**КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

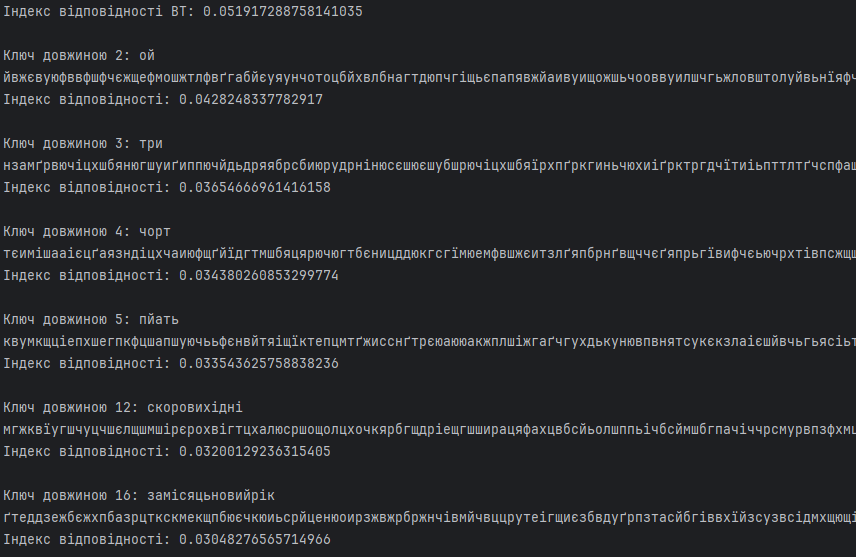
**Криптоаналіз шифру Віженера**

**Роботу виконали  
студенти групи ФБ-14:**Земляний Олександр та Гавриленко Давид

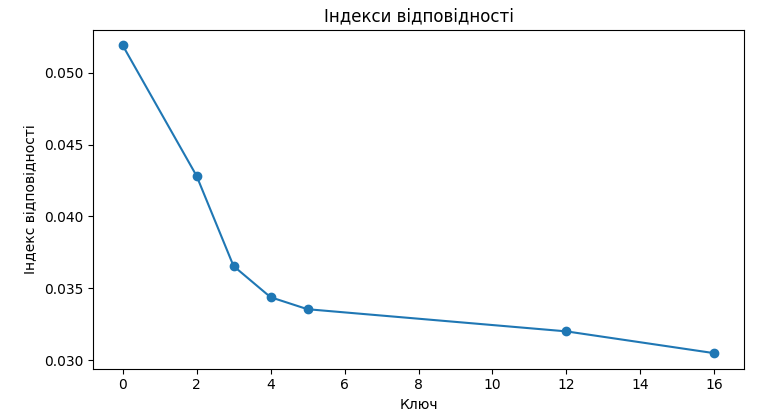
**Варіант 6**

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

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.

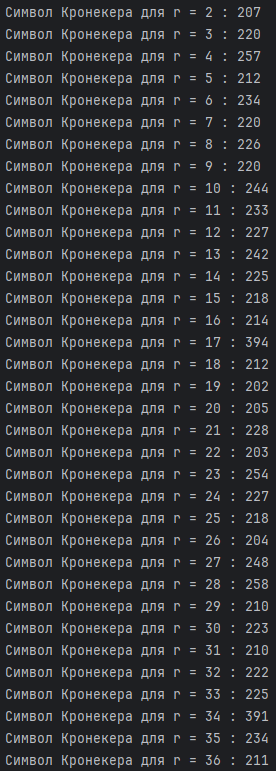


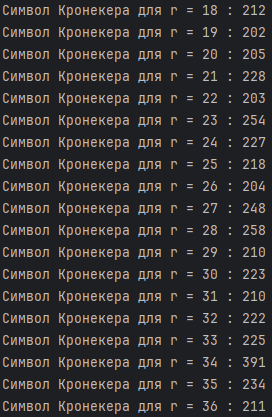
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.



Отже чим довший ключ тим менший індекс відповідності. Це пов’язано з тим, що більший період ключа більше спотворює частоти літер у шифротексті.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Для визначини довжини ключа використали символ Кронекера.



Найбільше значення символ Кронекера приймає при довжині ключа r = 17 : 394, також можна побачити, що при r = 34 : 391, значення також сильно відрізняється від інших та наближене до значення при ключі довжиною 17, отже r = 17.

Для знаходження значення ключа використовували обернену формулу до шифрування :

k = (y – x) mod m,

де y – найчастіша буква блоку, x – начастіша буква російської мови ‘о’



Логічно що у частині ключа ‘возвращение’ все ок. У частині ‘джлнда’ є помилки.  
якщо подивитися на розшифроаний текст очевидно, що у підстроці ‘дорофейльвовиф’ останню букву треба замінити на ‘ч’. ‘ч’ знаходиться на 3 позиції правіше ‘ф’, отже букву ‘л’ з ключа треба зсунути на 3 вліво – отримуємо ‘и’. Пройшовши далі по розшифрованому тексту: ‘дорофейльвовичпсвторыкобылыниразьвжизни’ очевидно, що замість ‘ь’ має стояти ‘у’, зміщуємо 15 букву ключа на 9 вправо, отримуємо ‘н’. Фінальний ключ: ‘возвращениеджинна’

