж. Ж. Дцхугпзрнс Р. Г. Есосжлр Л. Г. Ёулёсусель Е. Л.
Ёцжсуявр З. Ф. Жзпзьзрнс П. Е. Жзхнсефнлм Н. Г. Жцжнс Б. Л. Нгогдлр Р. Г. Нсхсег Н. Г.
Нцжсы Г. Ф. Нцтузмълн П. Ж. Нцусэжсе Ж. Ф. Пгнгусе Г. Ф. Плрлз Ф. Е. Фелрнсефнлм Л. Ф.
Фсуснг Ж. Ч. Фхцжзрлърлн Р. Л. Фцёгнс Х. Г. Хзозёс З. Г. Хлпсызель Н. Ф. Хусынс Г. С.
Шсплъ Г. Г. Щгуцн Е. Г. Бшлпцн Г. П. Вупгн Е. Ф.

Рисунок 2.6 – Проверка шифрования методом Цезаря на онлайн-сервисе

**Зашифрованный
текст**

Кщикол М. Ы. Ллочшгжв Ч. Л. Яьцкл Ы. О. Мсийлкъшцм Е. К.
Нмгщпже У. Л. Бзуомзщнжо М. Ф. Бкоъоуйщ Г. И. Оркъдрлвщ
Ш. А. Ыпюиёмэиаф Ц. Ю. Ыюпиё И. Ф. Ичцляаш Щ. Ю.
Вщюмщк Ц. Ю. Вюпмп К. Э. Икъыгбвфи Д. О. Цсзщрвём П.
П. Дкцюзщн Ю. И. Чфлав Э. А. Имфлвщнпвух Ж. И. Ъьоёхл
В. Л. Ъюсыпщжошфи Е. У. Эськцм И. К. Юггпом Ъ. К.
Юждщдгщуг И. И. Эьмпхъ Ю. Ё. Аъкав Л. Ю. Нкъсв М. Л.
ьмушсв К. Ш. Эзчли Щ. Ъ.

Рисунок 2.7 – Проверка шифрования методом Виженера на онлайн-сервисе

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы была разработана и протестирована программа, реализующая шифр Цезаря и шифр Виженера. Реализация выполнена на языке *Python* с учетом особенностей русского и английского алфавитов, что позволило корректно обрабатывать текстовые файлы на обоих языках.

Для реализации шифра Цезаря были разработаны функции *caesar_encrypt* и *caesar_decrypt*, выполняющие сдвиг символов входного текста на заданное количество позиций в алфавите. Данные функции поддерживают как русский, так и английский языки, корректно обрабатывая верхний и нижний регистры. Также были созданы вспомогательные функции *encrypt_file_caesar* и *decrypt_file_caesar*, предназначенные для шифрования и расшифровки текстовых файлов. Они считывают содержимое входного файла, выполняют соответствующую операцию шифрования или дешифрования и записывают результат в новый файл, что позволяет легко применять алгоритм к большим объемам данных.

Шифр Виженера был реализован с помощью функций *vigenere_encrypt* и *vigenere_decrypt*, которые используют ключевое слово для изменения сдвига каждого символа в зависимости от его позиции в тексте. Как и в случае с предыдущим алгоритмом, были разработаны функции *encrypt_file_vigenere* и *decrypt_file_vigenere*, выполняющие аналогичные операции с файлами. Эти функции обеспечивают удобство использования программы и автоматизируют процесс работы с текстовыми данными.

Программа успешно прошла тестирование, продемонстрировав правильность шифрования и последующего восстановления исходного текста. Таким образом, поставленные в начале работы задачи были успешно решены и разработанная программа может использоваться для шифрования и дешифрования текстовой информации с применением двух популярных классических методов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Шифр Цезаря или как просто зашифровать текст [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/articles/534058/>. – Дата доступа: 09.02.2025

[2] Шифр Виженера. Разбор алгоритма на Python [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/articles/140820/>. – Дата доступа: 09.02.2025