КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

ФБ-12 Юрченко Вікторія

Варіант 10

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

Для шифрування беру частину тексту з файлу для минулої роботи. Ключі генеруються випадковим чином з символів алфавіту (функція `gen_key`). Зашифрування проходить так:

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

Де y(i) – літера шифртексту, x(i) – літера відкритого тексту, k(i mod(r)) – літера ключа, m – кількість літер у алфавіті, n – довжина відкритого тексту.

Індекс відповідності обчислюється за формулою:

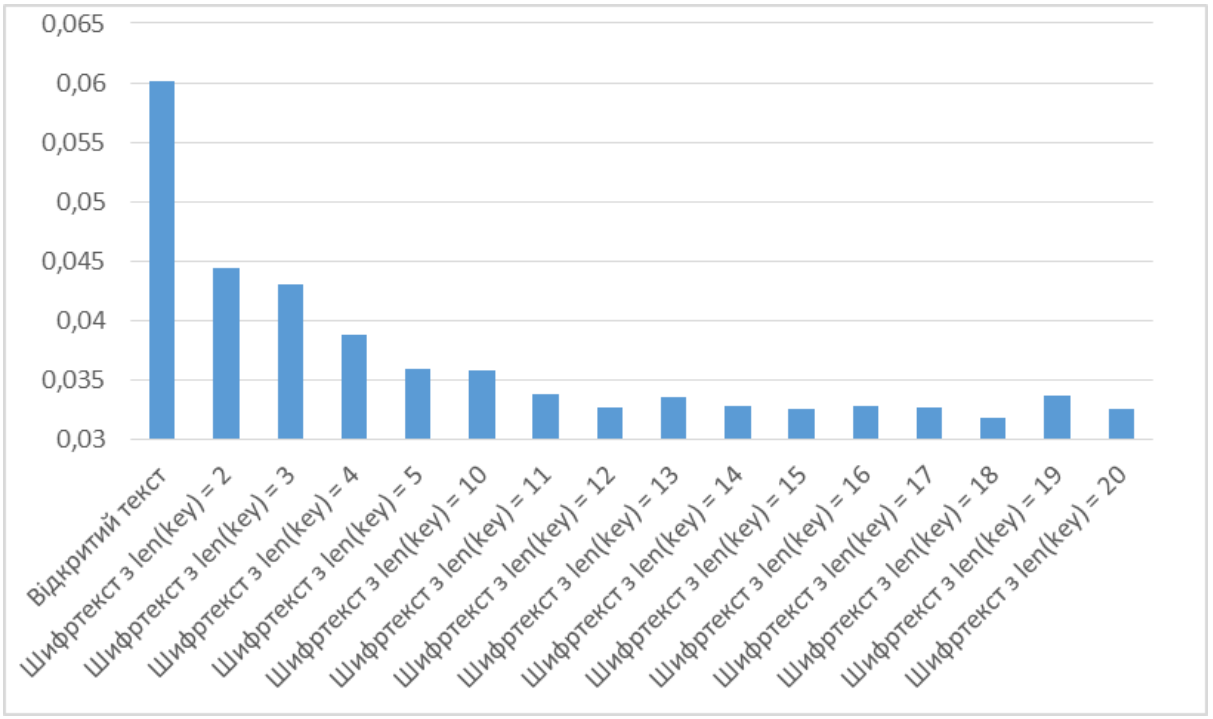
$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y) - 1)$$

Де n – довжина тексту, $N_t(Y)$ – кількість поява букви t у тексті Y.

Використовуючи одержані під час виконання першого комп’ютерного практикуму дані, було отримано теоретичне значення індексу відповідності: *0.05698919496*

Індекс відповідності для відкритого тексту: 0.06013166793867079

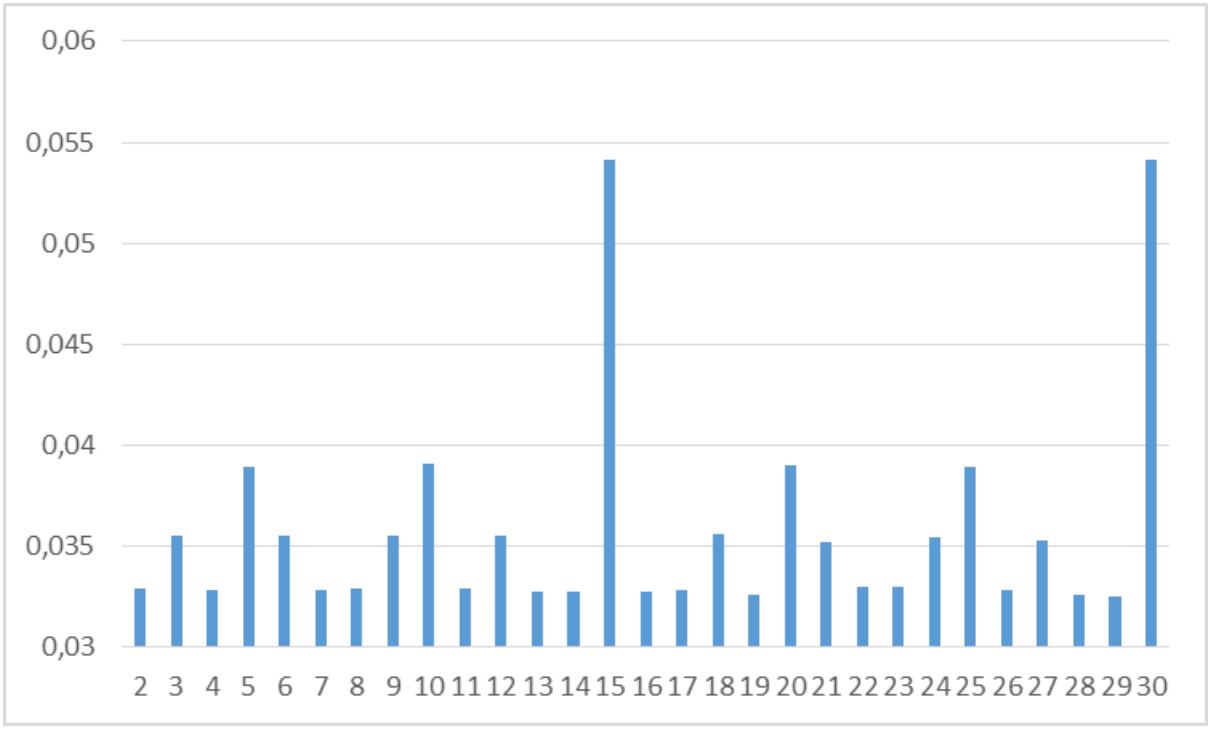
Вид тексту	*Індекс відповідності*
Відкритий текст	0.06013166793867079
Шифртекст з len(key) = 2	0.04444692640370308
Шифртекст з len(key) = 3	0.04305951117812401
Шифртекст з len(key) = 4	0.03882404770325695
Шифртекст з len(key) = 5	0.03587051618547681
Шифртекст з len(key) = 10	0.03585562442992498
Шифртекст з len(key) = 11	0.03374720003971135
Шифртекст з len(key) = 12	0.03270105421219511
Шифртекст з len(key) = 13	0.0335908366064171
Шифртекст з len(key) = 14	0.0328350800121616
Шифртекст з len(key) = 15	0.03251738922705584
Шифртекст з len(key) = 16	0.032805296501057936
Шифртекст з len(key) = 17	0.03269609029367783
Шифртекст з len(key) = 18	0.0318298865124129
Шифртекст з len(key) = 19	0.0336863920378747
Шифртекст з len(key) = 20	0.03257199233074589



Знаходжу довжину ключа за допомогою індексу відповідності використовуючи перший алгоритм.

Отримані значення індексу відповідності:

Довжина ключа	*Індекс відповідності*
2	0.032877738665435585
3	0.035511015195058095
4	0.03285068688745027
5	0.03894136808973479
6	0.03554174900395774
7	0.03281305025083284
8	0.03286395324059388
9	0.035533119890661796
10	0.03906223063788319
11	0.03287539910336675
12	0.03551094923059566
13	0.03275253869807873
14	0.0327271625482461
15	0.05412912668726622
16	0.03278219191290689
17	0.03283481506840726
18	0.03556826032151608
19	0.03257691246313836
20	0.03903893597260114
21	0.035222889283870754
22	0.032971869516499594
23	0.03296989737402624
24	0.035405713400276366
25	0.03893424049105661
26	0.03284691571712534
27	0.03527554990465837
28	0.032547490332057595
29	0.032536848966869245
30	0.05412601669569691



Довжина ключа – 15. Знаходжу сам ключ за формулою:

$$k = (y^* - x^*) \bmod m$$

Де y^* – буква, що частіше за всіх зустрічається у фрагменті Y_i, x – найімовірніша буква у мові (для російської – ‘о’), m – кількість букв у алфавіті.

Після знаходження ключа за допомогою ‘о’ було отримано ключ ‘крадущяйгявтени’

Можна здогадатися, що правильним ключем буде ‘**крадущийсявтени**’

Частина розшифрованого тексту:

тихотактихочтослышнокакмотыькицепляютсяхрупкимикрылышкамизаночнуюпрохладу
пораужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомосто
рожничаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестеныздания п
огруженноговтеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияживувн
ейтолькоонавсегдаготовапринятьменяспастиотстрелзлобносверкающихвлуннойночи
клинковилиоткровожадныхзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабра
тфоркогдахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмыаоттьмы
недалекоидоненазываемогочушьненазываемыйитьмаабсолютноразныевещиэтовсеравн
очтосравниватьограивеликанатеньэтожизньтеньэтосвободатеньэтоденьгитеньэтов
ластьтеньэторепутацияужгарреттеньзнаетобэтомнепонаслышкетеньпоявляетсятоль
котогдакогдасуществуетхотябыкрупицасветатакчтосравниватьеестьмойпоменьшейм
ереглупономоемустаромуучителюяестественноэтонеговорюяйцакурицунеучатнаузко
йночнойулочкескаменнымидомамизаставшимитихиевременанераздавалосьнизвукалиш
ьпоскрипывалажестянаявывесканадлавкойбулочникаотгуляющегопокрышамгородасла
боговетеркамедленныйсерожелтыйночнойтуманкоторымславиласьнашастолицаговоря
тфокускакоготомаганедоучкипрошлогооткоторогонемогутизбавитьсяипоныневсеарх

имагикоролевствазастилалмощенныюгрубымкамнемиизбитуютелегамимостовуютихоти
хословно

Висновок:

Під час виконання комп’ютерного практикуму, я навчилась розділяти текст на блоки потрібної довжини для подальшої роботи з ними, обраховувати індекс відповідності для тексту, і в залежності від отриманих результатів, визначати довжину ключа. Отримала практичні навички розшифрування та зашифрування тексту шифром Віженера.