Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

з предмету «Криптографія»

«Криптоаналіз шифру Віженера»

Виконав:
Студент 3 курсу,
ФТІ, групи ФБ-05
Савченко Ярослав

Київ - 2022

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).

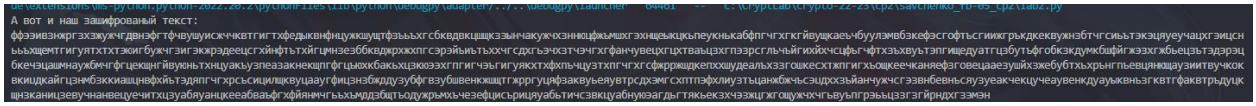
Варіант №9

Хід роботи

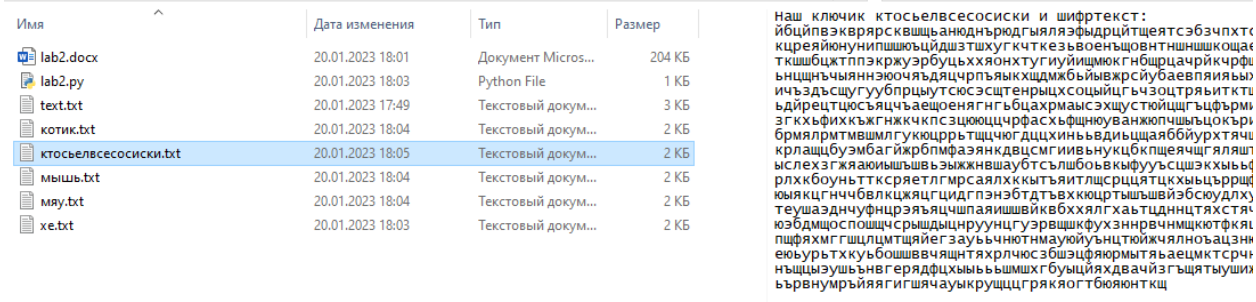
Оберемо фрагмент з тексту на 2кб, що використовували в першій лабораторній.

Напишемо код, що буде шифрувати наш текст. Візьмемо декілька рядків з коду першої лабораторної роботи для роботи з файлами.

Для зручності зробимо так, щоб ми могли вказувати ключ зашифрування безпосередньо перед зашифруванням прямо в консолі.

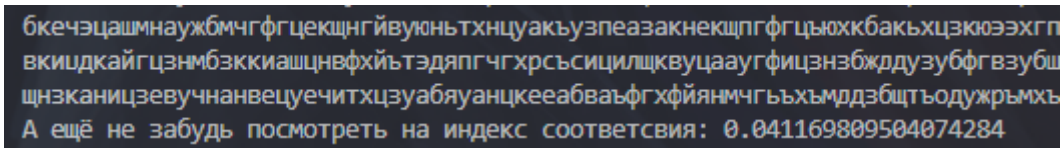


Чудово, все працює. Зробимо це для всіх наших ключів



Також зробив запис зашифрованого тексту у файл з назвою ключа для зручності :3

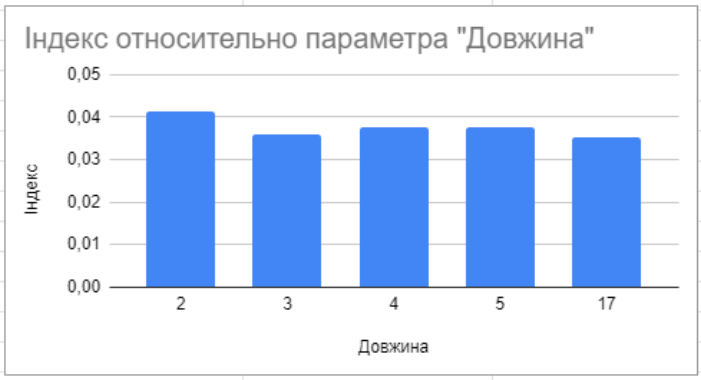
Тепер для наступної задачі додамо функцію для знаходження індексу відповідності. Його також запишемо в файл



Чудово :3

Порахували для кожного і побудували діаграму

Довжина	Індекс
2	0,0411698095
3	0,03594325938
4	0,03754450522
5	0,03750054945
17	0,03530694731

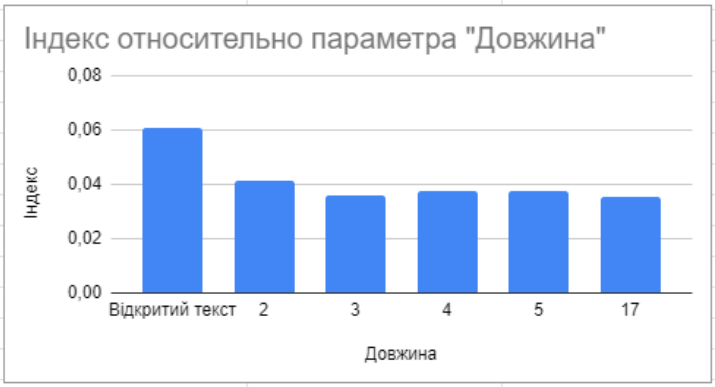


Зовсім трохи, але можемо побачити що індекс зменшується з довжиною ключа. Якби ми взяли більше ключів, то побачили б спадний графік ще краще.

А також я пропустив прорахування для відкритого тексту, але швидко це виправив

```
А ещё не забудь посмотреть на индекс соответсвия: 0.04116980950
А тут я видимо проспал что нужно сделать: 0.06062802279022374
PS C:\CryptLab\crypto-22-23\cp2\savchenko_fb-05_cp2>
```

Довжина	Індекс
Відкритий текст	0,06062802279
2	0,0411698095
3	0,03594325938
4	0,03754450522
5	0,03750054945
17	0,03530694731



Перейдемо до найцікавішого. Розшифрування тексту за варіантом.

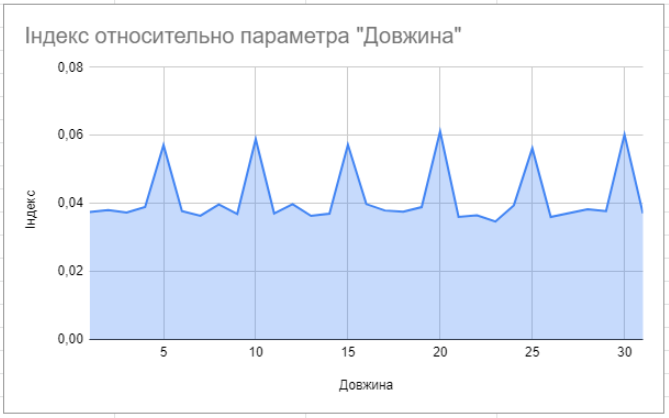
Збережу текст свого варіанту в файл, та створю окремий python файл для цього завдання.

Спочатку напишу функцію що порахує індекс відповідності для всіх можливих довжин ключа до 32

```
0.037500549447099234
Results: {1: 0.037500549447099234, 2: 0.038008314056790365, 3: 0.03730061349693251, 4: 0.038916596794556724, 5: 0.057128399337530424, 6: 0.03771870029538741, 7: 0.036386578403647986, 8: 0.039684539407377546, 9: 0.03689484067126564, 10: 0.05891366856020759, 11: 0.03706386893840664, 12: 0.03979913178761418, 13: 0.03634679213626582, 14: 0.036986098787341014, 15: 0.05725718725718727, 16: 0.039788251366120214, 17: 0.03791807103966814, 18: 0.037571381177251194, 19: 0.03889973803286497, 20: 0.06115664350846721, 21: 0.036020929082908736, 22: 0.03651205501099793, 23: 0.03466470313988132, 24: 0.03945174067125287, 25: 0.05617543859649123, 26: 0.03598740440845704, 27: 0.037133959356181 57, 28: 0.038268034486521885, 29: 0.03774432970680435, 30: 0.06021912675138483, 31: 0.037075095386749 92}
PS C:\CryptLab\crypto-22-23\cp2\savchenko_fb-05_cp2>
```

Тут ми бачимо що індекс досягає найбільшого значення кожні 5 довжин. Для зручності перенесу дані в таблицю і покажу графік

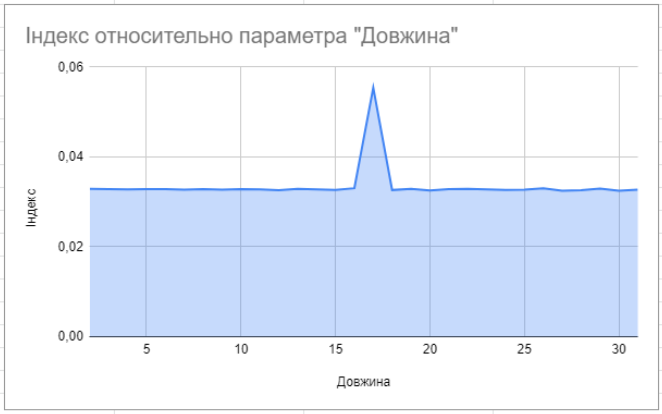
6	0,0377187003
7	0,0363865784
8	0,03968453941
9	0,03689484067
10	0,05891366856
11	0,03706386894
12	0,03979913179
13	0,03634679214
14	0,03698609879
15	0,05725718726
16	0,03978825137
17	0,03791807104
18	0,03757138118
19	0,03889973803
20	0,06115664351
21	0,03602092908
22	0,03651205501
23	0,03466470314
24	0,03945174067



Тепер знаючи довжину ключа знайдемо його. Для цього створимо нову функцію що за довжиною ключа та даними з першої лабораторної роботи видасть результати

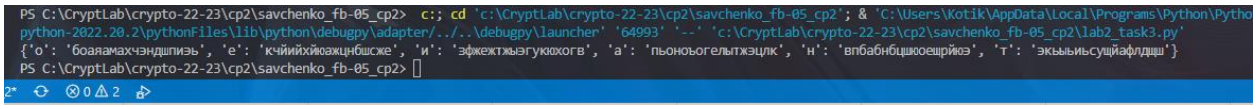
На цьому моменті я отримав бурю емоцій адже зрозумів що весь цей час намагався знайти ключ довжини 5... Але ця довжина ключа була знайдена для одного з моїх файлів. Витративши більше 6 годин щоб це зрозуміти я врешті решт виконав частотний аналіз для потрібного шифтексту (нарешті) і отримав результат з яким працював далі

7	0,03272796105
8	0,0328344001
9	0,03269883174
10	0,03285327345
11	0,03276673214
12	0,03261653075
13	0,03287678682
14	0,03278042052
15	0,03262709665
16	0,03304101176
17	0,05539037433
18	0,03262856071
19	0,03288426956
20	0,03255886369
21	0,03281434393
22	0,03286955317
23	0,03278321294
24	0,03263777421
25	0,03271734599
26	0,03302848405



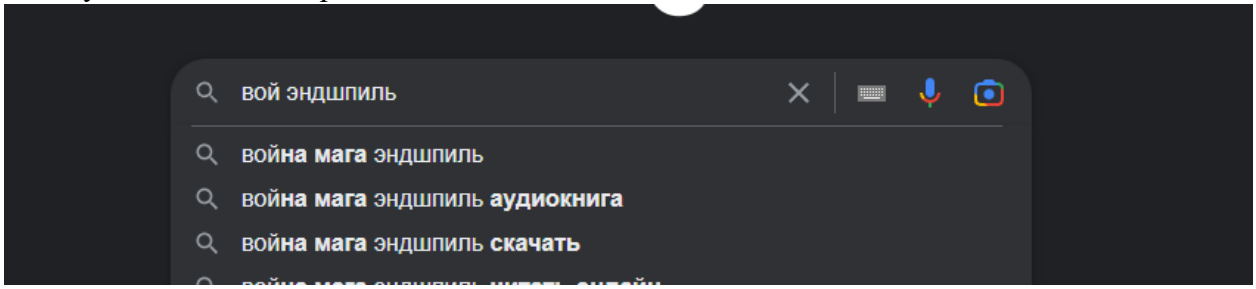
Тож довжина зашифрованого тексту – 17

Напишемо функцію для знаходження можливого схожого ключа користуючись методом з методички і знайдемо результат

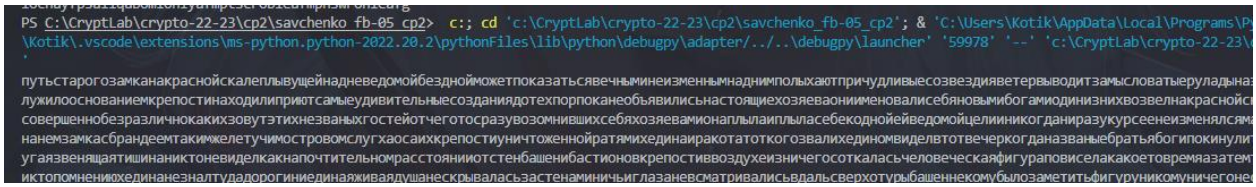


Ммда... Не густо. Але в очі кинулося можливе слово “эншпиль”. Почав копати під нього)

Взявши можливі слова та просто перші можливі букви та повводивши все в гуглі наткнувся на такий запрос



Роман письменника Ніка Перумова. Використаємо його як ключ для розшифровки. Допишемо функцію розшифрування і отримаємо початковий текст



“Путь старого замка на красной скале плывущей над неведомой бездной может...”

Висновок: на цій лабораторній роботі я навчився навичкам частотного криптоаналізу. Принципам шифрування, методам знаходження довжини ключа та значення самого ключа. А також навчився бути уважнішим до свого ж коду, в якому встиг не раз запутатися через один єдиний параметр :)