Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”

КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Тема: “Криптоаналіз шифру Віженера”

Варіант: 7

Виконали: студенти Оласюк Олександр
групи ФБ-32 та Гарбар Дар’я
групи ФБ-33

Київ 2025

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

Хід роботи:

ПІдібравши текст для шифрування (файл our_text.txt) та ключі довжини r = 2, 3, 4, 5, 10-20 знаків, написали скрипт, який шифрує відповідними ключами текст (файл encrypt.py)

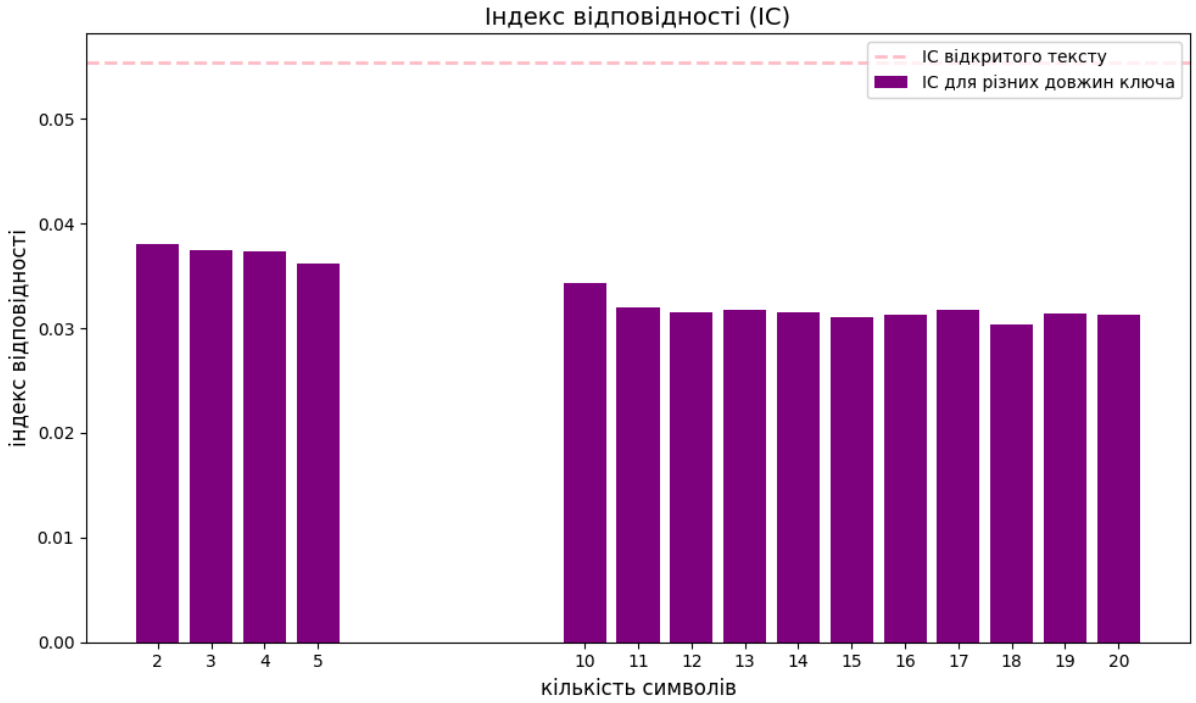
Далі підрахували індекси відповідності для відкритого тексту та всіх одержаних шифртекстів:

```
Індекс відповідності для відкритого тексту: 0.05539

Ключ 1: IC=0.03807
Ключ 2: IC=0.03745
Ключ 3: IC=0.03738
Ключ 4: IC=0.03619
Ключ 5: IC=0.03430
Ключ 6: IC=0.03205
Ключ 7: IC=0.03148
Ключ 8: IC=0.03178
Ключ 9: IC=0.03153
Ключ 10: IC=0.03103
Ключ 11: IC=0.03131
Ключ 12: IC=0.03174
Ключ 13: IC=0.03036
Ключ 14: IC=0.03140
Ключ 15: IC=0.03124

Всього створено 15 шифротекстів
```

Порівняємо їх:
Відкритий текст: 0.05539, що є типовим для російської мови.

Ключ з 2 символів: IC=0.03807
Ключ з 3 символів: IC=0.03745
Ключ з 4 символів: IC=0.03738

Ключ з 5 символів: IC=0.03619
Ключ з 10 символів: IC=0.03430
Ключ з 11 символів: IC=0.03205
Ключ з 12 символів: IC=0.03148
Ключ з 13 символів: IC=0.03178
Ключ з 14 символів: IC=0.03153
Ключ з 15 символів: IC=0.03103
Ключ з 16 символів: IC=0.03131
Ключ з 17 символів: IC=0.03174
Ключ з 18 символів: IC=0.03036
Ключ з 19 символів: IC=0.03140
Ключ з 20 символів: IC=0.03124



У ключів довжиною 2-5 індекс відповідності варіюється від 0.03619 до 0.03807, що є доволі високим показником, що значить, що шифртекст частково зберігає закономірності мови. Ключі вже від 10 симовіл мають варіацію від 0.03036 до 0.03619, при чому чим більший ключ від 12 симовів, тим менше повторюваності. Тобто зі збільшенням довжини ключа шифртекст стає більш подібним до випадкового набору символів, а розпізнати структуру мови стає все важче.

Згідно свого номеру варіанта – 7 (файл text_var7.txt):

пабьлхэбтэхмвахьфаййпяфаарсроппюдцецупнювигаооцыжащкуоагтчехвэшрнпшфоэъофлтоэухтхныеьипмэхотгймжьпсьъхфлсдшасалдвтмкцуяивэбсисаричврбнивлчйрнцдаыччъдс…

Розшифрували наданий шифртекст (скрипт для дешифрування у файлі decrypt.py) і отримали таке розшифрування:

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктонежилпонастоящемузаэтовремяонсменилодиннадцатьхозяевнониктоизнихневыдерживал…. (файл decrypted_text.txt).
ключ: арудазовархимаг (А. Рудазов Архимаг)

Висновки:
В ході лабораторної роботи ми реалізували скрипт для шифрування і дешифруння текстів шифром Віженера. Засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Було визначено за допомогою індексу відповідності, що зі збільшенням довжини ключа шифртекст стає більш подібним до випадкового набору символів, а розпізнати структуру мови стає все важче.