

## 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 поточкових 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 російською 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  $x_i$  – символи ВТ та  $y_i$  – 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:

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

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

Довжина ключа	Індекс відповідності
BT	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  $r = 2, 3, \dots$  (від 2 до 30) розбити шифртекст  $Y$  на блоки  $Y_1, Y_2, \dots, Y_r$
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 вірно. Якщо сукупність значень схиляється до значення  $I_0 = \frac{1}{m}$ , що відповідає мові із рівноімовірним алфавітом, то значення  $r$  вгадане неправильно.

Теоретичний індекс відповідності був взятий як індекс відповідності BT.

Набори значень індексів відповідності (середнє значення):

Довжина періоду	Індекс відповідності
2	0.033853888
3	0.036151871
4	0.033742934
5	0.039520848
6	0.036125056
7	0.033821792
8	0.033740945
9	0.036082806
10	0.039522528
11	0.033676546
12	0.036044857
13	0.033575199
14	0.033924554
15	0.056051773
16	0.033683288
17	0.033688674
18	0.036089865
19	0.033536423
20	0.039389365
21	0.036193882
22	0.033594664
23	0.034086543
24	0.036087592
25	0.039017166
26	0.033468936
27	0.035640379
28	0.033727647
29	0.03404426
30	0.056003132



Після цього, для кожного блоку тексту для даної довжини ключа ( $r$ ) ми шукали літеру, що зустрічається найчастіше, і знаючи те, що літера «о» російської 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  $Y_i$  зашифрований шифром Цезаря з ключем  $k$ . Знайти цей ключ можна за формулою  $k = (y^* - x^*) \bmod m$ , де  $y^*$  – буква, що частіше за всіх зустрічається у фрагменті  $Y_i$ , 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.