КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Варіант 2

Виконали:

Винник Михайло та Кузнєцов Олексій ФБ-12

Мета роботи:

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

Порядок виконання 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

Перед початком роботи ми підібрали Вхідний текст російською мовою, як сказано в умові. Далі нам треба було його очистити від пробілів, знаків пунктуації, великих літер та літер «ё». Проблем не виникло, бо таке завдання ми робили в минулій роботі.

Після цього можна приступати до виконання основних завдань комп'ютерного практикуму.

Для шифрування тексту шифром Віженера використовуємо таку 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.

А вже для дешифрування ми використали деякий алгоритм, в якому треба було знайти індекс відповідності тексту. Він шукається за формулою:

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

де Nt − кількість появи літери t в тексті.

А 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 32) розбити шифртекст Y на блоки Y1, Y2, …, Yr.

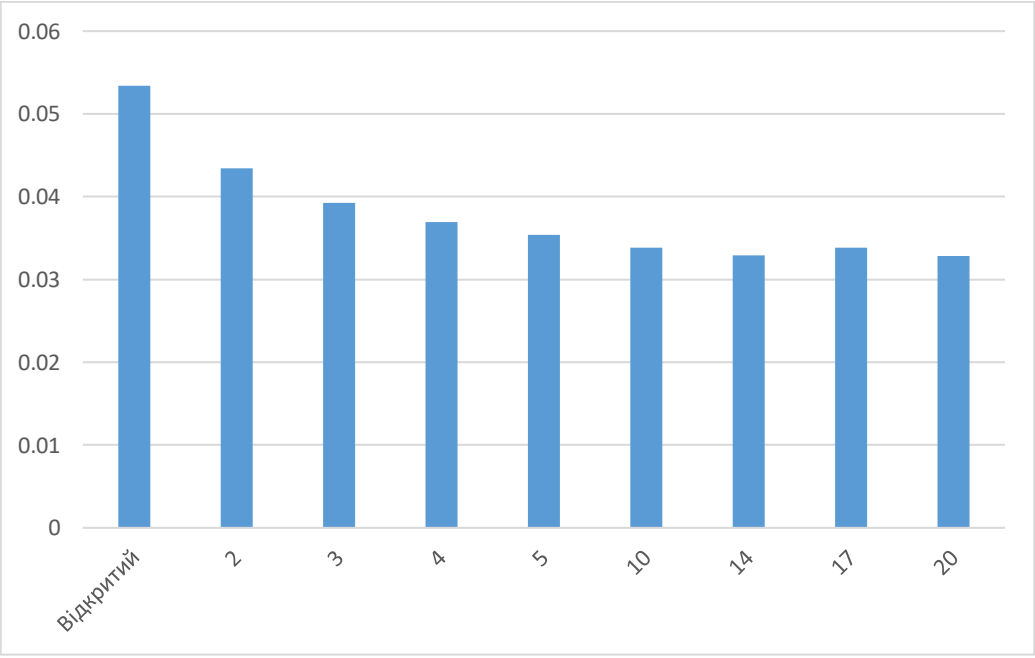
2) Обчислити значення індексу відповідності для кожного блоку.

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.

Обчислені значення індексів відповідності для вказаних значень r (довжини ключа)

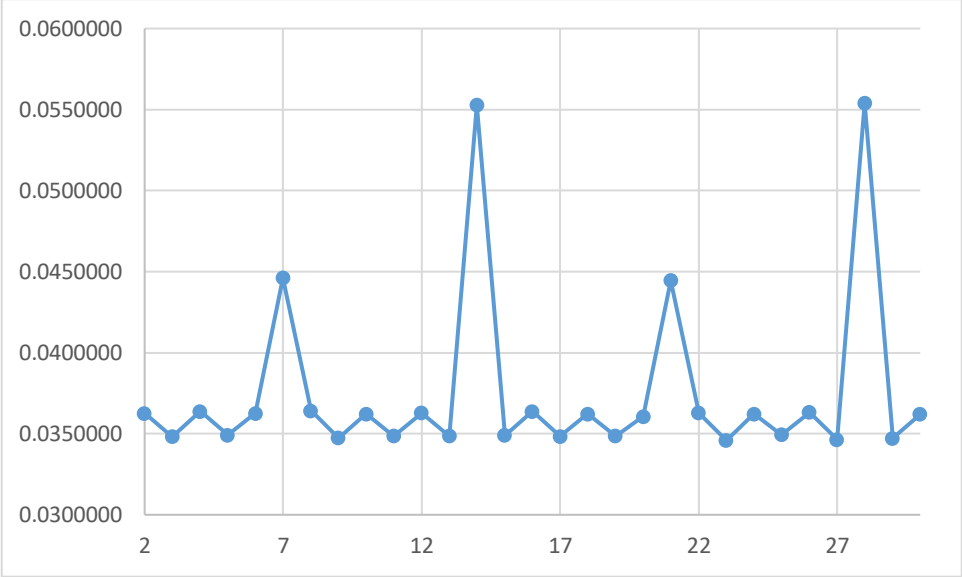
Індекс відповідності тексту - 0,053412

Ключ	Індекс відповідності
2	0,0434415
3	0,039256927
4	0,036911934
5	0,03540511
10	0,033811436
14	0,032892692
17	0,033872127
20	0,032840372



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

Довжина ключа	Індекс відповідності
2	0,0362714
3	0,0348287
4	0,0363756
5	0,0349165
6	0,0362595
7	0,0446164
8	0,0364284
9	0,0347406
10	0,0362268
11	0,0348599
12	0,0362851
13	0,0348648
14	0,0552841
15	0,0348962
16	0,0363726
17	0,0348376
18	0,0362311
19	0,0348614
20	0,0360686
21	0,0444651
22	0,0362898
23	0,0345868
24	0,0362267
25	0,0349490
26	0,0363224
27	0,0346423
28	0,0554043
29	0,0347288
30	0,0362009



Далі, для кожного блоку тексту для даної довжини ключа (r) ми шукали літеру, що зустрічається найчастіше, і знаючи те, що найпопулярніша літера російської мови це літера “о”, 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. Кожен фрагмент Yi зашифрований шифром Цезаря з ключем k .Знайти цей ключ можна, поклавши k= (y* – x*)modm, де y* – буква, що частіше за всіх зустрічається у фрагменті Yi, а x* – найімовірніша буква у мові.

Ключ для нашого варіанта – последнийдозор

Як виглядає розшифрований текст:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайнейсеройравнинывзгляднефиксир
оваляркихкрасоквцелойкартиненостоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзелень
юнадголовойзастылобелоесрозовымбудтомолочнуюрекуперемешалискисельнымиберегамидаивыплеснуливнебесаащеду
лветерибылохолодномневсегдахолодноначетвертомслоесумраканоэтоиндивидуальнаяреакциягесерунапротивбыложаркол
ицораскраснелосьполбустекаликапелькипотамненехватаетсилысказалялицогесерасовсемпобагровелоответнеправильныйт
ывысшиймагтакполучилосьслучайнонотывысшийпочемувысшихмаговтакженазываютмагамивнекатегорийпотомучторазни
цавсилемеждуниминастольконезначительначтонеможетбытьисчисленаиневозможноопределитьктосильнееактослабеепро

Висновок: Під час виконання лабораторної роботи ми здобули навички роботи та аналізу шифрів, на прикладі шифру Віженера. Ми зашифрували свій обраний вхідний текст, а також шляхом криптоаналізу підібрали довжину ключа та визначили сам ключ до шифротексту, що був наданий у варіанті, після чого розшифрували текст.