Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Варіант №2

Виконав: ФБ-11 Тимощук Ілья

Київ – 2023

Мета роботи

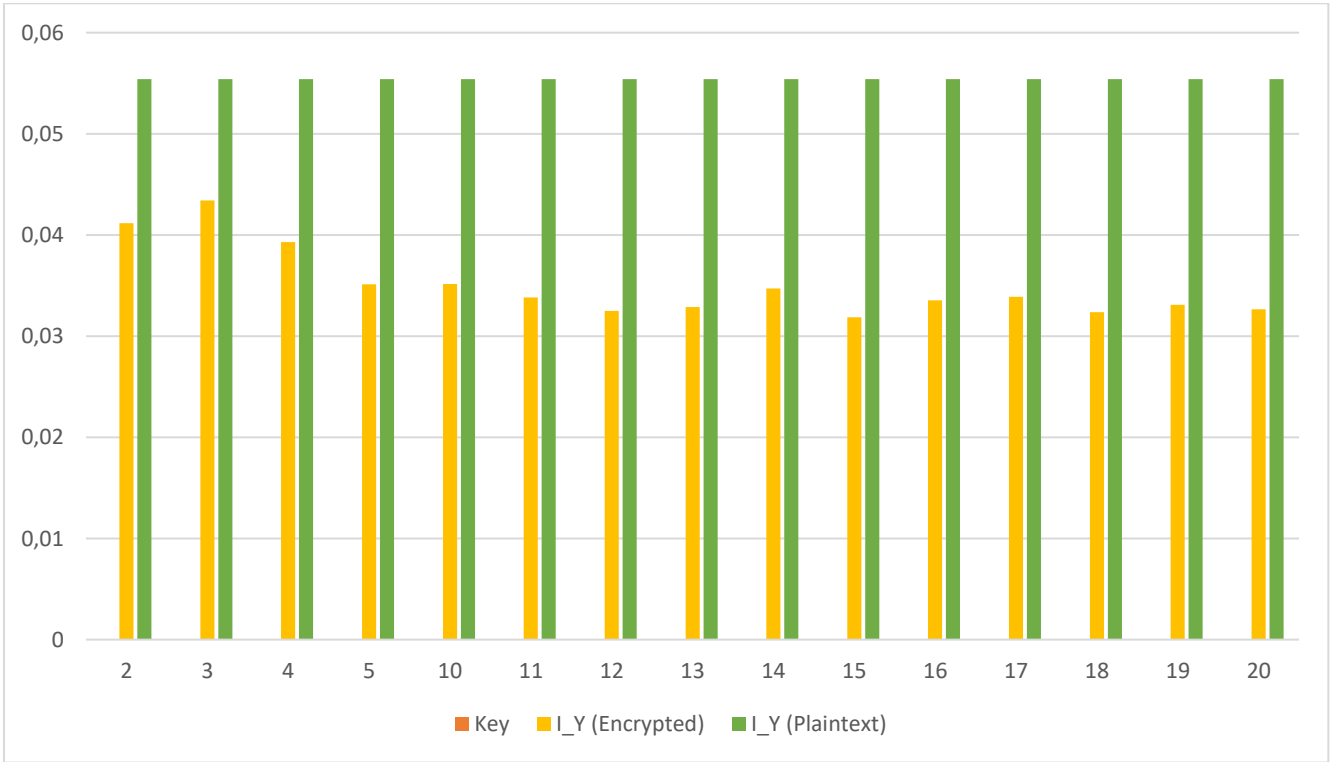
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Хід роботи

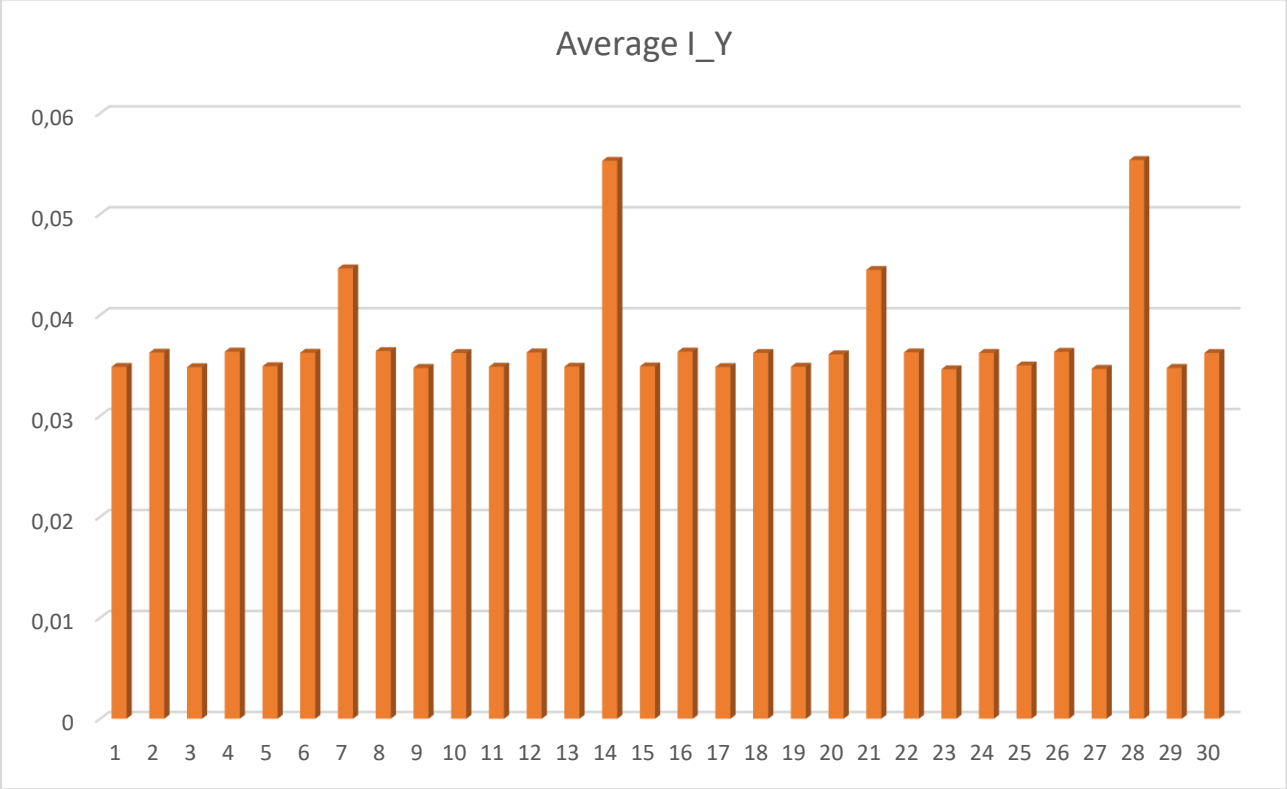
Відредагований мій відкритий текст (my_text.txt) було відредаговано та записано в файл text_edited.txt, з яким і проводяться наступні виміри.

Обчислені значення індексів відповідності для вказаних значень r (дана таблиця збережена в **vigenere_matching_indices.xlsx**):

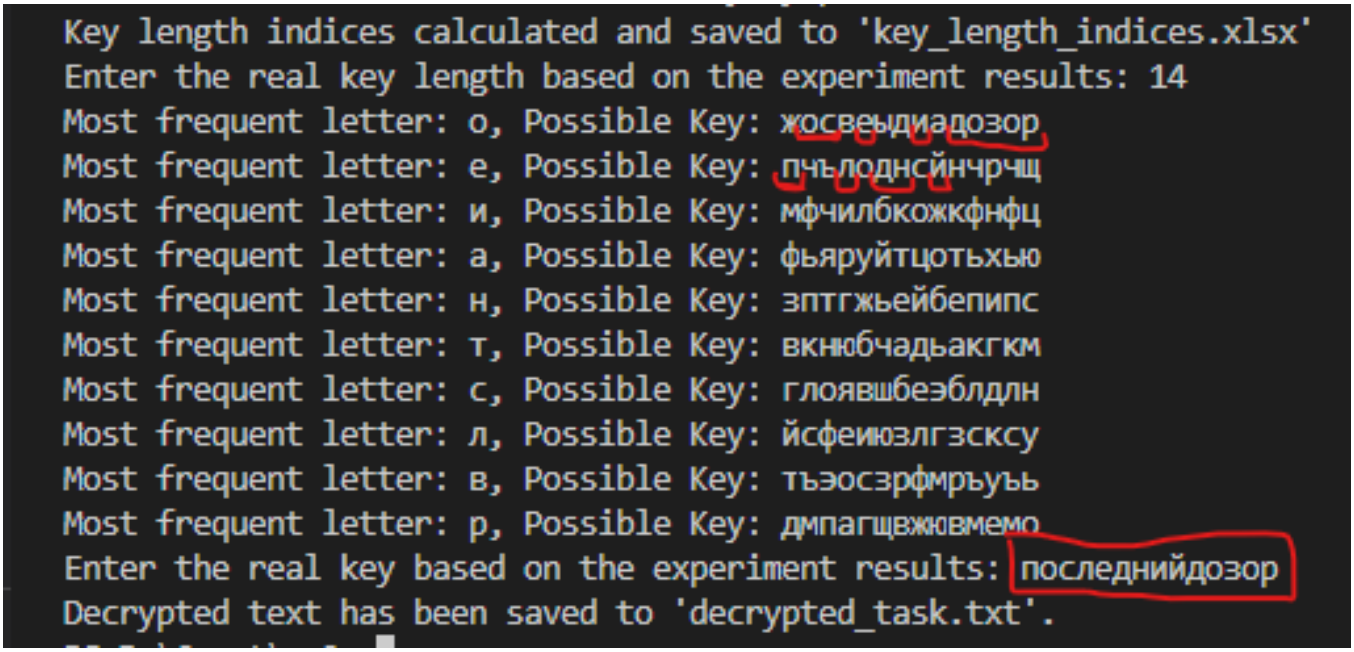
Key Length	Key	I_Y (Encrypted)	I_Y (Plaintext)
2	ау	0,041165	0,055418
3	юхы	0,043422	0,055418
4	ющчч	0,039288	0,055418
5	еянйэ	0,035113	0,055418
10	ияъюгкышыь	0,035153	0,055418
11	ъдкьпмзпгзе	0,033826	0,055418
12	охосэзшкфйхн	0,0325	0,055418
13	гйырчтсбрссец	0,032878	0,055418
14	чнртпкчтохмжнъ	0,034709	0,055418
15	ыжржтчсылйвщапс	0,031857	0,055418
16	щзтфщохбвбфьопсй	0,03354	0,055418
17	свяувэвбэкхпаэмпз	0,033878	0,055418
18	жисюжуфхжмолъпомгд	0,032365	0,055418
19	тсьяиьшсйущсяхбмтац	0,033089	0,055418
20	ддспмйзлъщешнкмаьйфж	0,032637	0,055418



Набори значень індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера для **зашифрованого тексту** (таблиця цих значень збережена в **key_length_indices.xlsx**):




```
Matching indices calculated and saved to 'vigenere_matching_indices.xlsx'
Довжина ключа: 1  Значення ключа:  е  Середнє значення індексу відповідності:  0.034857801467683
Довжина ключа: 2  Значення ключа:  юв  Середнє значення індексу відповідності:  0.036268205482179
Довжина ключа: 3  Значення ключа:  ьты  Середнє значення індексу відповідності:  0.034827681829885
Довжина ключа: 4  Значення ключа:  охяя  Середнє значення індексу відповідності:  0.036368140634726
Довжина ключа: 5  Значення ключа:  аянтр  Середнє значення індексу відповідності:  0.034922938298912
Довжина ключа: 6  Значення ключа:  жкшчвб  Середнє значення індексу відповідності:  0.03625749982569
Довжина ключа: 7  Значення ключа:  кубюьжс  Середнє значення індексу відповідності:  0.044625980002924
Довжина ключа: 8  Значення ключа:  бмджнхкб  Середнє значення індексу відповідності:  0.036422614360369
Довжина ключа: 9  Значення ключа:  щтбьейаы  Середнє значення індексу відповідності:  0.034758231846951
Довжина ключа: 10  Значення ключа:  юмгяцспбдч  Середнє значення індексу відповідності:  0.03622973929008
Довжина ключа: 11  Значення ключа:  цпййсбхбфча  Середнє значення індексу відповідності:  0.034872670996714
Довжина ключа: 12  Значення ключа:  нюярвпиьзуэх  Середнє значення індексу відповідності:  0.036286975422561
Довжина ключа: 13  Значення ключа:  жмелидкцблдфд  Середнє значення індексу відповідності:  0.034880863375454
Довжина ключа: 14  Значення ключа:  ичучхдгеуючльв  Середнє значення індексу відповідності:  0.05528168514214
Довжина ключа: 15  Значення ключа:  хйимценнбдгцфыц  Середнє значення індексу відповідності:  0.034905048211263
Довжина ключа: 16  Значення ключа:  юцьжгчйбтркщдку  Середнє значення індексу відповідності:  0.03636959762262
Довжина ключа: 17  Значення ключа:  внжячьнригфггрызв  Середнє значення індексу відповідності:  0.034842144619378
Довжина ключа: 18  Значення ключа:  енпучфджчсзькуцяюч  Середнє значення індексу відповідності:  0.03623606945108
Довжина ключа: 19  Значення ключа:  ухтыпйэпычдылтщщиьэ  Середнє значення індексу відповідності:  0.034872246708387
Довжина ключа: 20  Значення ключа:  угсыйвюуашджалэбьичю  Середнє значення індексу відповідності:  0.036100466411422
Довжина ключа: 21  Значення ключа:  зоъьыюзухиуоабтццэибй  Середнє значення індексу відповідності:  0.044469842267784
Довжина ключа: 22  Значення ключа:  щнэнсенцяжыятсюнйтвоюв  Середнє значення індексу відповідності:  0.036291615578824
Довжина ключа: 23  Значення ключа:  ктлаеибуывкгкуэтыашакиь  Середнє значення індексу відповідності:  0.034620481881822
Довжина ключа: 24  Значення ключа:  явяицхбдтцяваххзквичепжш  Середнє значення індексу відповідності:  0.036241608017956
Довжина ключа: 25  Значення ключа:  оирхмьпмищьехынцфгксыеогх  Середнє значення індексу відповідності:  0.034999922078327
Довжина ключа: 26  Значення ключа:  лвщаьчдаепыхйеьегххфцьфмэф  Середнє значення індексу відповідності:  0.036350457674377
Довжина ключа: 27  Значення ключа:  фгьпнхрвййюссбанймшвъффйашз  Середнє значення індексу відповідності:  0.034663226443448
Довжина ключа: 28  Значення ключа:  йгэлпжмырфьщгплохомяушнсчем  Середнє значення індексу відповідності:  0.055360826912551
Довжина ключа: 29  Значення ключа:  бщякфпсежгьзхддопфвящбятгсьмп  Середнє значення індексу відповідності:  0.034753828308246
Довжина ключа: 30  Значення ключа:  уянуцроиеогэюхлэщыхяххъйловом  Середнє значення індексу відповідності:  0.036235602788643
Key length indices calculated and saved to 'key_length_indices.xlsx'
Enter the real key length based on the experiment results: 14
```



Частина розшифрованого тексту(повний текст збережен в decrypted_task.txt):

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайней серойравнинывзгляднефиксироваляркихкрасоквцелойкартиненостоиловсмотретьсявотдельну юпесчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюнадголовойзастылобелоесрозов ымбудтомолочнуюрекуперемешалискисельнымиберегамидаивыплеснуливнебесааещедулвет ерибылохолодномневсегдахолодноначетвертомслоесумраканоэтоиндивидуальнаяреакциягес ерунапротивбыложарколицораскраснелосьполбустекаликапелькипотамненехватаетсилысказ алялицогесерасовсемпобагровелоответнеправильныйтывысшиймагтакполучилосьслучайнон отывысшийпочемувысшихмаговтакженазываютмагамивнекатегорийпотомучторазницавсиле междуниминастольконезначительначтонеможетбытьисчисленаиневозможноопределитьктоси льнееактослабеепробормоталяборисигнатьевичяпонимаюномненехватаетсилыянемогупройт инапятыйслойгесерпосмотрелсебеподногиподделноскомботинкапесокподбросилввоздухшаг нулвпередиисчезэточтосоветяподбросилпередсобойпесокшагнулвпередтщетнопытаясьпойма тьсвоютеньтенинебылоничегонеизменилосьяпопрежнемуоставалсянач

Труднощі, які виникли під час виконаня роботи

Під час виконання даної лабароторної роботи труднощів особливо не виникало, хібащо довго не міг зрозуміти який саме ключ мав бути, допоки не не придивився до результатів уважніше.

Висновок: в цій лабараторній роботі було засвоєно поняття індекса відповідності, його знаходження та криптоаналізу текста, зашифрованого шифром Віженера та подібними.