МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**КРИПТОАНАЛІЗ ШИФРУ ВІЖЕНЕРА**

**Виконав:** курсант навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_Петренко К.В.

19.05.2024

**Перевiрив:** викладач кафедри № 33

капітан \_\_\_\_\_\_\_\_\_\_\_\_Прийма О.О.

Київ – 2024

1.**Програмні коди**

Усі програмні коди розміщнні на GitHub: [KuMuLaTiV4iK/PK-2: Vigener Attack (github.com)](https://github.com/KuMuLaTiV4iK/PK-2)

# **Виконані завдання**

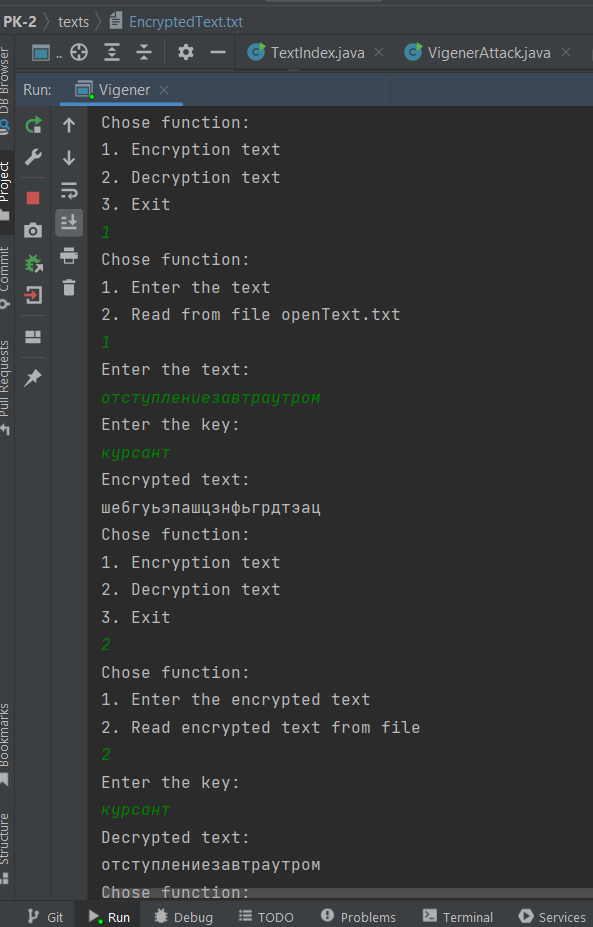
Завдання 1. Написати програми, які виконують шифрування та розшифрування

шифром Віженера текстів російською мовою. Програми повинні працювати із відфільтрованими текстами (див. комп’ютерний практикум 1). З алфавіту вилучається літера «ё»; відповідно, Загальна кількість літер у

алфавіті m = 32. У текстах літера «ё» повинна бути замінена буквою «е»; модифікуйте ваш фільтр за необхідності.

У класі Vigener було реалізовано шифрування і розшифрування шифром Віженера для відфільтрованих текстів (із заміною літери «ё») російською мовою. Інтерфей програми представлений зручним меню у якому є всі необхідні функції для операцій над текстом. Текст можна вводити як з клавіатури так і читати з файлу. Всі результати шифрування записуються у файл EncryptedText.txt, рознифрування у файл DecryptedText.txt.

Результат роботи:



Завдання 2. Дослідити поведінку індексу відповідності для шифротекстів.

Для виконання завдання вам необхідно самостійно підібрати текст для шифрування (3-5 кб) та ключі довжини r = 2, 3, 4, 5, 6, а також довжини 10, 15 та 20 знаків.

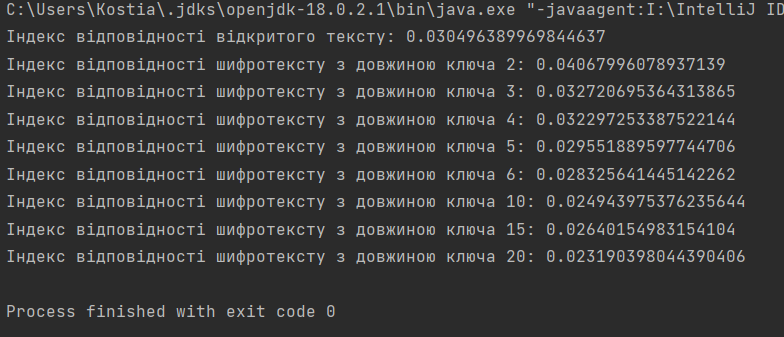
1. Зашифруйте обраний відкритий текст шифром Віженера з обраними ключами.

2) Обчисліть індекси відповідності для відкритого тексту та всіх одержаних шифротекстів і порівняйте їх значення.

Одержані значення необхідно навести у звіті таблицею та діаграмою.

У класі TextIndex було реалізовано обчислення індексів відповідності для фільтрованого відкритого тексту та всіх одержаних шифротекстів. Порівнявши їх значення можна війти висновку, що зі збільшенням довжини ключа індекс відповідності зменшується.

Результат роботи:



Завдання 3. Дешифрувати заданий шифротекст.

Використовуючи наведені теоретичні відомості, напишіть програму, яка реалізує атаку на шифр Віженера та розшифруйте з її допомогою наданий шифртекст (згідно свого номеру варіанта - 20 варіант).

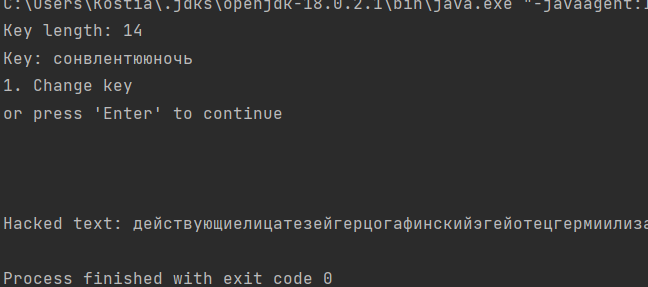
У класі VigenerAttack було реалізовано атаку на шифр Віженера методом частотного аналізу. Для цього реалізовано метод знаходження довжини ключа та метод взлому шляхом частотного аналізу з обчисленням функції M(g).

Результат роботи атаки на наданий текст:

Довжина ключа: 14 сиволів

Ключ: сонвлетнююночь

Розшифрований текст наведений у файлі HackedText.txt.



**Висновок:** За результатами виконаних робіт було успішно реалізовано атаку на шифр Віженера методом частотного аналізу. Результатом атаки стало дешифрування шифротексту за визначеним частотним аналізом ключем.

Точність визначення ключа забезпечила реалізація функції M(g). У процесі реалізації атаки було засвоєно основи алгоритму шифрування Віженера та специфіка проведення частотного аналізу.