

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Мета роботи

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

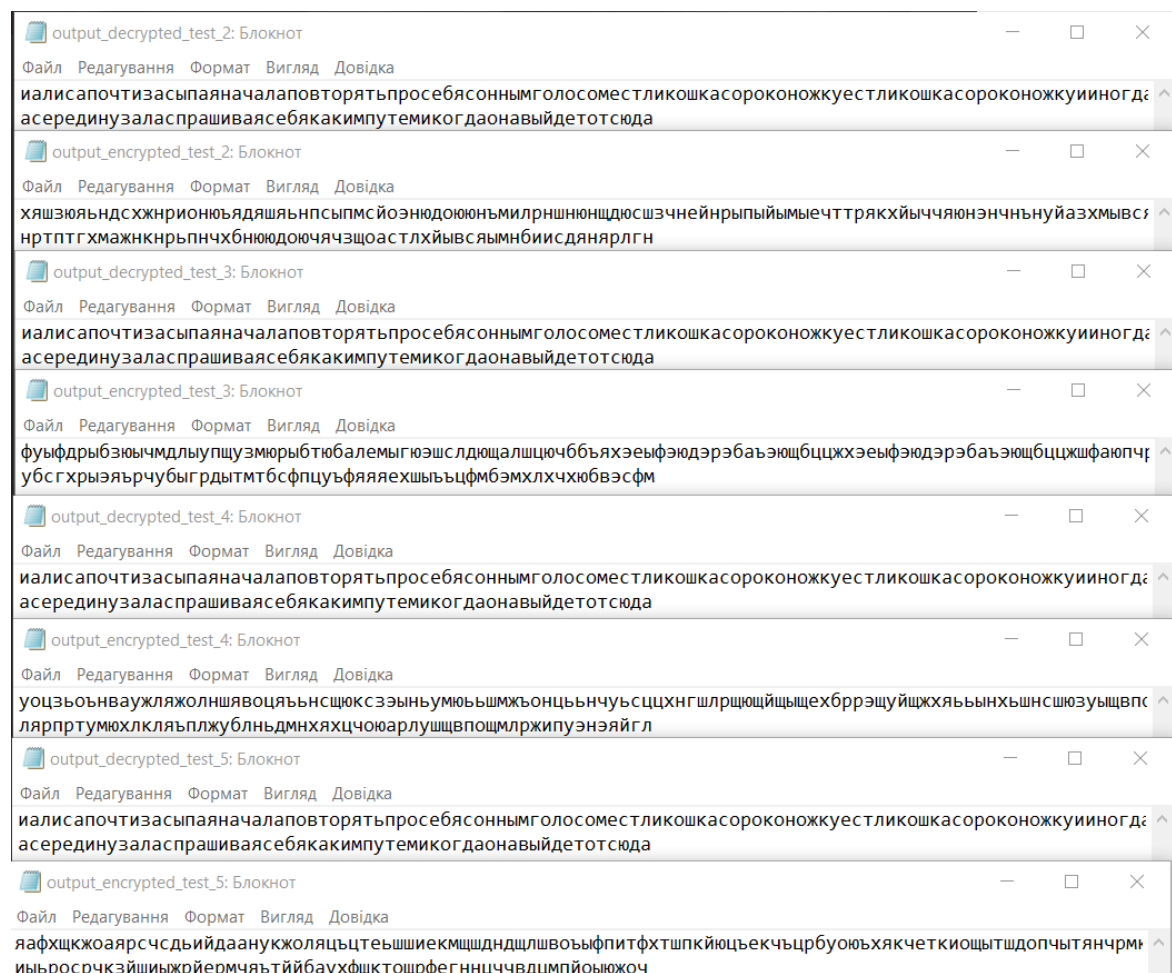
Виконали: Соколовська Дарія, Дудник Нікіта, ФБ-13

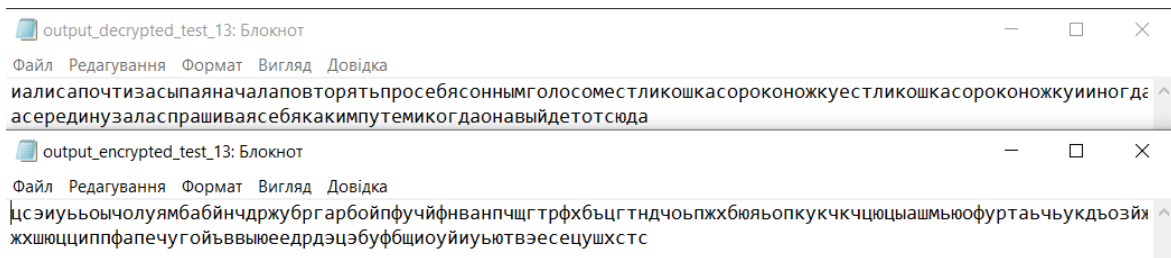
Довільний текст у файлі text.txt

Текст із завданням по варіанту (1): task.txt

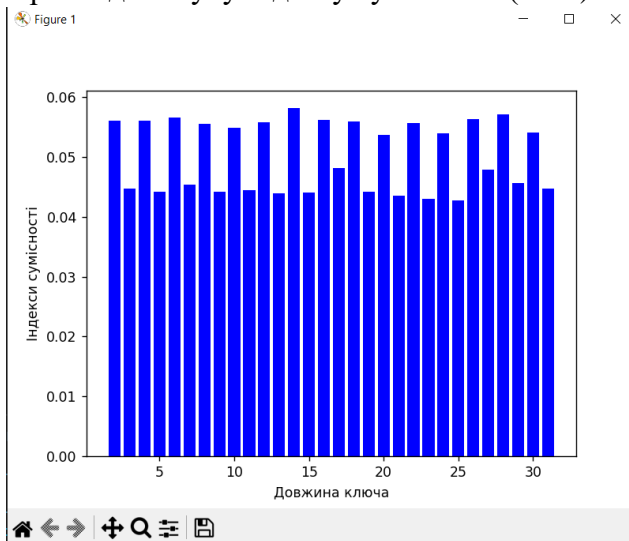
Ключі:

2	ня
3	мур
4	лоля
5	чайник
13	оставь надежду

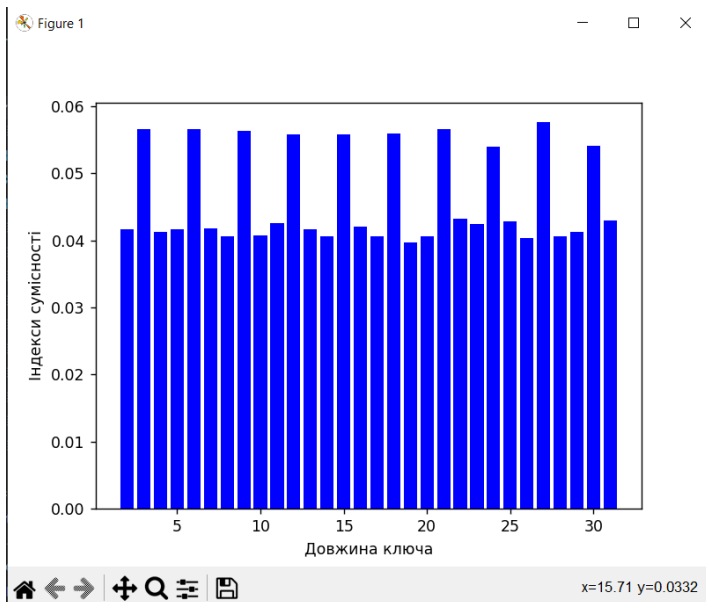




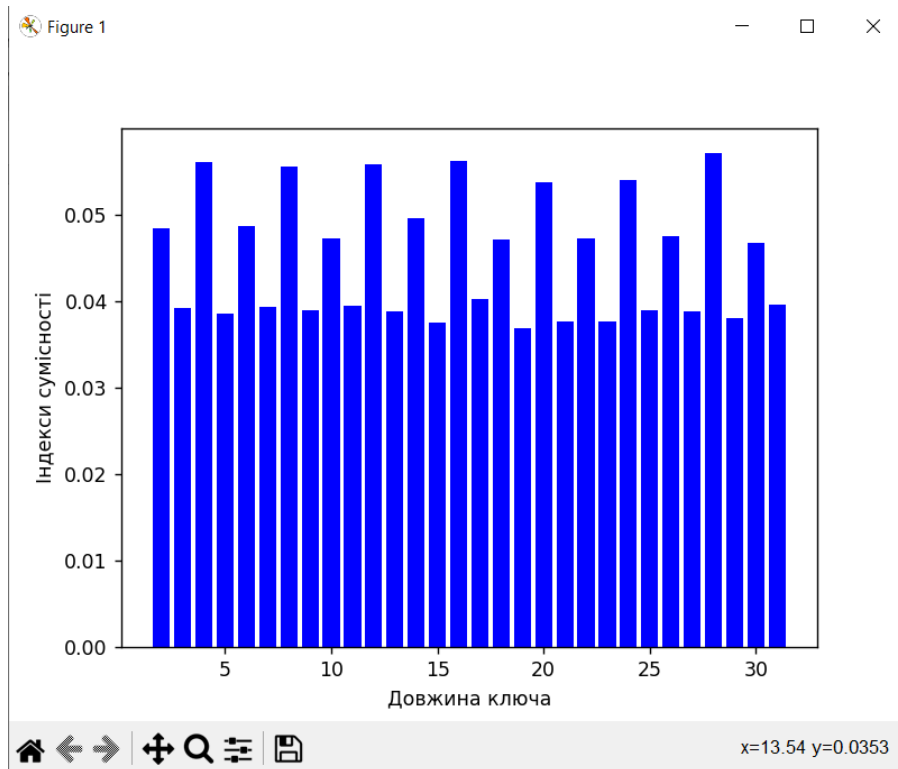
Приклад пошуку індексу сумісності ($r = 2$)



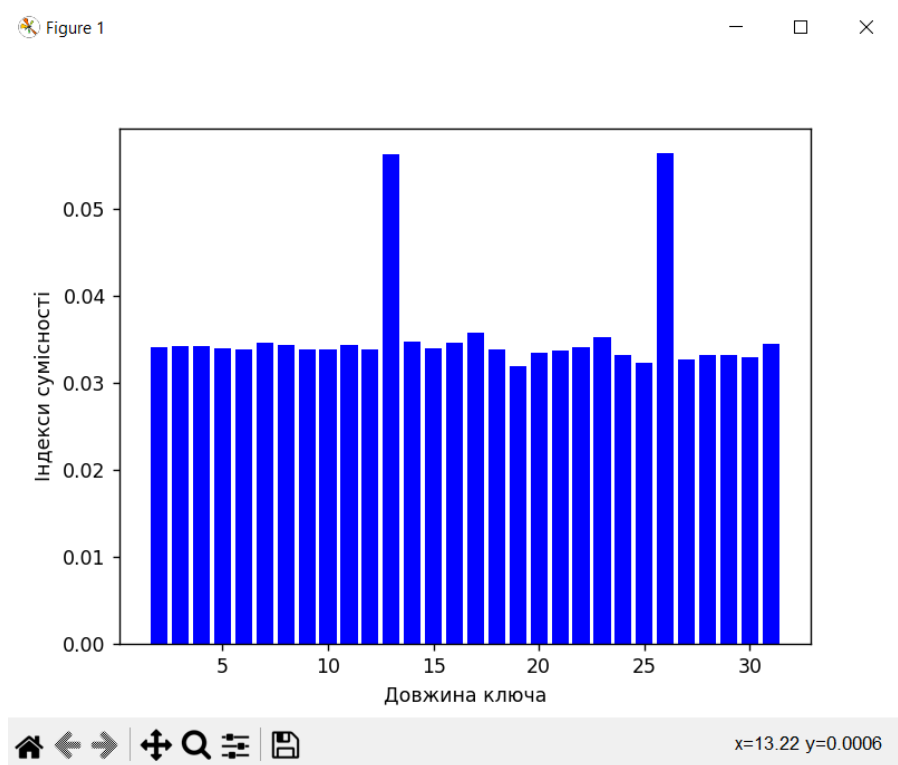
$r = 3$



r=4



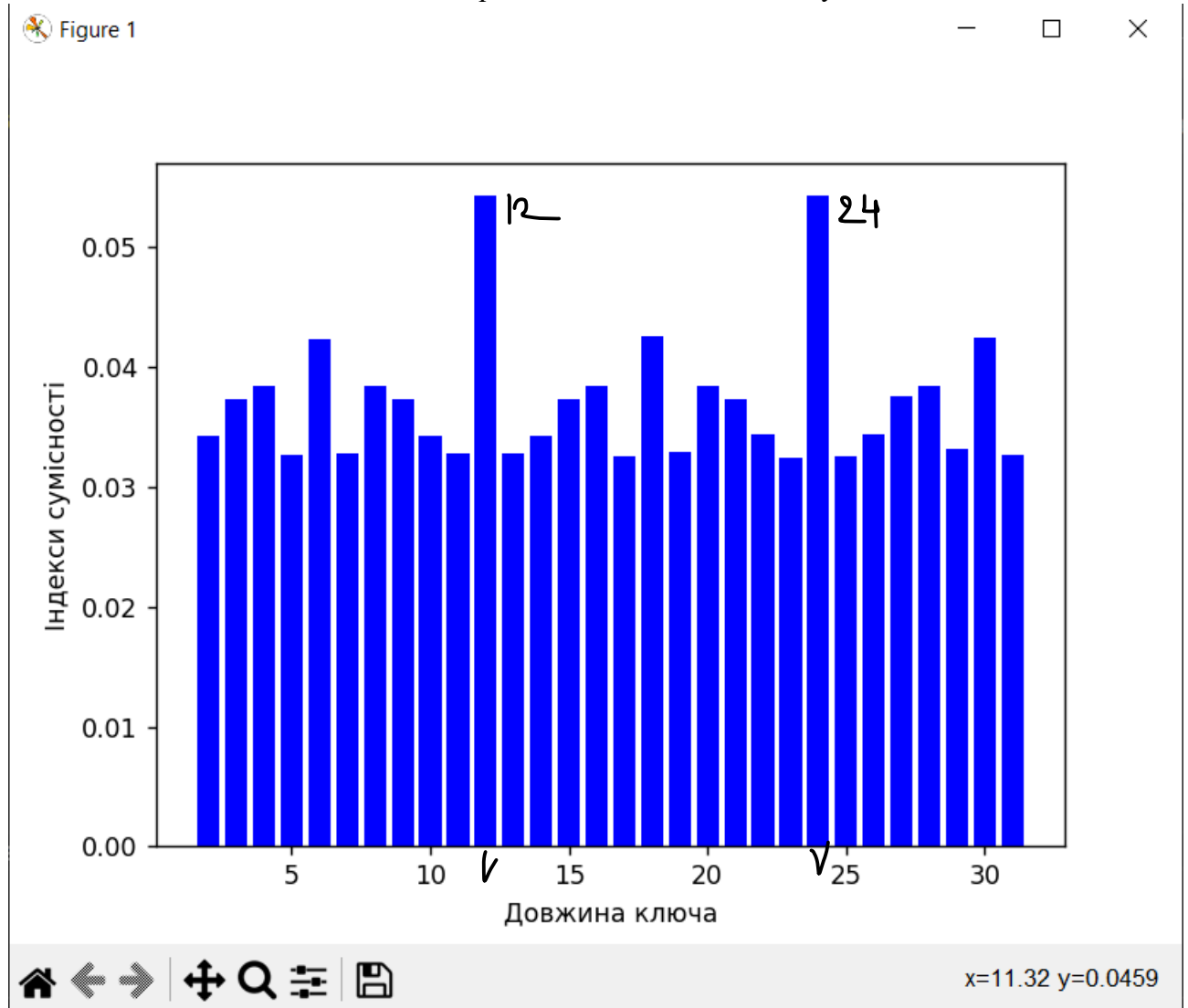
r=13



оригінальний текст: I = 0.056425806009524786

Отже, все працює, тепер переходимо до дійсно важливих справ

Тепер варто подивитися на текст, який нам надано по варіантах. Для початку, так само подивимося на індекси відповідності різних довжин блоків тексту:



Бачимо, що можливий період – 12 (з 24 не спрацювало, плавали, знаємо). Підставляємо його у наступну функцію, яка на основі частотного аналізу символів у блоці (лаба 1 привіт) видаватиме нам можливий ключ:

вшебспирбуря

Трохи криво-косо, але можна здогадатися що використовувати варто ключ «вшекспирбуря» (В.Шекспір «Буря»). Трохи магії скриптів з поту, крові й сліз і:

output_decrypted_test: Блокнот

Файл Редагування Формат Вигляд Довідка

действующилицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантс
егчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимваламнетделадокорольмаршпс
тьянязватебевглоткупроклыйгорланнечестивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтес
еровходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасу
выиволоснеупалсидисьслушайвсейчасузнаешьмирандавычастособиралисьмнеоткрытьктомыипрерывали
похоронныйзвондухидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоетс
ыкорольнеаполясаммоиглазастехпорнепросыхаликаквиделичтомойотецкорольпогибвморскихволнахмира

Дякуємо за увагу.

Труднощі які виникли:

- Під час написання скрипту для отримання індексів сумісності трохи ступили, і використали замість розділення на певну кількість блоків, розділення на блоки певної довжини.
- Розуміння призначення математичного індексу. Трохи згодом допетрили.

Висновки:

Було цікаво зламувати шифр Вінежера, при чому доволі неочікуваним способом. Достатньо яскравий приклад як математичні (на перший погляд абстрактні) величини та методи набувають практичного сенсу для розв'язання таких завдань. Також, трохи неочікувано було виявити що шифр Цезаря є лише частковим випадком шифру Вінежера, хоча саме це потім на кінцевих кроках дає можливість швидко розшифрувати текст.