

Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ No2

Виконала студентка гр. ФБ-24:  
Тішевська Анна

Київ–2025

Порядок виконання роботи

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

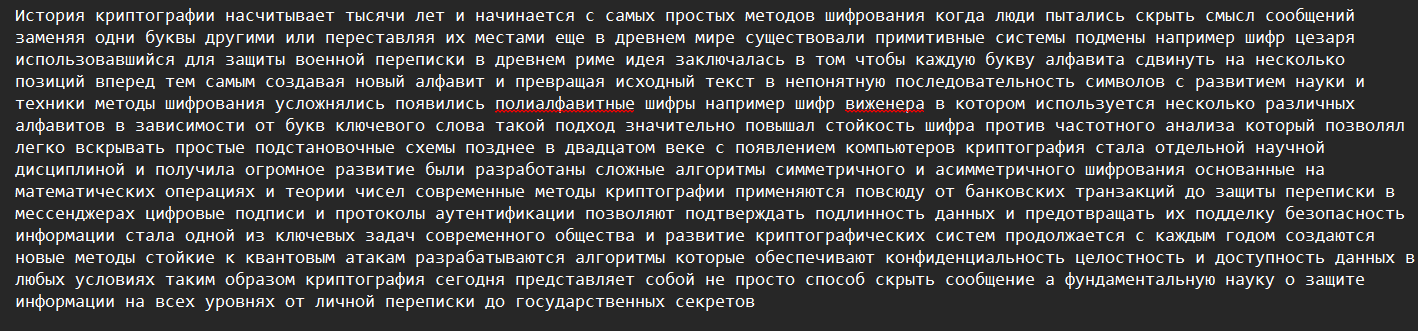
Віженера з цими ключами.

Шифрування тексту різними ключами

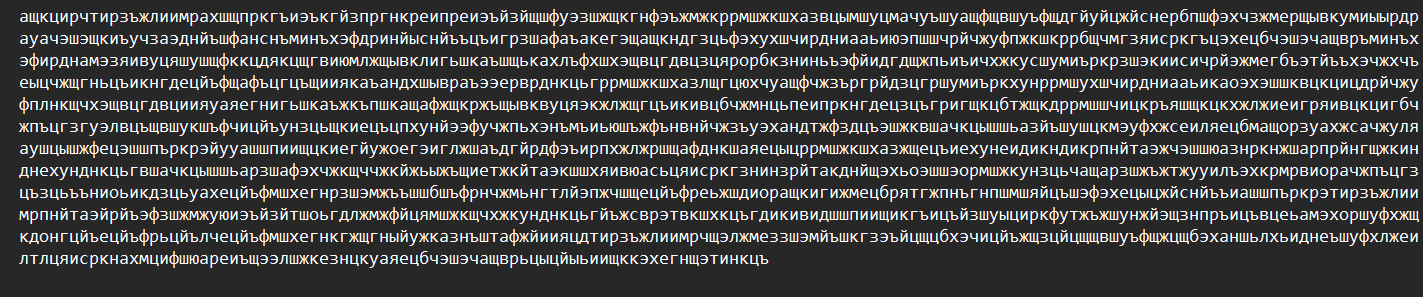
Обрано відкритий текст — файл text\_task1.txt.

Використано ключі:

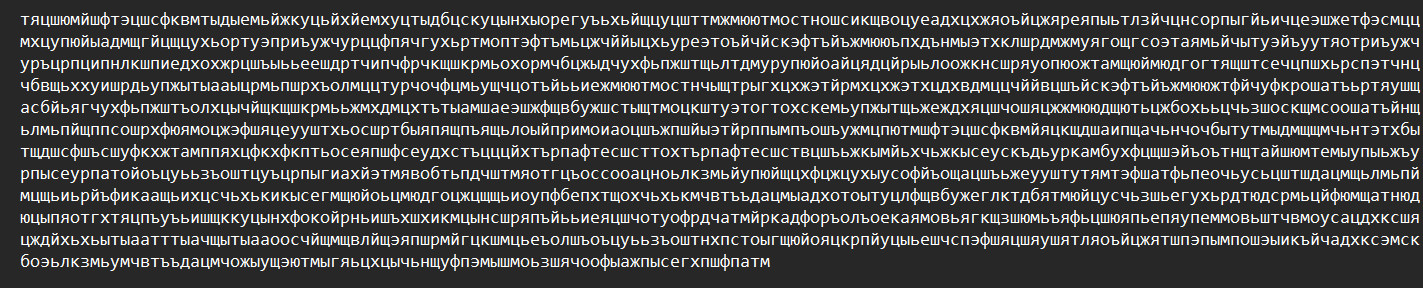
1. "ши" (r=2)
2. "код" (r=3)
3. "тест" (r=4)
4. "ключи" (r=5)
5. "математика" (r=10)
6. "криптоанализ" (r=13)
7. "частотныйанализ" (r=16)
8. "безопасностьданных" (r=18)



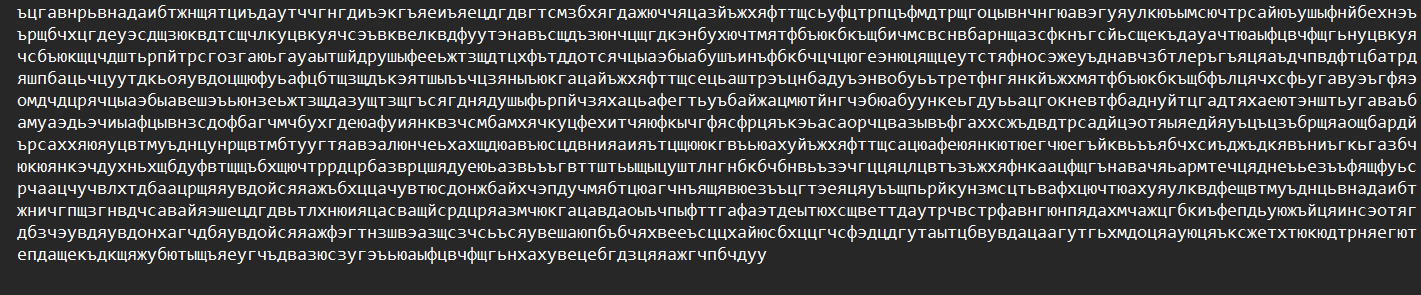
1. "ши" (r=2)



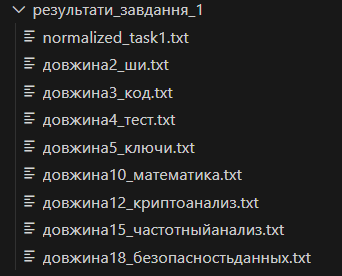
1. "код" (r=3)



1. "тест" (r=4)



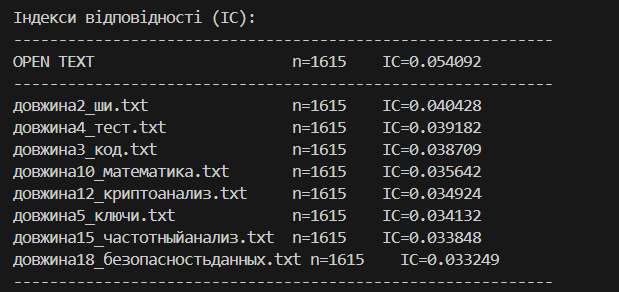
Щоб сильно не робити довгий протокол, інші результати можна подивитись в папці:

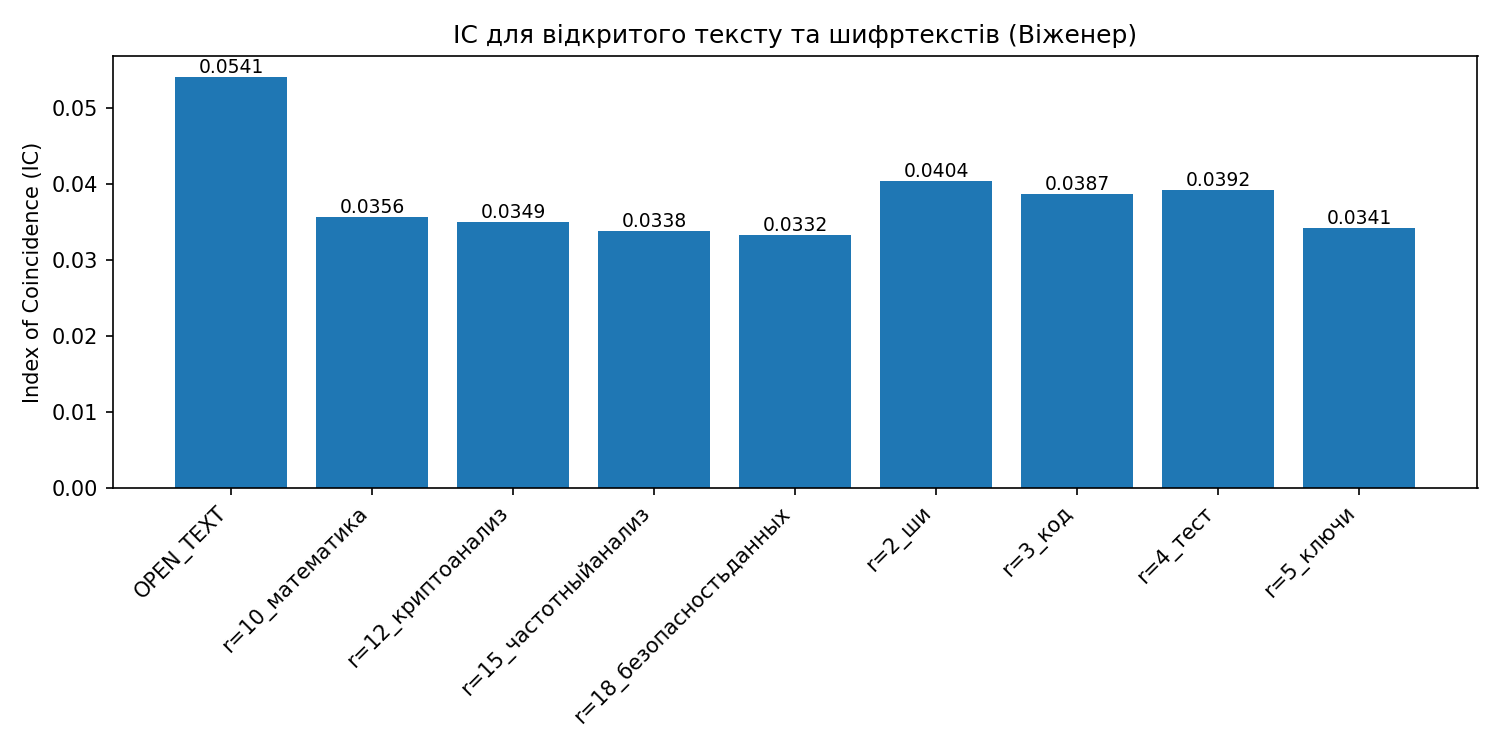


2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних

шифртекстів і порівняти їх значення.

1. Для відкритого тексту та всіх шифртекстів обчислено IC за формулою:
2. Використано скрипт, який формує CSV та діаграму.





Висновок:  
IC зменшується при збільшенні довжини ключа → шифр стає ближчим до випадкового. Це підтверджує зниження кореляції між символами та підвищення криптостійкості.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий

шифртекст (згідно свого номеру варіанта).

Суть завдання

У цьому пункті потрібно було розшифрувати зашифрований текст.  
Тобто треба знайти:

1. яка довжина ключа (період r) використана,
2. який сам ключ,
3. і в результаті - відновити вихідний текст.

Зрозуміло, що тут ключ нам невідомий, тому треба провести криптоаналіз шифру Віженера - не “підглядати” ключ, а визначити його статистично.

Як саме я це робила

1. Підготовка файлу

Я відкрила файл var5.txt, де був зашифрований.  
Перед обробкою програма нормалізує текст:

переводить усі літери у нижній регістр,

замінює ё → е,

прибирає всі символи, які не входять до 32-літерного російського алфавіту.

Це потрібно, бо інакше розрахунок індексів і пошук ключа будуть некоректними.

2. Визначення довжини ключа (періоду r)

Щоб зрозуміти, з якою довжиною ключа шифрували, я порахувала індекс відповідності IC(r) та значення Dᵣ(r) для різних r (від 2 до 40).

IC(r) показує, наскільки частоти літер у кожному “стовпчику” схожі на звичайну мову.  
Якщо IC близький до значення для російської (~0.066) - це може бути справжня довжина ключа.

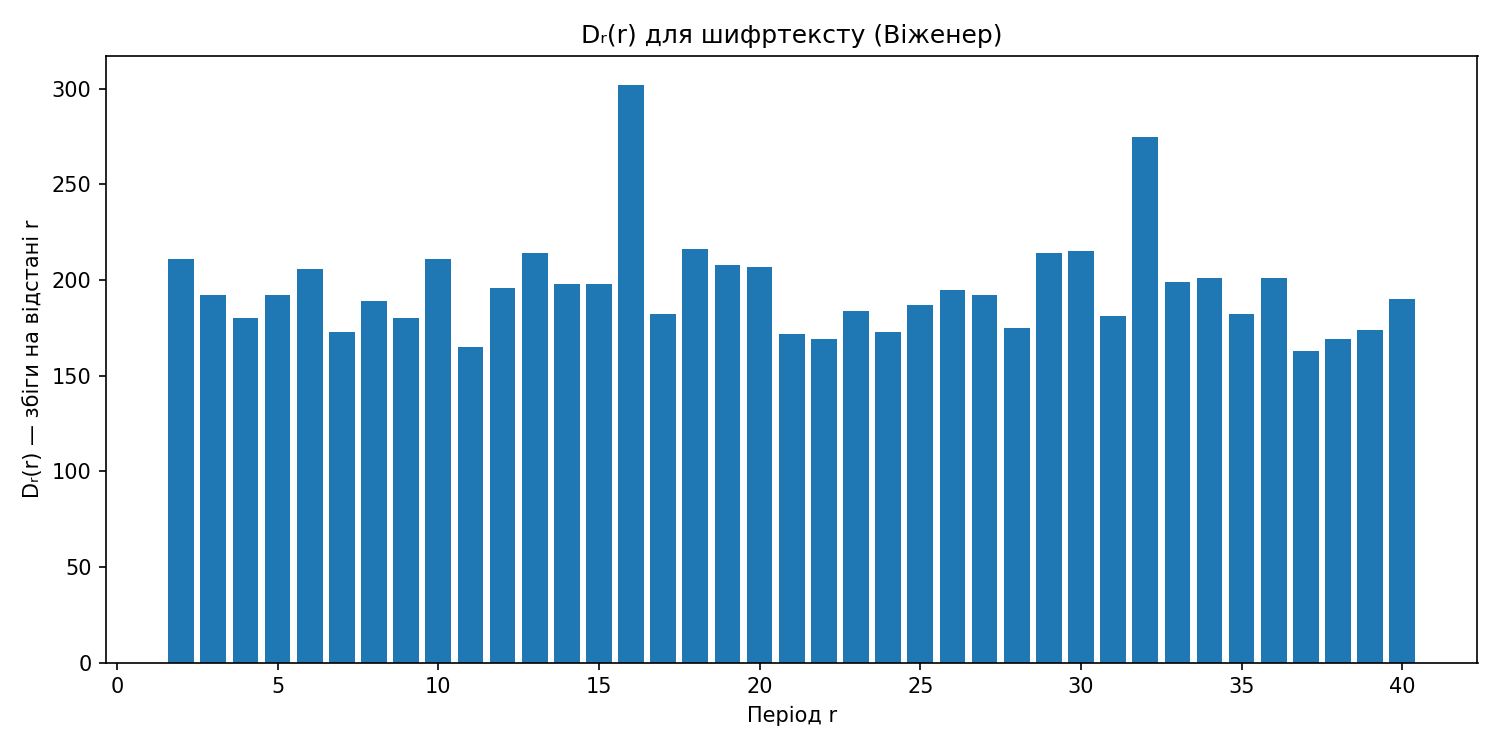
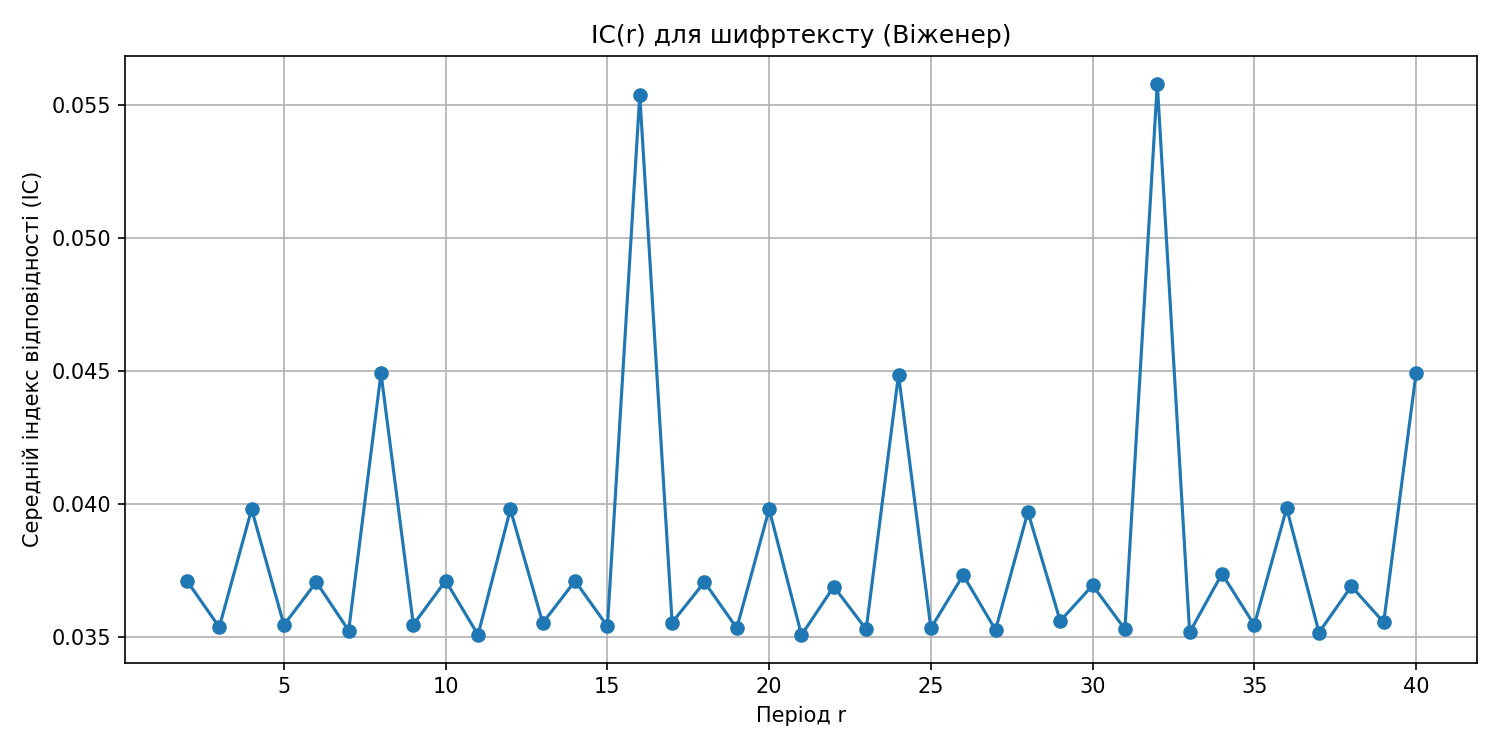
Dᵣ(r) - це просто кількість однакових літер, які повторюються через r позицій.  
Якщо Dᵣ великий - це теж натяк, що r може бути справжнім періодом.

Програма будує дві діаграми:

IC(r) - плавна крива з піками на підозрілих значеннях r.

Dᵣ(r) - стовпчикова діаграма збігів.

На цих графіках легко побачити, при якому r з’являється помітний пік - це і є довжина ключа.



3. Пошук самого ключа

Коли знайдено можливий період, текст ділиться на r колонок, і для кожної колонки робиться частотний аналіз.

Для кожної колонки програма:

зсуває її на всі можливі варіанти (0–31),

порівнює отриману частотну таблицю з типовими частотами російських літер,

обирає той зсув, де різниця (χ²) найменша.

Так знаходиться кожна літера ключа (по суті, це найімовірніший “зсув” для кожної позиції).

Далі програма ще кілька разів уточнює ключ (локальна оптимізація), перевіряючи сусідні варіанти літер, щоб зменшити сумарну χ²-помилку.  
Результат зберігається у вигляді:

cand\_r16\_keyCHI2\_первичныйключ.txt

cand\_r16\_keyREF\_уточненныйключ.txt

другий файл — кращий, бо вже після уточнення.

4. Розшифрування

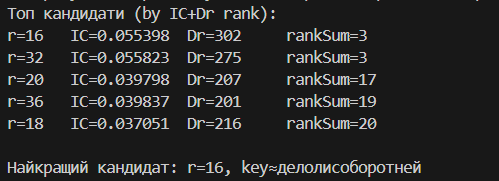
Після того, як знайдено ключ, текст розшифровується за формулою:

і записується у звичайний файл .txt.  
Якщо ключ підібраний правильно — текст читається нормально, з осмисленими словами.



5. Аналіз результатів

На екрані програма також виводить таблицю:

...

Найкращий кандидат: r=16, key≈делолисоборотней

Отже, для мого варіанта 5 найімовірніша довжина ключа була r = 16,  
а знайдений ключ — приблизно “делолисоборотней”

Висновок по завданню 3

1. Визначено можливий період ключа за допомогою IC(r) і Dᵣ(r).
2. Пікове значення IC показало довжину ключа ~16.
3. Ключ відновлено за χ²-методом та уточнено.
4. Отримано повністю читабельний відкритий текст.
5. Робота показала, що шифр Віженера можна розкрити без знання ключа, якщо текст досить довгий і мова відома.

**Висновок**

У ході роботи було досліджено шифр Віженера, виконано шифрування текстів з різною довжиною ключа, обчислено індекси відповідності та проведено криптоаналіз наданого шифртексту.  
Отримано, що зі збільшенням довжини ключа стійкість шифру зростає, а статистичні методи (IC, Dᵣ, χ²) дозволяють успішно відновити ключ і розшифрувати повідомлення.  
Робота закріпила практичні навички з криптографії та аналізу шифрів.