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

Комп’ютерний практикум №2

З дисципліни «Криптографія»

Виконали:
Студенти групи ФБ-33
Рудий А.О., Шкуропінський М.М.

Київ – 2025

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:

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).

Хід роботи:

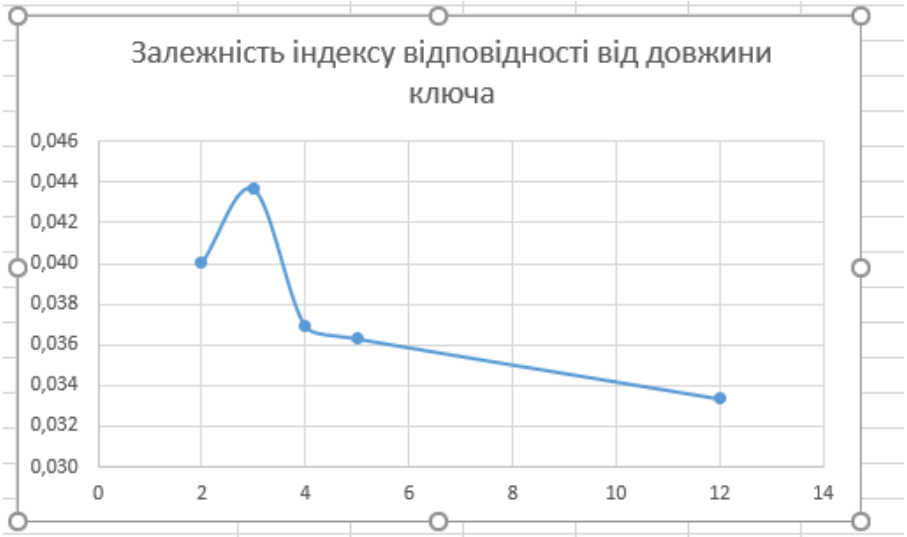
1. Для шифрування було обрано фрагмент з тексту попередньої роботи (Гоголя)
   Текст було зашифровано з ключами 2: «ум», 3: «век», 4: «глаз», 5: «земля», 12: «криптография».
   2:
   бюшвхмдфюфьмзмамдишоыгфзююхъггшээъьчыгаъдюпкбщвфдмюэефифыц
   жыюсездъкфалюыпсдзыэушжгуэеобоучхфиыбэемаъхцшочъямлщшшесуюгс
   въясмфэмчюгъмфаээъцъхыбэюсчэеоыфзьууофъйефиыпсдыыэуюшчпщыцбч
   ухцъцъюиыэвъюиъъхмюоэмксдюхсрыыпгмзъхцдъгъкфаээъьлгшуьэсыцямьэ
   …
   3:
   рчпшзкунхкокцечвцжззтщженчмрхбзцфрохкьчрцьюгшпфтуехучтчнтмшщнк
   ьэцшщнчбрщюкыэнывсэщеыфзшдехднясуыфечрзфззорскътпочпвчьзфшокгк
   пкжчърютпцфришдфшурпжцьднтцхкйатйвькъщюкыснывчпнбчкпшнеуеунрр
   жкцщрржйумврммебзцьдкзснntеюрзфууърьтпцфройтсктппкпцвоымуупубку
   …
   4:
   сэеэелспоуйзчлнзфзейлвбвоэвхувешнщйтлвнхфэьесшппфллшхухплхуцортв
   фщчпрклцярсвльауцвашхнойгцвпшъошхлнхехейзщмзышеухращурпхпрщпн
   лдщущщпрькхжщвцсьлмзьтйлуфчгтыпкитпшъьмфъишгэетяшиссцаржщгхоз
   иштщлгкщвзонкзърсщерэцлорзчщвсфщрхъуншнщйжучачнрисплйшнщйфсв
   …
   5:
   хчсббзцфцзреалмзцирбпьнжкщзъыцмццщитнгшншчийнфффьятцюуфпнцюот
   кюжрхьфшютфиррвнэллъьмьсйуолкйнбъншчмшнйпснгхсмгммсюрящхсънук
   еуйзйюынанщьйхиъноxцчргшчоузыхмтъпмйэзьфиррцнэлсмришзсучликупщ

кгнэънтбущбзрохяюкээбмвыувчеащбсцъынюнщьйхолылзхцрзссмфрсухшню
…
12:
Швнефофшльсяюрхпгкитилйъхвкэвеибквсктзхэгаяообчзыруадцшшиюыоххъ
кгъъшнууожхщкъягьулирьтцстщешхгцрьрхэфшитдвфявэныдугврщчнцхбчьо
зврвбзчбтэхьеяоеудобъсъцчааыгзснъчзэяхсгррквнъоылъояиинюлээклбпвуыс
юкпэрнрчщщсмхеюъсурфвкйыюшэйцрбквсюъьияьулъмфсрфюсьаелюньйъх
…

2. Індекс відповідності для відкритого тексту: 0.05608186892575381

key	Index
2	0,0400136060050287
3	0,0436525994670981
4	0,0369231429258733
5	0,0363056631931516
12	0,0333592276447055

Графік залежності

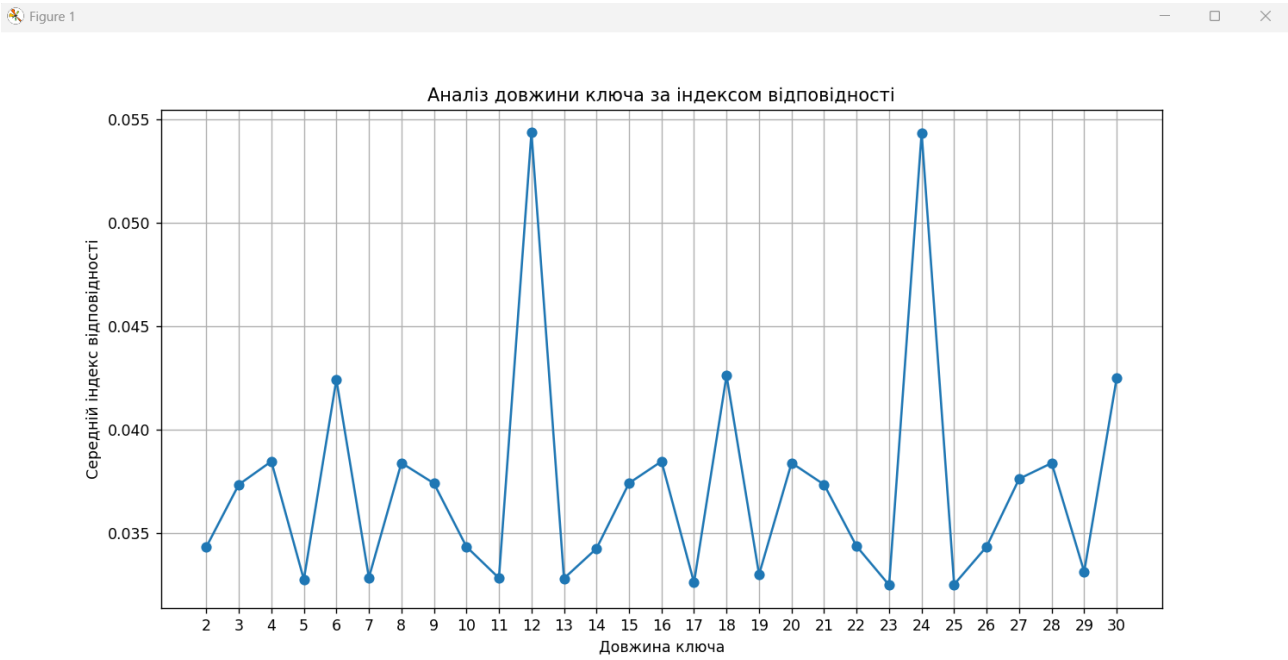


Можна зробити висновок, що чим більший ключ, тим краще шифр приховує повідомлення, бо індекс відповідності падає. Для 3 більший чим у 2, бо вийшла невдала комбінація, і вийшло трішки більше випадкових повторів у шифротексті, ніж очікувалось.

3. Зашифрований текст 1 варіант:

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузк
ъяциъпаэълыкъзэльйюрмувнусьъюоыюдежжъсбххиуънпеусздкруытчкбзхсаъ
мгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпу
ютерпэбыпвбхлкдюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрмуацфяюшш
…

Для початку порівняємо значення індексу відповідності для ключів довжиною від 1 до 30:



На графіку видно, що значення при довжині ключа 12, є найбільшим, тому припускаємо, що наш ключ довжиною 12.

Тому знаходимо ключ та за допомогою нього розшифровуємо текст:

Знайдений ключ: вшекспирбуря

Розшифрований текст:

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацереаюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкорабльвморебуряггромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцыveселейребятаveселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзал

оуходятгонзалооднакоэтотмалыйменяутешилонотъявленныйвисельникакомусу
женобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовисе
лицысделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткора
бельногосейчаспользымалоеслиемунесужденобытьповешенныммыпропалигонз
алоуходитбоцманвозвращаетсябоцманопуститьстеньгуживонижениженепопробуе
мидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибур
юикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчего
вамнадочтожеброситьвсеиззавасиидтинадновамохотаутонутьчтолисебастьянязв
атебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобоцманахт
акнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгр
язныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабль
былнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакгло
ткуболтливойбабыбоцмандержикручекветрукручеставьгротифокдерживоткрыт
оеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьп
огиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмоль
бывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантонионаспогуб
илаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморе
мгонзалонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпо
топитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаидетибратпро
щайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятг
онзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойне
годнойпустошизаросшейверескомилидрокомдасвершитсяволягосподняновсетак
иябыпредпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовход
ятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтова
лиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсясне
босводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпогиба
вшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразб
илсявщепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбо
жествомяморевверглабывземныенедраскорейчемпоглотитьемудалабыкорабльс
несчастнымилюдьмипроспероутешьсяпустьдоброетвоенестонетсердцениктонеп
острадалмирандаужасныйденьпроспероникто непострадалявсеустроилзаботясьо
тебемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтове
домотебечтотвойотецзоветсяпроспероичтоемупринадлежитубогаяпещерамиран
дарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрыть
нопомогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемиран
деутешьсяотримирандаслезысострадальстольбедственноекораблекрушеньекот
ороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеостались живыдац
елывсектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголовыиволос
неупалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткрыть
ктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперонопробил
часвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригода
итынаверноенеможешьвспомнитьотомчтобылопреждемиранданетяпомнюпросп
еротыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятисвое

йпоявляетсяневидимыйариэльонпоетвсопровожденииимузыкизанимследуетферд
инандариэльпоетдухигорлесовиводвсевхороводутихломоревлегкойпляскесплес
комруксомкнитекругмнедружновторявнимайтедухисовсехсторонгаугауариэльп
сысторожевыелайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопе
ньепетухакукарекуфердинандоткудаэтамузыкаснебесилиземлитеперьонаумолк
латоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегу
вдругповолнамкомнеподкрались сладостныезвукиумеривяростьволнискорбьмо
юсследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетот
ецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкост
истанутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронн
ыйзвондухидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследний
сонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюдани
сходятсвысотыпросперомирандеприподнимижезанавесресницвзглянитудамира
ндачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасенонноэтолишьвиде
ньепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспасся
вплавьприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоск
орбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандаб
ожественнымегобяназваларольнеаполяфердинандонслышитдивясьчтовдругтыв
спомнилпронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквид
еличтомойотецкорольпогибвморскихволнахмирандаувынесчастныйфердинандп
огиблиснимивсееговельможипогибмиланскийгерцогвместессыномпросперовст
оронумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьещеневре
мяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвобо
дузаэтодамвслухпослушайтесиньорзачемпозоритесебянеправдой

В результаті наш зашифрований текст виявився твором Вільяма Шекспіра «Буря».

Висновок: під час виконання комп'ютерного практикуму було досягнуто поставлену мету, а саме: засвоєно та застосовано на практиці методи частотного криптоаналізу для розкриття шифру Віженера.

На першому етапі роботи було проведено шифрування фрагменту тексту твору Гоголя з ключами різної довжини. В результаті аналіз індексів відповідності отриманих шифротекстів підтвердив, що зі збільшенням довжини ключа індекс відповідності падає.

Для шифротексту(1 варіанту) за допомогою методу індексу відповідності було проаналізовано ймовірні довжини ключа, де графік показав найвищий пік при довжині 12. На основі цієї довжини, шляхом частотного аналізу, було знайдено ключ "вшекспирбуря" та успішно розшифровано повідомлення.