**Міністерство освіти і науки України**

**Міжрегіональна академія управління персоналом**

**Факультет комп’ютерно-інформаційних технологій**

**Лабораторна робота №1**

З дисципліни «Технології захисту інформації»

**Виконав:**

Студент ІК-9-15-Б1РС(4.0 д)

Кварцяний Петро Олександрович

**Перевірила:**

Чолишкіна О. Г.

Київ 2018

Зміст

1. Тема, ціль, завдання………………………………………………………..3
2. Теоретичні відомості………………………………………………………4
3. Хід роботи………………………………………………………………….6
4. Висновки………………………………………………………………......13
5. Список літератури………………………………………………………...13
6. Додатки……………………………………………………………………14

**Тема:** Шифрування Цезаря

**Ціль:** Ознайомитися з шифруванням Цезаря та реалізувати програмно на будь-якій мові програмування

**Завдання:**

1. Ознайомитися з шифруванням Цезаря
2. Реалізувати програмно на будь-якій мові програмування
3. Висновки

**Теоретичні відомості:**

**Ознайомитися з шифруванням Цезаря**

У криптографії шифр Цезаря, відомий також як шифр Цезаря, шифр зсуву, кодекс Цезаря або зміна Цезаря, є одним із найпростіших і найбільш широко відомих методів шифрування. Це тип заміну шифру, в якому кожна буква в звичайному тексті замінюється буквою певною фіксованою кількістю положень вниз по алфавіту. Наприклад, з лівим зрушенням 3, D буде замінено на A, E стане B, і так далі. Метод названий на честь Джуліуса Цезаря, який використовував його в особистому листуванні.

Крок шифрування, виконуваний шифром Цезаря, часто включається як частина більш складних схем, таких як шифр Vigenère, і все ще має сучасне застосування в системі ROT13. Як і в усіх шифрах заміщення з однією алфавітом, шифр Цезаря легко розбивається, і в сучасній практиці він практично не надає ніякої безпеки зв'язку.

**Приклад**

Трансформація може бути представлена ​​шляхом вирівнювання двох алфавітів; алфавіт шифрування - це простой алфавіт, що повертається ліворуч або праворуч за деякою кількістю позицій. Наприклад, тут використовується шифр Цезаря, який використовує ліве обертання трьох місць, еквівалентний правильному зсуву 23 (параметр shift використовується як ключ):

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

При шифруванні особа шукає кожну букву повідомлення у рядку «простий» та записує відповідне літеру у рядку «шифр».

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Розшифровка виконується в зворотному напрямку, з правильним зміщенням 3.

Шифрування також може бути представлено за допомогою модульної арифметики , спочатку перетворюючи букви на цифри, відповідно до схеми, A → 0, B → 1, ..., Z → 25. Шифрування букви х зсувом n можна описати математично як En(x)=(x+n) mod 26.

Розшифровка виконується аналогічно Dn(x)=(x-n) mod 26.

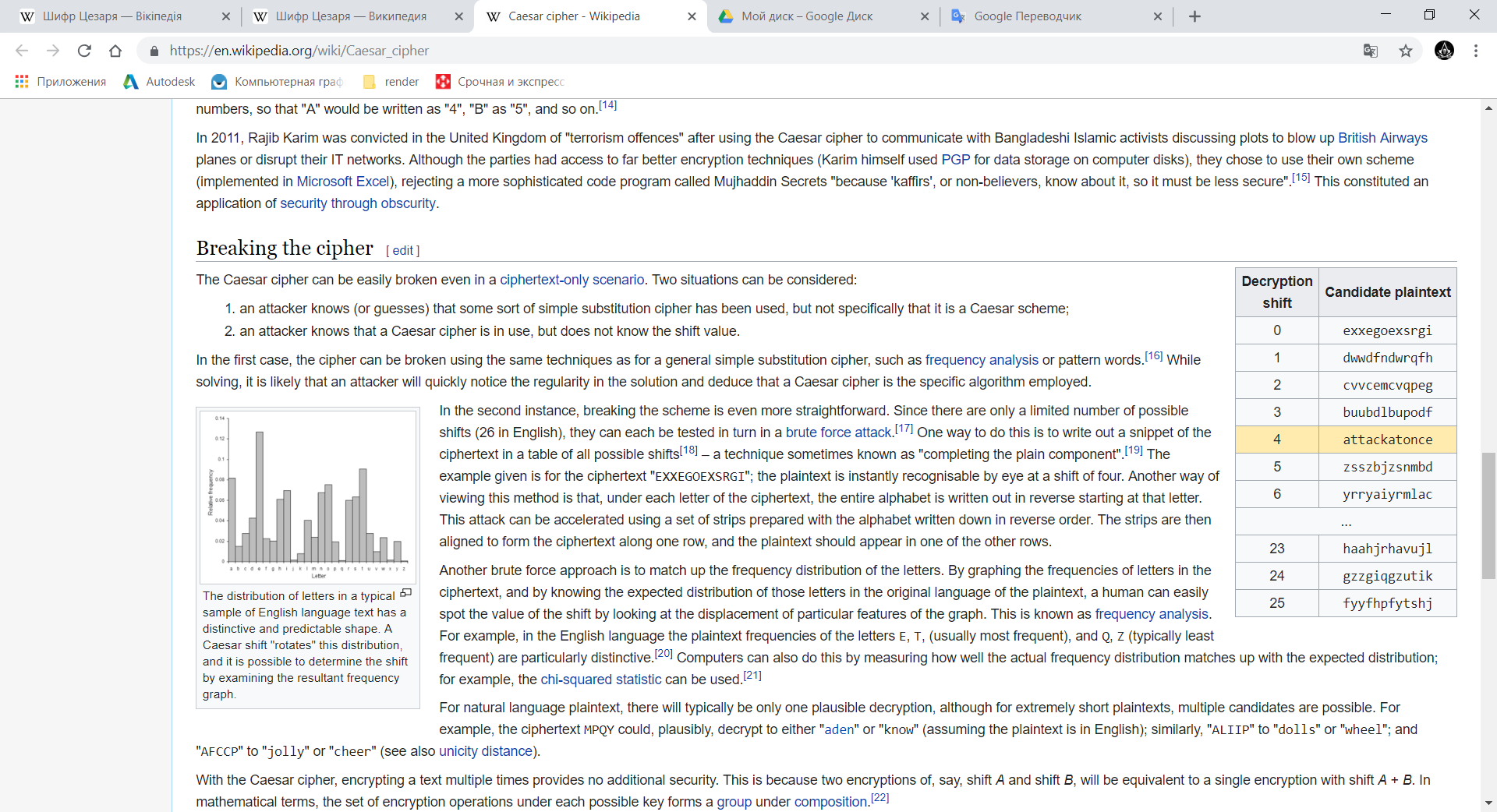
(Існують різні визначення для операції по модулю . У наведеному вище, результат знаходиться в діапазоні від 0 до 25, тобто якщо x + n або x - n не знаходяться в діапазоні від 0 до 25, нам доведеться відняти або додати 26 .)

Заміна залишається незмінною протягом всього повідомлення, тому шифр класифікується як тип моноалфайличної заміни , на відміну від поліальфальної заміни.

**Злом шифру**

Шифр Цезаря може бути легко зламаний навіть в разі, коли зломщик знає тільки зашифрований текст. Можна розглянути дві ситуації:

1. Зломщик знає (або передбачає), що використовувався простий шифр підстановки, але не знає, що це - схема Цезаря.
2. Зломщик знає, що використовувався шифр Цезаря, але не знає значення зсуву.

У першому випадку шифр може бути зламаний, використовуючи ті ж самі методи що і для простого шифру підстановки, такі як частотний аналіз і т. Д. Використовуючи ці методи, зломщик, ймовірно, швидко помітить регулярність в рішенні і зрозуміє, що використовується шифр - це шифр Цезаря.

У другому випадку злом шифру є навіть більш простим. Існує не так багато варіантів значень зсуву (26 для англійської мови), всі вони можуть бути перевірені методом грубої сили. Один із способів зробити це - виписати уривок зашифрованого тексту в стовпець всіх можливих зрушень - техніка, іноді звана як «завершення простого компонента». Розглянемо приклад для зашифрованого тексту «EXXEGOEXSRGI»; відкритий текст негайно розпізнається оком в четвертому рядку.

Інший спосіб застосування цього методу - це написати алфавіт під кожною буквою зашифрованого тексту, починаючи з цієї літери. Метод може бути прискорений, якщо використовувати заздалегідь підготовлені смужки з алфавітом. Для цього потрібно скласти смужки так, щоб в одному рядку утворився зашифрованістю текст, тоді в деякій іншій рядку ми побачимо відкритий текст.

Інший підхід до застосування методу грубої сили для злому - перевірити частотизустрічальності букв. Зобразивши діаграмою частоти встречаній букв в зашифрованому тексті, і знаючи очікуване розподіл букв для звичайного тексту на даному мовою, можна легко визначити зрушення, глянувши на зміщення деяких характерних рис на діаграмі. Цей метод відомий як частотний аналіз . Наприклад, в тексті на англійській мові частота букв E , T , (зазвичай найбільш частих), і Q , Z (зазвичай більш рідкісних) особливо розрізняються. Цей процес можна автоматизувати, зробивши, щоб комп'ютерна програма оцінювала, наскільки добре фактичний розподіл частот відповідає очікуваному розподілу. Наприклад, може використовуватися критерій хі-квадрат.

Для звичайного тексту на природній мові, швидше за все, буде лише один варіант декодування. Але, якщо використовувати дуже короткі повідомлення, то можливі випадки, коли можливі кілька варіантів розшифровки з різними зсувами. Наприклад зашифрований текст «MPQY» може бути розшифрований як «aden» так і як «know» (припускаючи, що відкритий текст написаний англійською мовою). Точно також «ALIIP» можна розшифрувати як «dolls» або як «wheel»; «AFCCP» як «jolly» або як «cheer» (див. Також відстань єдиності ).

Багаторазове шифрування ніяк не покращує стійкість, так як застосування шифрів із зсувом a і b еквівалентно застосуванню шифру із зсувом a + b. У математичних термінах шифрування з різними ключами утворює групу.

**Хід роботи:**

**Реалізувати програмно на будь-якій мові програмування**

Для реалізації шифрування Цезаря я обрав мову Python. Мова тексту для шифрування – англійська.

Срипт шифрування:

def cipher(*s*,*n*):

*if* s>26:

        s=s%26

    caesar=''

*for* i in n:

*if* ord(i)>=ord('a') and ord(i)<=ord('z'):

*if* ord(i)+s>ord('z'):

                caesar=caesar+chr((ord(i)+s)-26)

*else*:

                caesar=caesar+chr(ord(i)+s)

*elif* ord(i)>=ord('A') and ord(i)<=ord('Z'):

*if* ord(i)+s>ord('Z'):

                caesar=caesar+chr((ord(i)+s)-26)

*else*:

                caesar=caesar+chr(ord(i)+s)

*else*:

            caesar=caesar+i

*return* caesar

Та дешифрування:

def decrypt(*n*):

*with* open('msg.txt', 'r') *as* f:

ciphertext = f.read()

result = ''

*for* l in ciphertext:

*try*:

i = (alphabet.index(l) - n) % 26

result += alphabet[i]

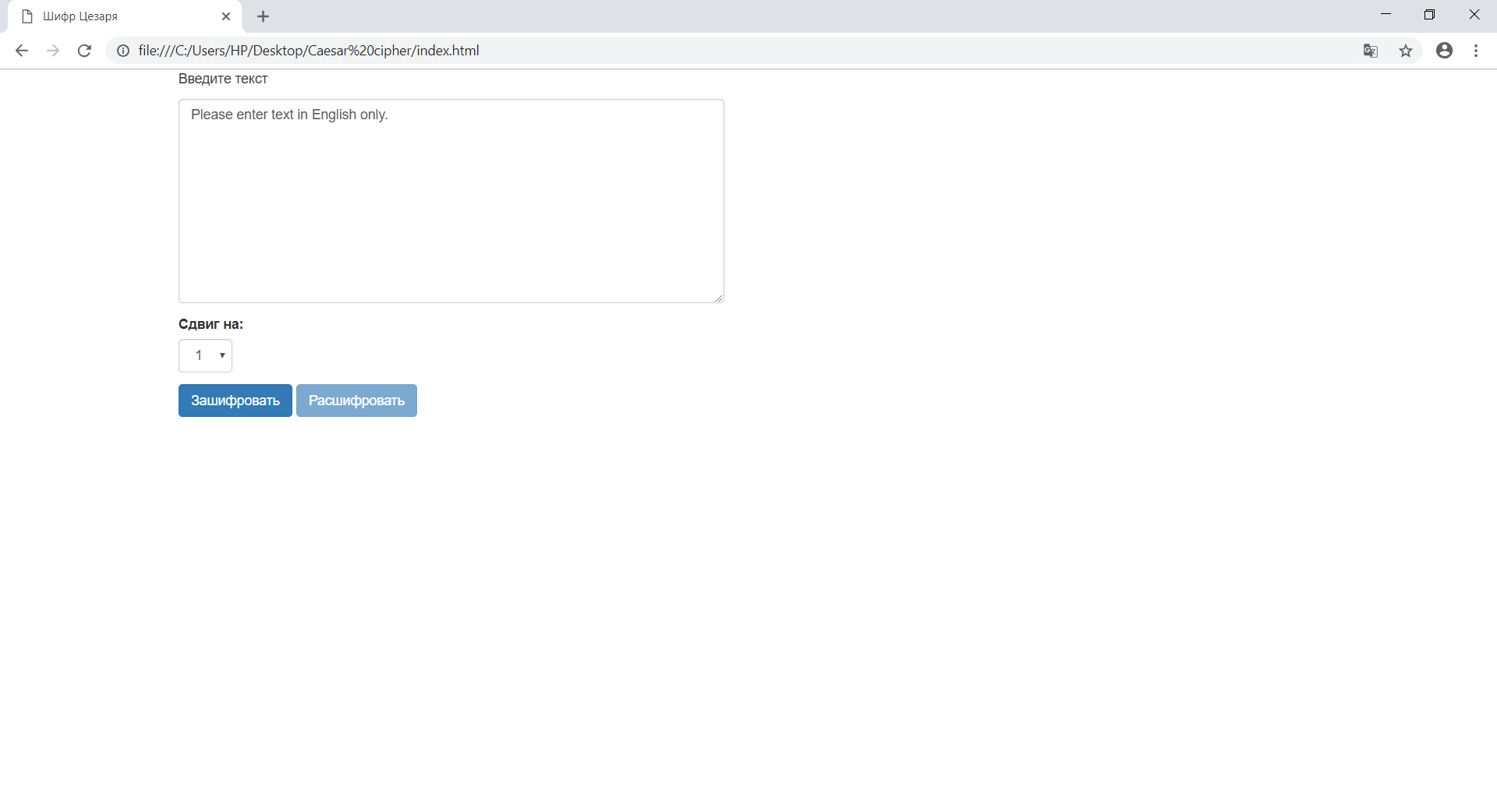
*except* ValueError:

result += l

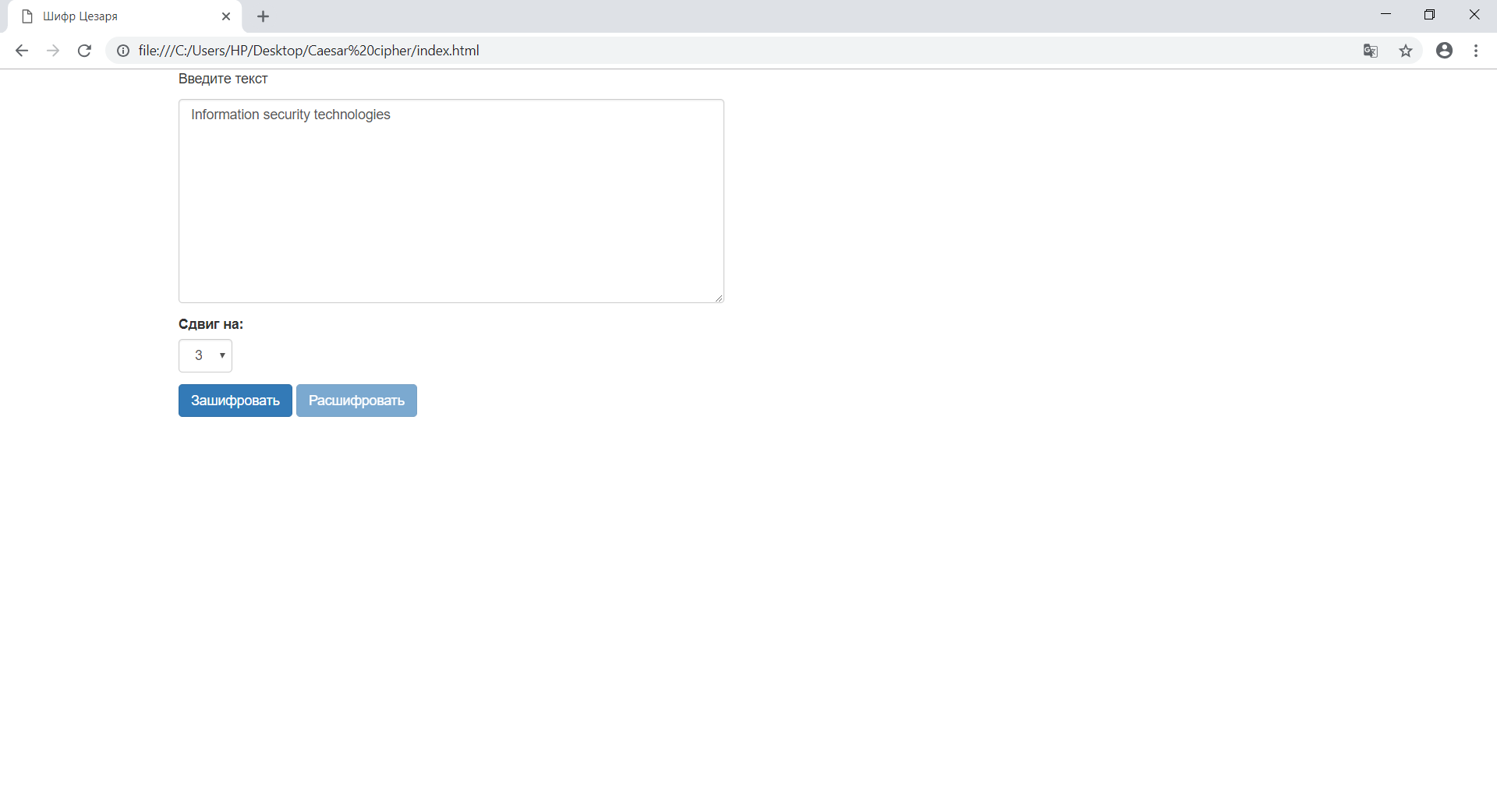
print(f"Key:{n}-Message:{result}")

**Робота створеної програми:**

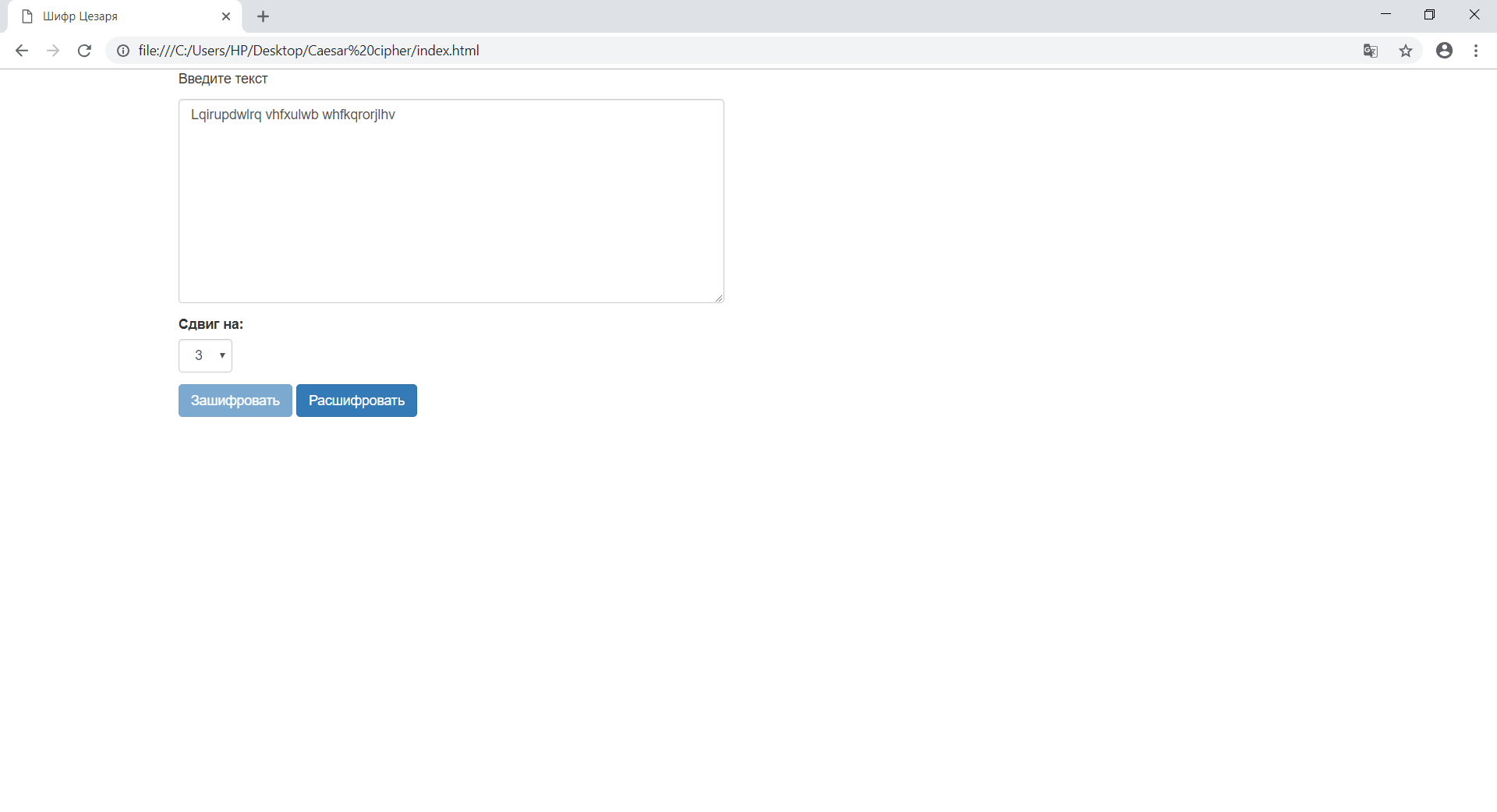
1. Запуск



1. Уведення тексту на англійскій мові «Information security technologies», обираємо здвиг на 3:



1. Натискаємо «Зашифровать»:



Як бачимо, програма шифрування працює, та видала текст у зашифрованому вигляді «Lqirupdwlrq vhfxulwb whfkqrorjlhv».

Дешифрування відбувається при натисканні на кнопку «Расшифровать».

**Висновки:**

Під час виконання лабораторної роботи було:

1. Ознайомлено з алгоритмом шифруванням Цезаря.
2. Створено програму для шифрування/дешифрування на мові python.
3. Було доведено працездатність створеної програми.

**Список використаної літератури:**

<https://en.wikipedia.org/wiki/Caesar_cipher>

https://stackoverflow.com/