lab2（Реализовать шифрование шифрами Цезаря и Вижинера.）

# Шифрование Цезаря

def caesar\_encrypt(text, shift):

    encrypted\_text = ""

    for char in text:

        if char.isalpha():

            # Определить случай

            ascii\_offset = ord('A') if char.isupper() else ord('a')

            encrypted\_char = chr((ord(char) - ascii\_offset + shift) % 26 + ascii\_offset)

            encrypted\_text += encrypted\_char

        else:

            encrypted\_text += char

    return encrypted\_text

# Шифрование по методу Виженера

def vigenere\_encrypt(text, key):

    encrypted\_text = ""

    key\_length = len(key)

    for i, char in enumerate(text):

        if char.isalpha():

            # Определить случай

            ascii\_offset = ord('A') if char.isupper() else ord('a')

            key\_char = key[i % key\_length]

            key\_offset = ord(key\_char.upper()) - ord('A')

            encrypted\_char = chr((ord(char) - ascii\_offset + key\_offset) % 26 + ascii\_offset)

            encrypted\_text += encrypted\_char

        else:

            encrypted\_text += char

    return encrypted\_text

# Расшифровка шифра Цезаря

def caesar\_decrypt(text, shift):

    return caesar\_encrypt(text, -shift)

# Расшифровка шифра Виженера

def vigenere\_decrypt(text, key):

    decrypted\_text = ""

    key\_length = len(key)

    for i, char in enumerate(text):

        if char.isalpha():

            # Определить случай

            ascii\_offset = ord('A') if char.isupper() else ord('a')

            key\_char = key[i % key\_length]

            key\_offset = ord(key\_char.upper()) - ord('A')

            decrypted\_char = chr((ord(char) - ascii\_offset - key\_offset) % 26 + ascii\_offset)

            decrypted\_text += decrypted\_char

        else:

            decrypted\_text += char

    return decrypted\_text

# Демонстрация основной функции

def main():

    name = "Tian kunlong"  # Заменить на свое имя

    caesar\_shift = 3  # смещение шифра Цезаря

    vigenere\_key = "KEY"  # ключ шифра Виженера

    # Шифрование с использованием шифра Цезаря

    caesar\_encrypted = caesar\_encrypt(name, caesar\_shift)

    print(f"Результаты шифра Цезаря: {caesar\_encrypted}")

    # Расшифровка с использованием шифра Цезаря

    caesar\_decrypted = caesar\_decrypt(caesar\_encrypted, caesar\_shift)

    print(f"Результаты расшифровки Цезаря: {caesar\_decrypted}")

    # Зашифровано с использованием шифра Виженера

    vigenere\_encrypted = vigenere\_encrypt(name, vigenere\_key)

    print(f"\nРезультаты шифра Вирджинии: {vigenere\_encrypted}")

    # Результаты расшифровки Вирджинии

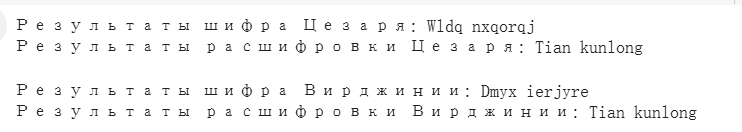
    vigenere\_decrypted = vigenere\_decrypt(vigenere\_encrypted, vigenere\_key)

    print(f"Результаты расшифровки Вирджинии: {vigenere\_decrypted}")

if \_\_name\_\_ == "\_\_main\_\_":

main()

Результаты выполнения кода



**Инструкции по выполнению кода**

1. Функция caesar\_encrypt

Цель: шифровать текст с помощью шифра Цезаря.

Логика:

Пройти каждый символ ввода.

Если это буква, определить базовое смещение на основе ее регистра (A для заглавных букв и a для строчных букв).

Применить смещение, чтобы сместить букву назад в алфавите на указанное количество позиций.

Небуквенные символы остаются неизменными.

Причина выбора кода:

Шифр Цезаря — это простой метод шифрования подстановкой, который легко реализовать и понять.

Шифрование достигается с помощью циклического сдвига, что подходит для новичков, чтобы понять основные принципы шифрования.

2. Функция vigenere\_encrypt

Цель: шифровать текст с помощью шифра Виженера.

Логика:

Использовать ключ для определения смещения каждого символа.

Повторить, когда длины ключа недостаточно.

Применить соответствующее смещение ключа к каждой букве.

Причина выбора кода:

Шифр Виженера более безопасен, чем шифр Цезаря, поскольку он использует переменное смещение.

Использование ключей увеличивает сложность шифрования и повышает безопасность.

3. Функция caesar\_decrypt

Цель: Расшифровать текст, зашифрованный шифром Цезаря.

Логика:

На самом деле, это обратная операция caesar\_encrypt.

Переместить буквы вперед в алфавите на отрицательное смещение, чтобы восстановить исходный текст.

Причина выбора кода:

Шифрование и расшифровка Цезаря симметричны, и расшифровка может быть достигнута простым изменением направления смещения.

4. Функция vigenere\_decrypt

Цель: Расшифровать текст, зашифрованный шифром Виженера.

Логика:

Использовать один и тот же ключ для восстановления каждого символа на обратное смещение.

Ключ используется в цикле для обеспечения согласованности с процессом шифрования.

Причина выбора кода:

Для шифрования и дешифрования Вижера требуется один и тот же ключ для поддержания согласованности шифрования и дешифрования.

5. основная функция

Цель: продемонстрировать весь процесс шифрования и дешифрования.

Логика:

Определить пример имени (можно заменить фактическим именем).

Установить смещение шифра Цезаря и ключ шифра Виженера.

Продемонстрировать шифрование Цезаря и Виженера и соответствующие им процессы дешифрования соответственно.

Причина выбора кода:

Предоставить полный пример использования для облегчения понимания и проверки процесса шифрования и дешифрования.

Показать, как использовать эти функции шифрования в реальных приложениях.