Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконав:

Студент групи ФБ-35

Ворона Сергій

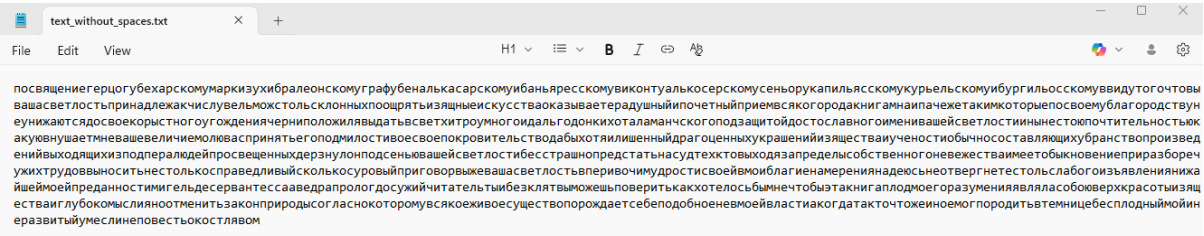
Київ — 2025

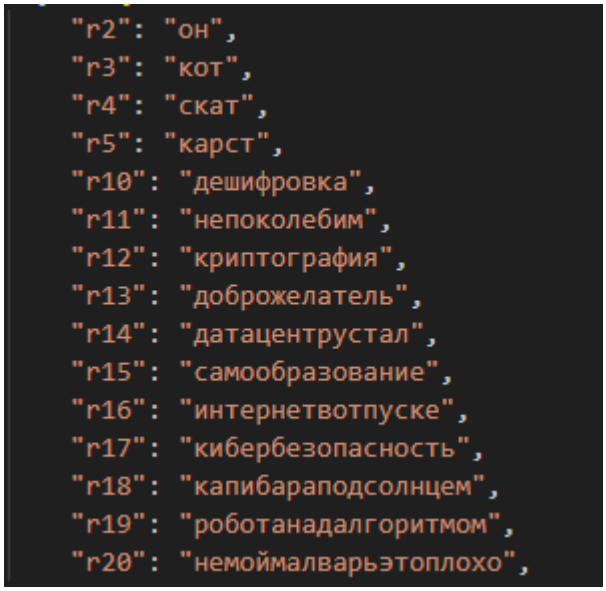
Мета роботи:

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

Порядок виконання роботи:

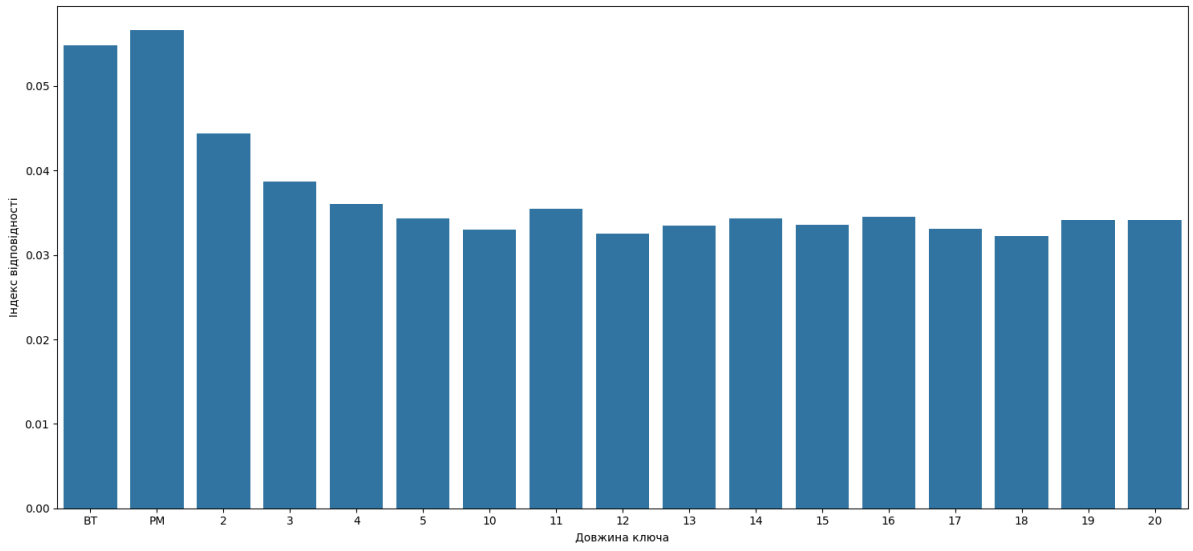
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.





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

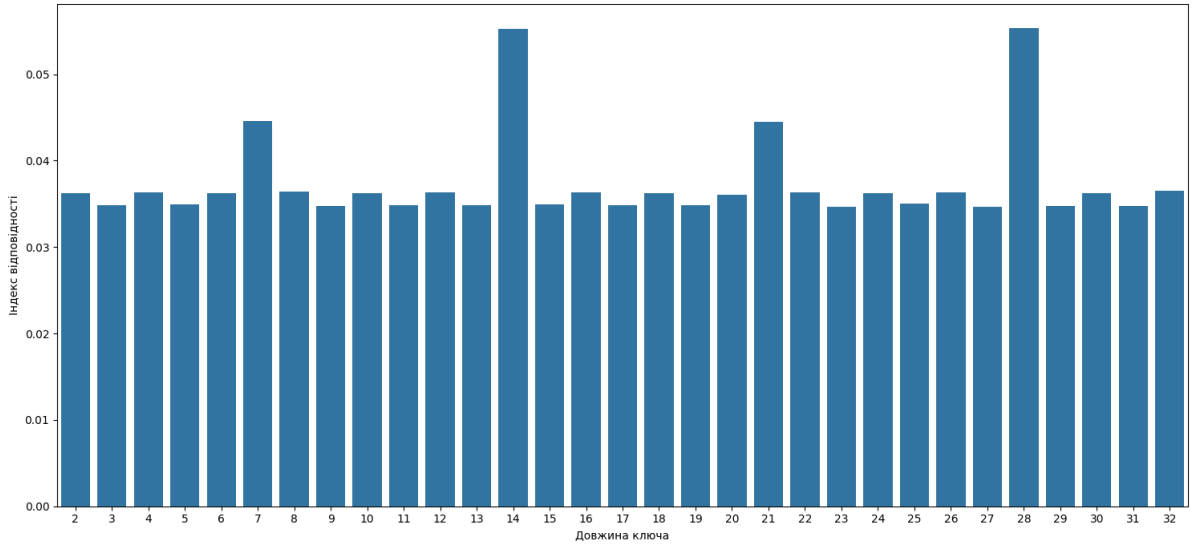
Довжина ключа	Індекс відповідності
ВТ	0,054822
РМ	0,056654
2	0,044353
3	0,038705
4	0,036019
5	0,034351
10	0,033004
11	0,035473
12	0,032538
13	0,033462
14	0,034344
15	0,033559
16	0,034482
17	0,033061
18	0,032269
19	0,034133
20	0,034176



3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно номеру варіанту). Варіант 2

Для знаходження довжини ключа використаємо перший алгоритм з методички

Довжина ключа	Індекс відповідності
2	0,036268205
3	0,034827682
4	0,036368141
5	0,034922938
6	0,0362575
7	0,04462598
8	0,036422614
9	0,034758232
10	0,036229739
11	0,034872671
12	0,036286975
13	0,034880863
14	0,055281685
15	0,034905048
16	0,036369598
17	0,034842145
18	0,036236069
19	0,034872247
20	0,036100466
21	0,044469842
22	0,036291616
23	0,034620482
24	0,036241608
25	0,034999922
26	0,036350458
27	0,034663226
28	0,055360827
29	0,034753828
30	0,036235603
31	0,034788022
32	0,036505018



Легко можна помітити наближення до ідеального індексу відповідності при довжині ключа 14 та 28, це нормально при кратних числах, найімовірніше, що довжина ключа 14.

Letter	Frequency
о	0,118635
е	0,084813
а	0,076447
и	0,070477
т	0,066341

Спробуємо знайти ключ відносно букви, що найчастіше зустрічається, та зробивши припущення, нею є одна з 5 найбільш частих букв в російському алфавіті (цю інформацію взяли з лабораторної роботи №1).

```
Ключ при 'о': жосвеыдиадозор
Ключ при 'е': пчълоднсйнчрчщ
Ключ при 'а': фьяруйтцотьхью
Ключ при 'и': мфчилбкожкфнфц
Ключ при 'т': вкнюбчадьакгкм
```

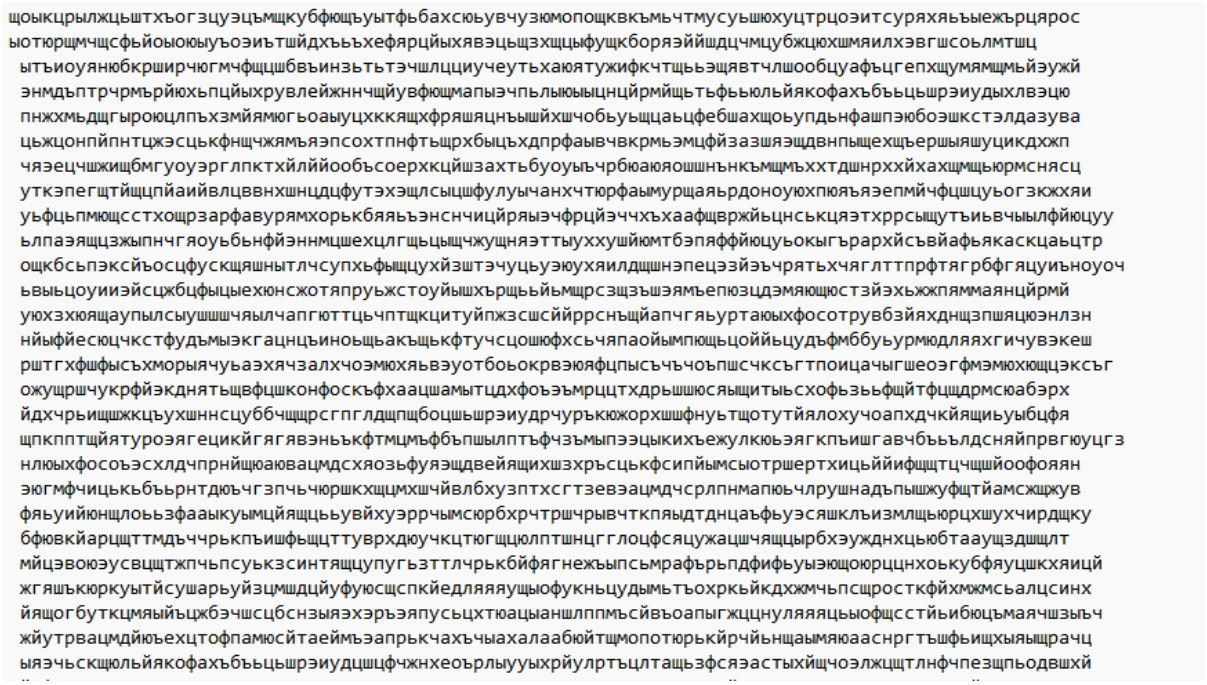
Можна помітити, що при “о” є логічне слово “дозор”, а от перша частина виглядає нелогічною, якщо ще раз уважно подивитися, то можна помітити, що при об’єднанні частин ключа при “о” та “е” вийде змістовний ключ.

```
Ключ при 'о': жосвеыдиадозор
Ключ при 'е': пчълоднсйнчрчщ
Ключ при 'а': фьяруйтцотьхью
Ключ при 'и': мфчилбкожкфнфц
Ключ при 'т': вкнюбчадьакгкм
```

Таким чином отримали ключ: “последнийдозор”

Спробуємо розшифрувати даний текст

ШТ



ВТ

Висновок

Впродовж виконання даної лабораторної роботи ми глибше на практиці розібралися з шифром Віженера, використовуючи його шифрували та розшифровували текст. Знаходили індекси відповідності для відкритого та зашифрованих різними ключами

текстів. Засвоїли методи частотного криптоаналізу і розібралися як проаналізувати шифртекест та знайти ключ для його розкодування.