

Міністерство освіти і науки, молоді та спорту України

Національний технічний університет України

“Київський політехнічний інститут”

Фізико-Технічний інститут

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**за семестровий курс предмету**

**«Симетрична криптографія»**

**Роботу виконали:**

Студенти групи ФІ-03

Гілевський Олександр,

Кузьменко Анна

**Приймав:**

Чорний Олег Миколайович

Київ-2023

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**Криптоаналіз шифру Віженера**

*Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.*

**Порядок виконання роботи**

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3,

4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності I\_r для відкритого тексту та всіх одержаних

шифротекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий

шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:

– визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь D\_r (на вибір);

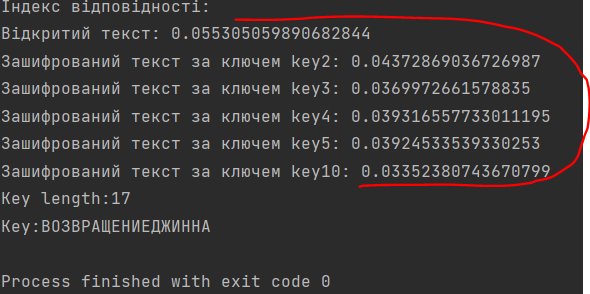
– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

– визначити символи ключа за допомогою функції M\_i(g);

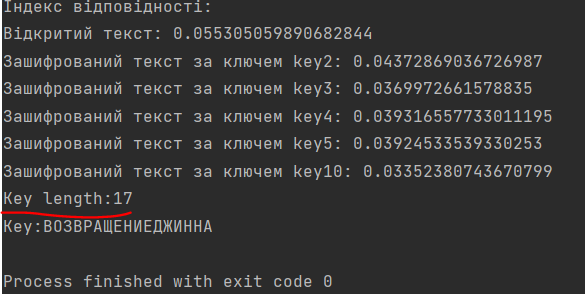
– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

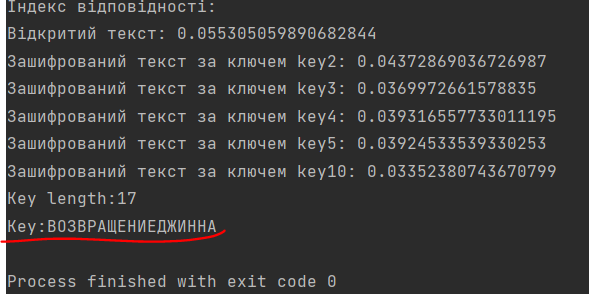
**Хід роботи**

**1, 2.** Підібравши текст, який знаходиться в файлі text.txt, шифруємо його за допомогою шифру Віженера та порівнюємо індекси відповідності:



Як бачимо, після ключа довжини 4 індекс зменшується.

**3.** За допомогою методу індексів відповідності маємо довжину ключа: 17  


І з функції M\_i(g) отримаємо ключ:  
  
Результат розшифрованого тексту в файлі result.txt  
  
**Висновок:** засвоїли методи частотного криптоаналізу, здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.