НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

Криптографія

Лабораторна робота №2

Підготував: Літвінчук В.С. ФБ-81
Перевірив: Чорний О.М.

Київ 2020

Мета роботи

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

Завдання до виконання

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).

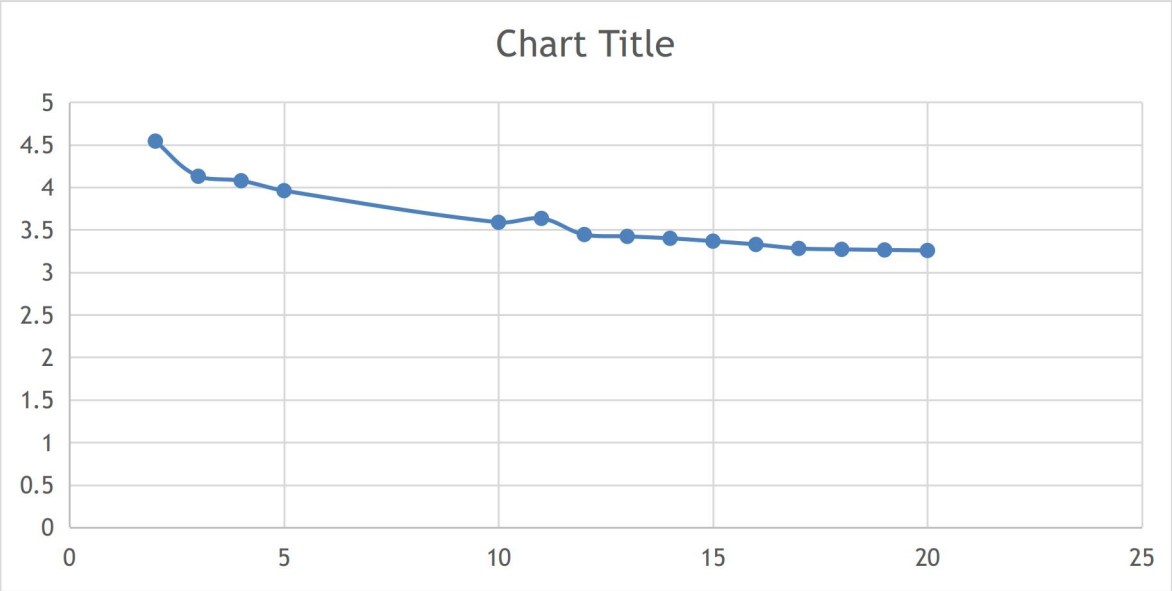
Індивідуальній варіант - 11

Хід роботи

1 та 2 завдання:

Довжина	Значення	Індекс відповідності ШТ
2	аб	0.04543211604160078
3	абв	0.04129974357115188
4	абвг	0.04077272289969708
5	абвгд	0.03960865047441735
10	абвгдежзик	0.035883110877757446
11	абвгдежзикл	0.036343830768809746
12	абвгдежзиклм	0.03444678205635679
13	абвгдежзиклмо	0.03422671989161656
14	абвгдежзиклмоп	0.0340032721551111
15	абвгдежзиклмопр	0.03366697202643116
16	абвгдежзиклмопрс	0.03327819553539009
17	абвгдежзиклмопрст	0.0328121151557095
18	абвгдежзиклмопрсту	0.03270095554941764
19	абвгдежзиклмопрстуи	0.03263352624509339
20	абвгдежзиклмопрстуин	0.03257032890547568

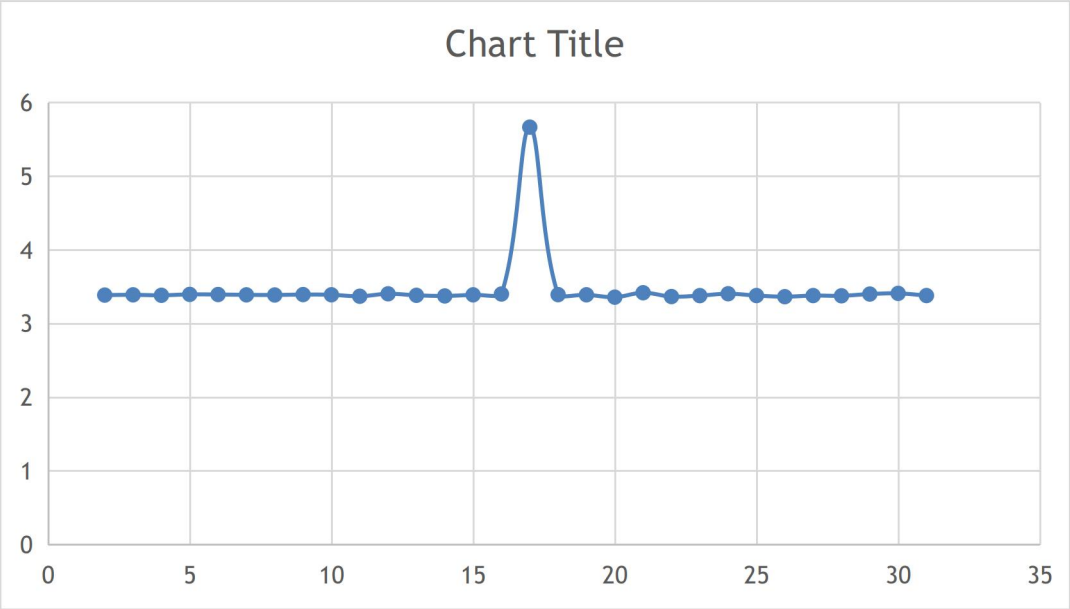
ВТ = 0.05539331456786139



(При побудові графіку значення індексів відповідності брались у 10^-2)

3 завдання:

Довжина ключа	Середнє значення індексу відповідності
2	0.03385469736120976
3	0.0338903572127828
4	0.03382856631255099
5	0.0339485646135541
6	0.03393201950461585
7	0.033887879672849
8	0.03387028521782783
9	0.033925669332816634
10	0.033896990798633383
11	0.03369705663706743
12	0.03402936176339339
13	0.03382497157080262
14	0.03374056874966326
15	0.03389000107283445
16	0.0340028030190302
17	**0.056652871546688466**
18	0.033914675695348
19	0.03389515679639485
20	0.033573302104999446
21	0.034174812268371026
22	0.03365396493285553
23	0.033783217934845344
24	0.03403767616107533
25	0.033792784827267594
26	0.03363761881728569
27	0.033791041307072986
28	0.03375970008060538
29	0.03399770139487165
30	0.03408868605919016
31	0.03379225398070093



З даний індексів бачимо, що найбільш іймовірна довжина ключа - 17,

Далі в ході виконання програми отримали наступний ключ:
”венецианскийкужьц”

Проте, розшифровай текст не у всіх місцях був коректний:
Антонионезнаюо**ыа**егоятакпечаленмцоэтовтягостьва.....

Причина цьому - у 15 і 16 блоках ВТ літера “о” не є найчастішою.

Літери з найбільшою частотою для 15 блоку ВТ:
'a': 0.09399477806788512
'o': 0.08877284595300261

Літери з найбільшою частотою для 16 блоку ВТ:
'e': 0.09921671018276762
'o': 0.09921671018276762

Не складно здогадатись що літери “жь” потрібно замінити на “пе”
Отримуємо наступний ключ - “венецианскийкупец”

З цим ключем, розшифрований текст має коректний вигляд:

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелильдобылчтосостављетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносаларионовыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканых...
(весь ВТ знаходить у файлі OT.txt)

Висновки: в результаті виконання лабораторної роботи я засвоїв методи частотного криптоаназілу. За допомогою обчислення індексів відповідності знайшов довжину ключа. Далі вважаючи що літера з найбільшою частотою - “о”, знайшов ключ та розшифрував повідомлення.