НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Лабораторна робота №2 з дисципліни

”КРИПТОГРАФІЯ”

Підготував:

студент групи ФБ-03

Заболотний Максим

Київ 2022

Тема роботи: Криптоаналіз шифру Віженера

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 шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Для виконання лабораторної роботи було обрано книгу Джейн Остін "Гордість і упередження"

1.

Ключі різної довжини:

```
keys = ['зд', 'здр', 'здра', 'здрав', 'здравствуймир']
```

Зашифровуємо текст:

```
for i in keys:  # шифрування тексту різними ключами
    result = ''
    for j in range(len(open_text)):
        letter = (letters_set.find(open_text[j]) + (letters_set.find(i[j % len(i)]))) % len(letters_set)
        result += letters_set[letter]
    encrypted_texts[i] = result
```

2.

Рахуємо індекси відповідності для відкритого тексту та всіх одержаних шифротекстів:

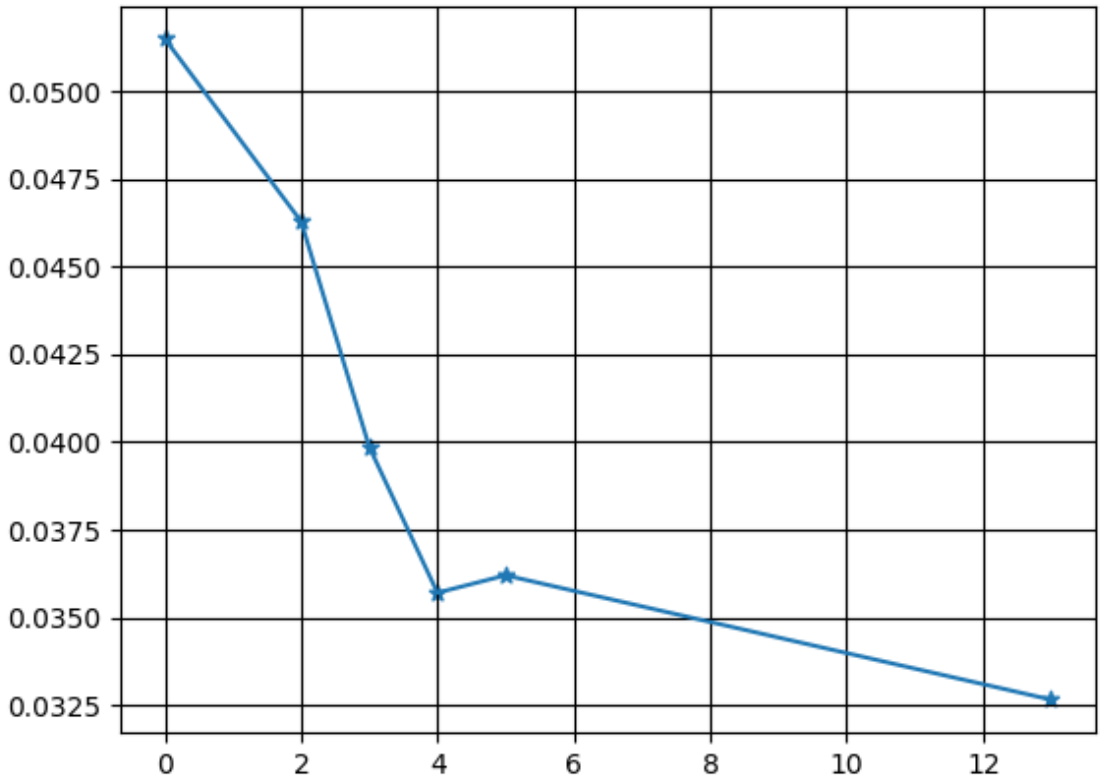
```
Індекс відповідності ВТ: 0.05149540523769878
```

```
[0.046287138895020646, 0.039860555149024875, 0.035703745161464136, 0.03620108378568321, 0.03265667702016296]
```

Порівняємо їх значення:

r	Індекс відповідності
Теоретичне	0.05149540523769878
2	0.046287138895020646
3	0.039860555149024875
4	0.035703745161464136
5	0.03620108378568321
13	0.03265667702016296

З діаграми видно, що зі збільшенням довжини ключа r значення індексу відповідності буде зменшуватись.



3.

Розшифруємо шифртекст згідно номеру варіанту (10 варіант):

Щоб виконати це завдання було обрано перший варіант розв’язання.
Запускаємо цикл, в якому розбиваємо текст на блоки, враховуючи усі можливі значення r на проміжку 2-30. Рахуємо середнє значення індексу відповідності, порівнюємо його з теоретичним значенням і знаходимо довжину ключа для зашифрованого тексту.

```
Довжина нашого ключа: 15
```

```
Ключ: "крадущийсявтени"
```

Розшифрований текст 10 варіанту:

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладупораужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомосторожничаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестеныздания погруженноговтеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегдаготовапринятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиоткровожадныхзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабратфорког

дахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмыаоттьмынедалекои
доненазываемогочушьненазываемыйитьмаабсолютноразныевещиэтовсеравночтосравн
иватьограивеликанатеньэтожизньтеньэтосвободатеньэтоденьгитеньэтовластьтеньэтореп
утацияужгарреттеньзнаетобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществ
уетхотябыкрупицасветатакчтосравниватьеестьмойпоменьшеймереглупономоемустаром
уучителюяестественноэтонеговорюяйцакурицунеучатнаузкойночнойулочкескаменным
идомамизаставшимитихиевременанераздавалосьнизвукалишьпоскрипывалажестянаяв
ывесканадлавкойбулочникаотгуляющегопокрышамгородаслабоговетеркамедленныйсер
ожелтыйночнойтуманкоторымславиласьнашастолицаговорятфокускакоготомаганедоучк
ипрошлогооткоторогонемогутизбавитьсяипонынеевсеархимагикоролевствазастилалмощ
еннуюгрубымкамнемиизбитуютелегамимостовуютихотихословновсклепебогатеяпослет
огокакегонавестиластаямелкихгородскихворишекскрипитвывескагуляетветерокмедлен
ноиленивоплывутоблакапоночномунебуноявсеещестоюслившисьстеньюзданияистараяс
ьнешевелитьсяинтуицияимойжитейскийопытзаставляютвслушиватьсявтишинуночного
городаниоднадажепустыннаяулицанеможетбытьтакойтихойособенноэтагдеживуттолько
однилавочникивночидолжныбытьзвукикрысышуршащиевмусорехрапящийтутжепьяни
цакоторогоужеуспелипочиститькарманникипреждечемзабитьсявкакуюнибудьщельнано
чьхрапизоконседыхдомовкрадущаясявотьмегрязнаясобакатяжелоедыханиеновичкаразб
ойникавожиданиисвоейжертвызастывшеговомглезажатымвпотнойладониножомшумвл
авкахимастерскихдажепоночамвнекоторыхизнихкипеларабо таничегоэтогонебылонатем
нойузкойулочкеукутаннойвперинутумананичегокрометишиныимракаветероксильнеезаг
улялвкрышахстарыхзданийитяжелыесерыеоблакапонеслись понебусловностадобольши
хпушистыховецобнажаянебесныйкуполбеспечныйгулякаветерласковотрепалволосыноя
несмелнакинутьдажекапюшонсаготчтожеэтокакбыотвечаянамоюмолитвуславныйбогвс
ехворовдалушамбольшечуткостишагитороплivыешагичеловекакоторыенесмогприглуш
итьдажетуманрасползающийсясерожелтойнакипьюнадкаменноймостовойвсоседнейвые
мкерасполагающейсянастенезданиянапротивязаметилмимолетноеколебаниевотьмектот
опрячетсяявсмотрелсявчернильнуюночьнетпоказалосьслишкомволнуюсьвожиданиинес
уществующихнеприятностейстареюнаверноечьятотребовательнаярукаудержаламеняна
местекакбыговорястойобождиещеневремяхсанкорменясожричтожепроисходитнатихойт
емнойулочкеремесленниковчеловекпоказалсяиззаповоротаулицыибыстрымшагомперех
одящимвбегнаправилсявмоюсторонудуракилихрабрецеслиодиншастаетвтемнотескорее
всегопервоехрабрецыдолгонеживутвнашеммирехотядуракитожееслионинешутынашего
славногокоролякакоенеотложноеделозаставиловыйтиегонаночнуюулицугдедажемаслян
ыефонаринегорелипопробуйтенайтифонарщикакоторыйвысунетвэтовремяносвкромеш
нуютьмуэтоведьнетихиевременакогдаребенокспокойномогпройтивсамуюглухуюночьиз
одногоконцаавендумавдругойиснимничегобынеслучилосьчеловекприближалсявысокий
хорошоможносказатьбогатоодетыйрукалежитнарукоятиприличногомечаслужитважной
шишкенаверноеоблакаснованаползлинанебозакрывсвоимтеломвыступившиенанебезвез
дыикполнойтьмедобавиласьтьмакромешнаяяуженесмогразглядетьлицаспешащегочелов
екаонпоравнялсясомнойидаженезаметилтихостоящуювтенитеньеслибыязахотелипротя
нулрукутоснялбыунегоспоясапузатыйкошелекноянемелкийкарманникчтобыпадатьтакн
изковременамолодостидавнокануливлетудаисудьбаподсказывалачтосейчаснестоитнеточ
тодергатьсяадажеглубокодышатьвнишенапротивтьмавновьпришлавхаотическоедвижен

иевскипаяиклубясьчернымцветкомсмертииязамерледенеяотужасаизтьмывырваласьтьма
принявобличьекрылатогосуществадемонасрогатойголовойчерепомнакоторойсиялиалые
узкиеглазаикаклавинасгоркарликовупаланаспешащегочеловекапридавивегосвоимвнуш
ительнымвесомчеловекиздалвопльраненойкошкипопыталсявыхватитьбесполезныймеч
нотьмасмялавсосалапоглотиланочногопутникаисуществокембыононибыловзмыловноч
ноеоблачноенебоуносяссобойсвежеемясоаможетидушуугольночерныйсилуэтнамигмель
кнулвоблачномночномнебеиисчезястаралсяуспокоитьдыханиетварьнезаметилатогоктов
сеэтовремянаходилсянапротивнееноеслибыяшевельнулсяеслибыяхотьнамигшевельнулс
яилихотябызадышалчутьгромчетоонабыбросиласьнаменяизнишизданиягдеподжидалал
егкуюдобычуповезловочереднойразмнеоченьповезлоудачавораженщинакапризнаявлюб
оймигможетотвернутьсянопокаонасомнойямогузаниматьсясвоимворовскимремесломвт
емномуглусоседнегозданиятихопискнулакрысазанейдругаявнебеохотясьзаприпозднивш
имисяиюньскимимотылькамипролетелалетучаямышьопасностьминоваламожнопродол
жатьпутьяотделилсяотстеныистараясьдержатьсянаиболеетемныхучастковулицыдвинул
сядальшеничтонеговорилооослучившемсянесколькоминутназадулицабыламолчаливыми
единственнымсвидетелемночнойохотыдемонаксчастьюлунынебылопушистыеоблакавн
овьнаползлииспряталиотгородазвездыпоэтомутенибылосколькоугоднобыстрымшагомн
еиздаваясапогаминиединогозвукаяперемещалсяотзданиязданиюизтенивтеньулицапека
рейосталасьпозадиясвернулвпереулокнаправоздесьтуманбылгущеонобволакивалменям
ягкимилапамиглушилшагискрывалотглазлюдейинелюдейвтенипососедствураздалосьшу
шуканьеязамервсматриваясьвсерожелтуюмглуворымолодыещенкикудавамдомастерапо
джидаютночногогулякуилиготовятсяпочиститьспящихгорожанзеленыслишкомшумятсл
ишкомнеопытныворыпрофипереговариваютсяжестаминеиздаютшумадажевтакойночик
огдагустеющийлипкийтумангаситвсезвукияпроскользнулрядомснимиаворишкидаженез
аметилитеньтеньвтенисложноувидетьнеопытномуглазувозниклодурацкоедетскоежелан
иевыскочитьизтуманаигромкосказатьбуимвлицоновполнеможнонарватьсянаслучайный
ножтемболеечтонечегопугатьмолокососовтемныйпереулокончилсяинависшиемрачные
стеныдомоввидавшихвэтоммиреирадостьигоререзкоразошлисьвстороныяпосмотрелнан
ебоветервсетакиразогналленивыеоблакаинебопревратилосьвскатертьнакоторойбогатей
рассыпалмонетысотниитысячизвездмерцалимнеснебаэтойхолоднойлетнейночьюсветло
какднемздесьгорелиодиночныефонарикакникакянаходилсянаоднойизцентральныхплощ
адейгородаифонарщикинесмотрянасвойстрахбылиобязанывыполнятьсвоюработупламя
фонарейзакованноевстеклянныеколпакиразбрасываловокругсебяпятнадрожащегосветаи
хаотичныетенимолчаливоплясалинастенахугрюмыхдомовэтоплохонадеюсьчтопогонщи
кветерсноваприведетсерыхпушистыховецнанебоапокапридетсядержатьсятенижмущейс
якстенамвысокихзданийкотораясталабледнойипугливойотвездесущегосвета

Висновок

У ході виконання даного лабораторного практикуму я підібрав текст для шифрування, ключі різної довжини та зашифрував обраний текст шифром Віженера з цими ключами.

Також я підрахував індекси відповідності для відкритого тексту та всіх одержаних шифротекстів і порівняв їх значення.

Наприкінці, використовуючи наведені теоретичні відомості та текст 10 варіанту, розшифрував наданий шифртекст.

В результаті я засвоїв методи частотного криптоаналізу, а також здобув навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.