Лабораторна робота №2

Криптоаналіз шифру Віженера

Виконали:

Борщевський Олександр(ФБ-03)

Ржевський Андрій(ФБ-03)

Мета роботи

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

Порядок виконання

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.

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

Варіант: 4, 16

Хід роботи

Початковою задачею було очищення тексту. Проблем на цьому етапу не виникло, усі не текстові символи видалили, прописні літери замінили на аналогічні стрічні, послідовність пробілів і знак переносу рядків замінили на пробіл. Після очищення тексту можна приступати до наступних задач

Шифровка тексту здійснювалася за такою формулою

$$y_i = (x_i + k_{i \bmod r} \bmod r) \bmod m$$

Дешифровка, відповідно

$$y_i = (x_i - k_{i \bmod r} \bmod r) \bmod m$$

Індекс відповідності обчислювався за формулою

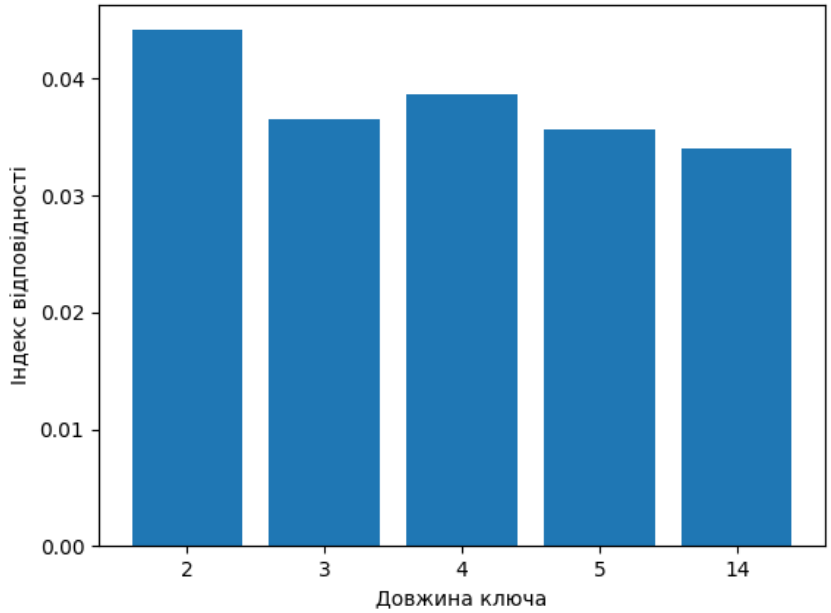
$$I = \frac{1}{n(n-1)} \sum_{t=0}^{31} N_t(N_t - 1)$$

де N_t – кількість появи літери t в тексті

Обчислені значення індексів відповідності для вказаних значень r

Індекс відповідності тексту - 0.05632

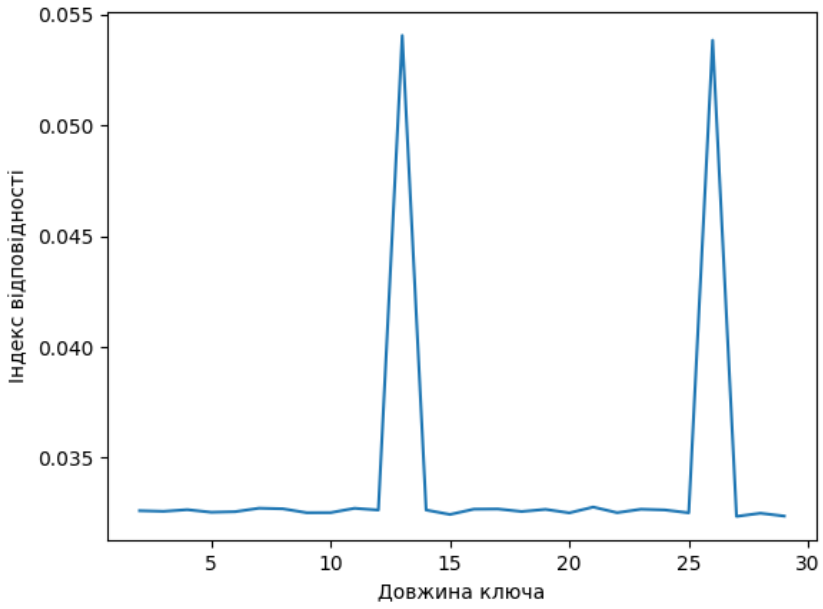
Довжина ключа	Індекс відповідності
2	0.04417
3	0.03653
4	0.03864
5	0.03570
14	0.03406



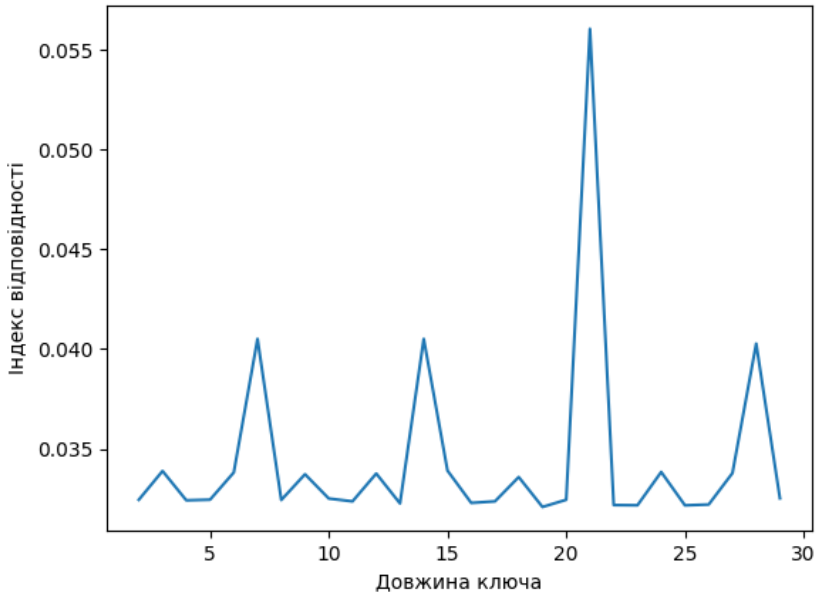
Набори значень індексів відповідності(взяте середнє значення), одержаних при встановленні довжини ключа шифру Віженера

Довжина ключа	Значення індексу відповідності(варіант 4)	Значення індексу відповідності(варіант 16)
2	0.032604	0.032455
3	0.032576	0.033896
4	0.032650	0.032429
5	0.032535	0.032460
6	0.032560	0.033823
7	0.032717	0.040513
8	0.032691	0.032444
9	0.032514	0.033734
10	0.032517	0.032518
11	0.032713	0.032376
12	0.032635	0.033770
13	0.054068	0.032272
14	0.032636	0.040512
15	0.032435	0.033916
16	0.032674	0.032299
17	0.032683	0.032377
18	0.032568	0.033593
19	0.032664	0.032095
20	0.032507	0.032456
21	0.032769	0.056041
22	0.032516	0.032190
23	0.032672	0.032180
24	0.032639	0.033847
25	0.032509	0.032177
26	0.053855	0.032218
27	0.032348	0.033791
28	0.032490	0.040274
29	0.032362	0.032527

4 варіант



16 варіант



Для розшифровки шифру Віженера ми розбивали текст на блоки для довжини ключа від 2 до 29. Для кожного блоку обчислювали середнє значення індексу відповідності. Та довжина ключа, чий блок, середнє значення відповідності якого найближче до середнього значення відповідності російської мови, була шуканою довжиною ключа. Далі, для кожного блоку тексту для даної довжини ключа ми шукали літеру, що зустрічається найчастіше і відштовхуючись від того, що найпопулярніша літера російської мови це літера “о”, робили висновки щодо літери, що міститься в ключі. Загалом, алгоритм підбирав близько 65-70% літер ключа вірно, інші літери можна було розпізнати “вручну”

Ключ для варіанта 4 – громыковедьма

Ключ для варіанта 16 – башняяростичерныемаки

Висновок: Під час виконання лабораторної роботи ми здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладу шифра Віженера. Також,

розшифрували текст, закодований даним шифром за допомогою аналізу індексів відповідності тексту.