Лабораторний практикум № 2 – Криптоаналіз шифру Віженера

Виконали: Гранік Микита ФБ-13, Тарасов Микита ФБ-12

Варіант: 7

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

Порядок роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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).

Хід роботи

На початку роботи ми підібрали текст $_{\text{р}}$осійською мовою. Далі очистили текст від пробілів, знаків пунктуації, великих літер та літери «ё». Зробили так само, як і під час виконання першого практикуму.

Далі переходимо до основної мети практикуму:

Для шифрування ВТ шифром Віженера використали наступну формулу:

$$y_i = (x_i + k_{i \bmod r}) \bmod m,\ i = \overline{0,n}.$$

Де xi – символи ВТ та yi – символи ШТ. Шифрування відбувається шляхом додавання букв ВТ до підписаних під ними букв ключа за модулем m.

Для знаходження індексу відповідності, який буде нам потрібний для дешифрування нашого ШТ, використовували наступну формулу:

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1)$$

Підібрали ключі різної довжини, та зашифрували довільний текст **golubki.txt** різними по довжині ключами. Табличка із індексом відповідности наведена нижче:

Довжина ключа	Індекс відповідності
ВТ	0.05802993326949858
2	0.03481115223700353
3	0.03471791600747666
4	0.03497394565363777
5	0.04184974759620721
15	0.0464745605687706

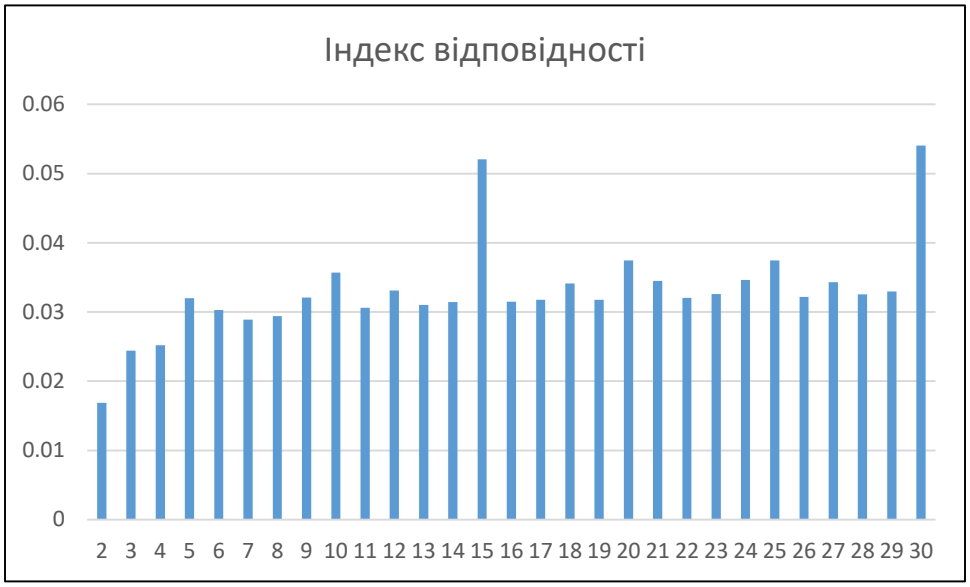
А вже для знаходження істинного значення r за допомогою індексу відповідності в методичці пропонується два можливих алгоритми. Ми обрали перший алгоритм, що виглядає так:

1. Для кожного кандидата r = 2,3,...(від 2 до 30) розбити шифртекст Y на блоки Y1, Y2, …, Yr
2. Обчислити значення індексу відповідності для кожного блоку.
3. Якщо сукупність одержаних значень схиляється до теоретичного значення I для даної мови, то значення r вгадане вірне. Якщо сукупність значень схиляється до значення $I_0 = \frac{1}{m}$, що відповідає мові із рівноімовірним алфавітом, то значення r вгадане неправильно.

Теоретичний індекс відповідности був взятий як індекс відповідності ВТ.

Набори значень індексів відповідності (середнє значення):

Довжина періоду	Індекс відповідності
2	0.016874205
3	0.024394107
4	0.025207316
5	0.031975676
6	0.030266286
7	0.028907152
8	0.029400311
9	0.032092322
10	0.035675636
11	0.030596433
12	0.03311262
13	0.031001398
14	0.031430682
15	0.052072491
16	0.031492667
17	0.031775284
18	0.034114674
19	0.031768944
20	0.037457226
21	0.034504428
22	0.032040283
23	0.032615172
24	0.034626392
25	0.037443598
26	0.032165825
27	0.0343041
28	0.032565601
29	0.03296068
30	0.054029234



Після цього, для кожного блоку тексту для даної довжини ключа (r) ми шукали літеру, що зустрічається найчастіше, і знаючи те, що літера «о» $_{р}$осійської мови зустрічається найчастіше, робили висновки щодо літери, що міститься в ключі. Це все робиться тому, що після встановлення значення періоду шифру подальше його розшифрування зводиться до серії розшифрувань шифрів Цезаря, тобто кожен фрагмент Yi зашифрований шифром Цезаря з ключем k. Знайти цей ключ можна за формулою $k= (y^* – x^*)modm$, де y^* – буква, що частіше за всіх зустрічається у фрагменті Yi, а x^* – найімовірніша буква у мові.

Знайдений ключ для нашого варіанту: *арудазовархмиаг*

Висновки: Під час виконання лабораторної роботи ми отримали досвід у роботі та аналізі шифрів, зокрема шифру Віженера. Ми зашифрували вибраний вхідний текст різними ключами, і потім, використовуючи криптоаналіз, визначили довжину ключа та сам ключ для розшифрування шифротексту, що був заданий у варіанті. Насамкінець, ми успішно розшифрували текст, застосовуючи отриманий ключ.