Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
студенти групи ФІ-93
Баєвський К.О.
Шифрін Д.С.

Перевірив:
Чорний О.М.

Київ – 2022

ЗМІСТ

ЗАГАЛЬНІ ВІДОМОСТІ

1. Мета комп’ютерного практикуму

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

2. Постановка задачі

Варіант 1.

Створити програму для знаходження ключа шифру Віженера двома способами та дешифрувати текст за варінтом.

3. Хід 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 I_r для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:

– визначити довжину ключа, використовуючи або метод індексів відповідності, абостатистику співпадінь D_r (на вибір);

– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

– визначити символи ключа за допомогою функції $M_i(g)$;

– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

4. Опис труднощів

Реалізовуючи програмний код, ми зіштовхнулися з проблемою, що для кожної формули потрібно знаходити порядковий номер літер текстів, шляхом пошуку букви у алфавіті. В результаті ми вирішили використати конструкцію мови – так зване «перераховування».

Ще одна проблема, з якою ми зіштовхнулися, це сортування частотності букв. В результаті ми сортували за значеннями за допомогою відсортованих словників. Ключі були всі відмінні, якщо це було не так, то при додаванні додавали 10^-15, щоб ключі відрізнялися.

Також проблемою було розбивання текстів на блоки. Але ми вирішили зберігати всі шифроблоки у списку, при першому різкому збільшенню значення індексу збігу.

ПРАКТИЧНА ЧАСТИНА

1. Значення індексів відповідності

0	0.055064274393094116
2	0.045387366331437244
3	0.04280177863804372
4	0.043642093614920316
5	0.03839833328932385
10	0.03412482849095994
11	0.033331143094063
12	0.033784256519185776
13	0.03395051000847234
14	0.033450521369059204
15	0.03321553121183073
16	0.033033106797090296
17	0.03323325782125232
18	0.03337945117516571
19	0.03320660649854226
20	0.033110195031595735

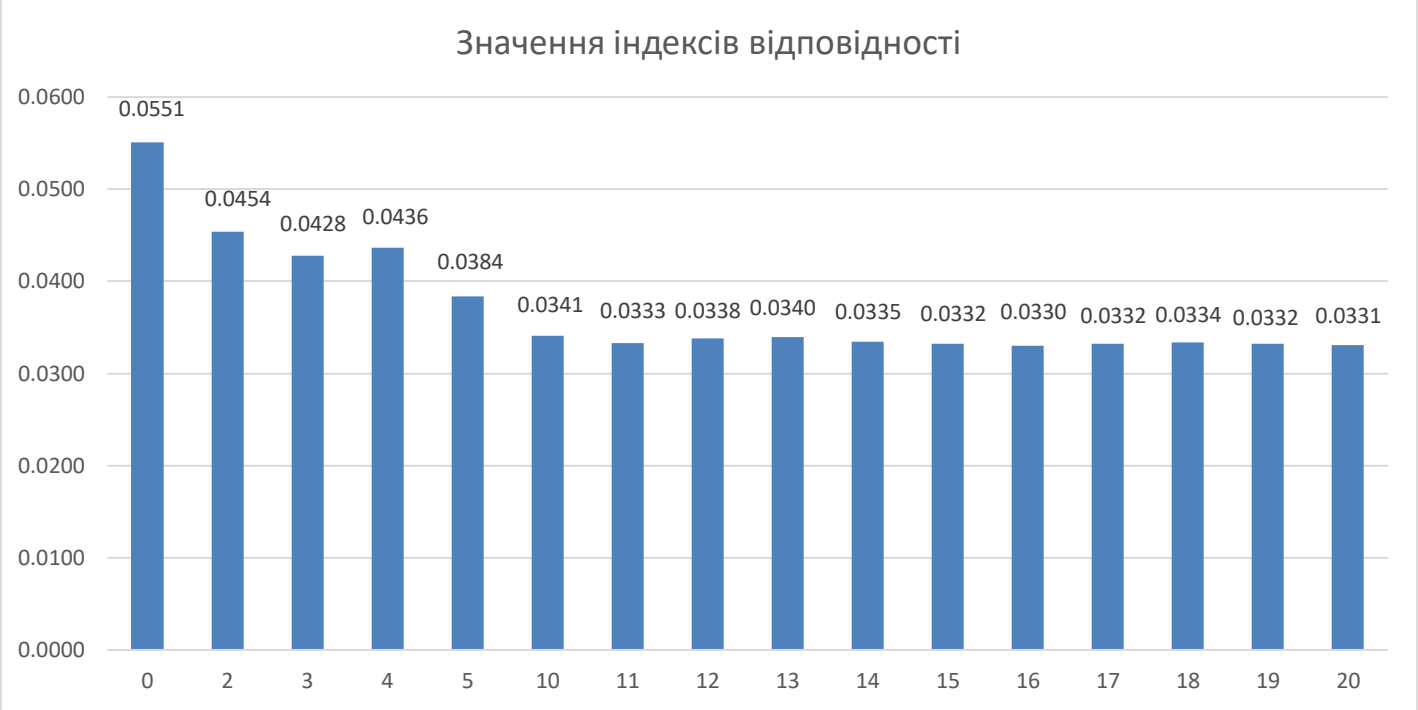

Рис.2.1 – Значення індексів відповідності

2. Встановлення довжини ключа

Рис.2.2 – Значення послідовності D_r

Отже, довжина ключа r = 12.

3. Знаходження ключа шифру Віженера

I. Значення ключа, одержане із використанням функції $M_i(g)$:
Ключ : вшекспиребуря

II. Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови:
Ключ : вшекспиребуря
Більшість літер були співставлені з найчастішою буквою російського алфавіту «о», а інші з другою по частоті – буквою «е».

4. Розшифрування шифртексту

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцыveселейребятаveселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсяmореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявленныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовиселицысделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешеннымыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстеньгуживонижежепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожебросительвсеиззавасиидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакглоткуболтливойбабыбоцмандержикручекветрукручествавыготифокдерживодкрытоеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподняновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеро

йпросперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбу
нтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсяснебосв
одановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпогибавшихразделяя
корабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщепывсердцеумен
язвучитихвопльувыонипогиблибылабыявсесильнымбожествомямореверглабывземныен
едраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипросперо утешьсяпусть
доброетвоенестонетсердцениктонепострадалмирандаужасныйденьпроспероникто непостр
адалявсеустроилзаботясьотебемоедитяодочериединственнойлюбимойведьтынезнаешькто
мыиоткудачтоведомотебечтотвойотецзоветсяпросперо ичтоемупринадлежитубогаяпещер
амирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьно
помогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемирандеутешьсяот
римирандаслезысостраданьястольбедственноекораблекрушеньекотороеоплакиваешьтыяс
илоюискусствасвоегоустроилтакчтовсеостались ьживыдацелывсектоплылнаэтомсуднектоп
огибалвволнахзовянапомощьсихголовыиволоснеупалсадисьислушайвсесейчасузнаешьми
рандавычастособиралисьмнеоткрытьктомыипрерывалисвойрассказсловаминетпостойеще
невремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисп
олнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопреждемиранданетяпомн
юпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятисвоей
появляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэ
льпоетдухигорлесовиводвсевхороводутихломоревлегкойпляскесплескомруксомкнитекру
гмнедружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигауга
уариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэта
музыкаснебесилизем литеперьонаумолклатоверногимныздешнимбожествамясмертьотца
оплакиваягорькосиделнаберегувдругповолнамкомнеподкрались ьсладостныезвукиумеривя
ростьволнискорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьар
иэльпоетотецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкос
тистанутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвонду
хидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоет
сявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпросперомир
андеприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенпр
авдаведьотецпрекрасенонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспит
иестичувствуеткакмыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропав
шихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасив
ыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсто
ронуслучилосьвсекакяпредначерталмойариэльискусныйязаэточередвднятебяосвобожу
фердинандтаквотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомос
тровеживешьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыф
еяилисмертнаямирандасиньорядевушкапростаяянечудофердинандкакмойроднойязыкное
слибябылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшимпросперопервей
шимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругтывспомни
лпронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецк
орольпогибвморскихволнахмирандаувынесчастныйфердинандпогиблиснимивсееговельм
ожипогибмиланскийгерцогвместессыномпросперовсторонумиланскийгерцогсдочерьюсв
оейтебялегкомоглибыопровергнутьещеневремяспервогожевзглядаогоньлюбвизажегсявих
глазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемпозоритесебя
неправдой

ВИСНОВКИ

У даній роботі було обраховано індекси відповідностей для текстів, зашифрованих ключами різних довжин. Також за допомогою послідовності I_r, знайдено довжину ключа. Значення ключа було знайдено двома способами: із використанням функції $M_i(g)$ та шляхом співставлення найчастіших літер блоків найчастішій літері мови. Перший спосіб виявився ефективнішим, бо значення, отримане другим способом, потребувало коригування.