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

Виконав:

Студент гр. ФБ-11

Ахунов Михайло

ВАРІАНТ 15

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.

Файли з текстом називаються encryption(довжина ключа).txt

Ключ ‘да’

Жндчдлйивлгвырйзжыыанntждроойвферяуоивйчйртдмнропоиончйлтвйкжыьепилсжоййоаро
фкмкtttрчюсасирапоцжмлацтвжсрпйрйупкйндупиъуммйдпесnткдкеыжнйрйшммтсциттурдвм
лхяоксурохтчосбпазоуопуынтилбйгсупвхтфеыихсжойющолянктйсапехтсиъеоарофкдезоурмхт
дмлдсаптдхаровкфожлййжыхооозоуяцибтджсозоиорамптхтдмлдбтлйесаькдфыерндкжафтмрч
кжафтмрсагжйхтзгйоайгтуооцофоносnднммдлбтчкдмтроухоееиориурмспузонптмйщдлдсаоин
тюпехтсиъеннмжйвттиепьсонкжафтмрйиоакдяйфалпфижыщоиесачлмцчерусеуръмйнсосаиое
ыпоуртхтдмтаммтхтзгйоисонкчхсиуоытмвхездндсцекьттжофесntйсапехтсиъумкджиынрдз
ропоиончйлтвйкуртхтдгммтччвхтжожапкдктецоеопелнйнсойицрчспижойоэуэесийкtttртгтс
цыиипсгиттооцофозорофщмлхятнеыпдтлкескфузорхтзгйоембтяпсгссеввхтфецицьхя

Ключ ‘дуб’

Жабыумйыяптгыгжлхьыуксбздглтшгфшнгвпихжышстчйсяппбетьшйюпжшлжощйюйлдгтшко
унтглмэпцбсчсодайрумтезмюэъбгжднушсйжмошоджммйфмяжиюжсапоулеогсшсйлйрбтцыпц
всдхйпдаоэочяпхефтавпудтвппжшсбйлфжзафпхтцгжыытххпйсцтъанэпнабпштцайъшлдяпфэб
йцпугйщбемюбхпртчтдяпвэстхмйьгядпобдтвацыюцузсбдтчпруйубцтчйпувтюжйабьэбшкжраб
охбфейфжлжусцыссуакшцтъанэбйцпчэпцбстьпсабсындююцжлдяпфэфхбвйчпрырфытпждтьрт
яжэумддэтчотсмйдусычйьомщжжбуишмаапнэгдгумгжмэбкчьнгблвсмхьщбейабчюйъжжржой
всйяжсапсуетфьпбрфбцтчйцпнмяпщбигьлмапнэфщайубшцыгхшдиуоддуйщэтегтгжсапнабпш
тцайъжйоузиокфуирбмтчпнкжпбгйэрфбцтчарынткфждужбгдюлдэпйепебмйъойаотшйцгфхюй
жбжтмфэшомшлтепфбдтдуячйпдамбуобутгпзбнтгъмютгбоеомибмкшоогфзбнщбигьлйывттмх
ттсшяждуфшумеэхт

Ключ ‘хлеб’

Чшешхцкйуцдгмыкичжьбюшузхыппънхжбкфпщнкшъыуеэшспащйпювкмгнклчжэжаумтчщккя
лспехнлгэусийтбвусбащчзэцбчгнзтбъксъюрлъшефауыфэчкеартогхелцжзоъыкщэчутзууудыегэ
ццаяхтфбщцуищтвалипдщрфмшуйьмкдвюргжэхжмуцтчщкякщмаюхуквлржжэтйлрпббщхлхри
пдынцгпнмхьбргпцббщглещзмъфзьжщппшщфазувухстпшщйпблнргауеэцевгцкжвлэлхяьжбше
лчлхуэышлчлхуэытбфскцгтдкялкдгюппзщхпющтохшннхцвуихенгыпфжщжжщщсйдынтаюип
юъунъдемхьбпщшуяарцувуыжюшнзънуущррэвщолчлхуэыкйяллерфхбьъхйчжъпщртбицнчирс
фврфсъчковщтбщщжьащфсгауеээбнэчуцгтдкяутпюхшцвуфпмэнгжриехшетзрлэгэзпертогфтба

рцувуыфэхезщжосхтспащйпювкмгнклдыуцгпднэчушинцучщзбахелгрчпцщржьшковщкйзышт
аузпъщюфортйъхуугыудгьчьщуртфуууящчпещипбщхъэццагшжьапумыртлеюипбауиффпжэму
ааьдтврггжэхжзучэжк

Ключ ‘туман’

Фамчнэшфюшсхгртщхзчныаъжнвэъепвшшяьачоедчгъдхяяълыцбхчтэбоечфодешъъэвычьцаща
гцичаеърарамнхюучояшычьгахосщбшьеаээсннеюфцаъясдшчащочтэныпяшьееъяъсяъбюпэтхф
люсэцнаюбэтааанлнхбыошекщохщфсгъеюосявшгиюгхъелзбуяцьбхннэшэтъъйскнюбькнчцъпэ
ъиъдхэуэььачэащасцрыфюсйпндъкыхбыяяърюауябпосаямиьаиъдхэуношчшщаеьуачтюамкптг
юиэеэоаэдыьннсщсхыщтхкнчцъучаеърыыбщнняышашпеякнюбькагбнесаяфпэъдчураьыощчм
млнгпъдъасчеюдафцтыафжтфбюдтэпщоцьхмряъгсичтщрыцвуупэъхзхыцшщааэывутюжщеьв
шшеъябщасафзлыбгъхыцыюьщъяъхыщтхкхябхказафпыйефвючцраътдюеуобювывшщныыамл
тгещигеыцауцохрнщяълыцбхчтэбоечбгъхыцтшищакявюдхъвнээмкычеъбыэшунтяаъехдгясшъ
хъеылжееъъшцояагъгыгездхэдлиыдэътывбпощагеишгтънонюрошшшщкэецъмваълйччыномэд
лсъчсосявшюияодл

Ключ ‘облачность’

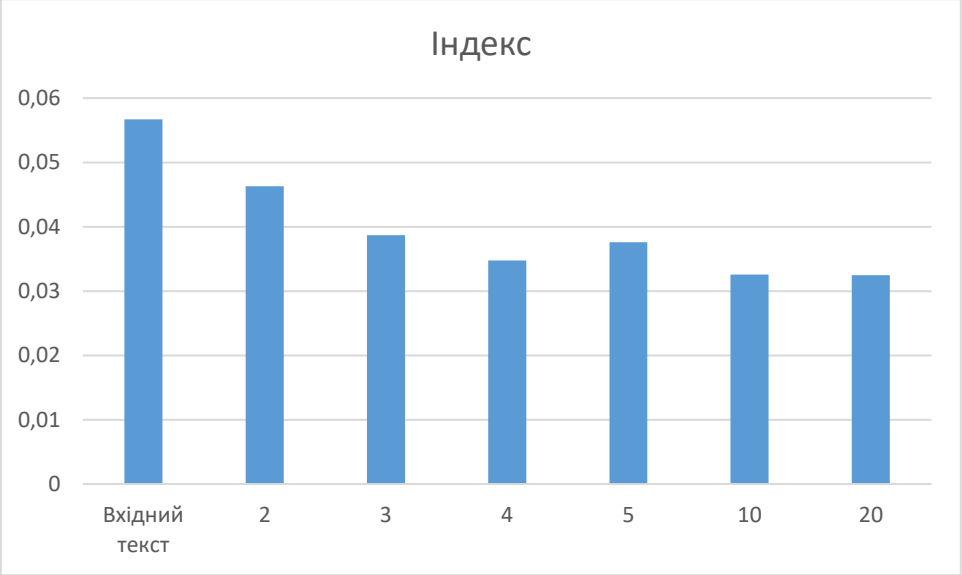
Ролччшущрзнгврьфрмйьчощжчэшячююжчяжытучуусщдяъъяэктпфчьшьучжрьгевххвфкукхаг
ыюыъжьущрклысядъбцойуцьотьгнсгьубчпщлрнчащщипцнрдвтыюажолмыщъубчфцнщсйхьгб
могулимшыяпъпьткыытэьспъоваеюадхвргдащугоюжвииюрячъгптяачьъяьщжьтдхдцььъпыкчт
сябмццщдяшоволъеьагымывкрмрйщияяькспъяйхлгтвыпооыыъсъльцщдяшотазужшапчоейбъо
лкщнюгъмблназяцбяьнзрхефнъььудщубыаявкчпшнчъцэтзлуюкчщьбыпяпмеыыъщбмцтцуъыча
аиуъллчюкяцйьяцеияыщибчоужьпьгцбщэшоачрсвоцсрибнфхнеюбтпзхрмзктжшакшцзебъфше
жэуэчйыпшаыыпмэкэсщхесцгоицнщхефнъьдыпфкквыщбкеуувитсхтйотэеэйьгфкюжшнецысэ
бяушинацытвтьфрчфъяэктпфчьшьучжэсщхеснэъиьшювияряфьщллкетаяукщжтньъыячдасюсв
хрячкзфдедхуыаоьсщгеюамцдщткиеяшядкюпоогыюкъзяащншищхазфжшкзасяюсьикйбтцтаы
щтксдтмугоюжэиййяр

Ключ ‘завтрапятницакайфуем’

Йнвйрлфзршзшчъерцоьмрнршррщнчпшымйпчшхкгмррцшнынэымдйбефвххцйыъчыицрфыня
ккмчдэнцхтрвгюьяяхфцлштпьюбвхвдгьпфпчауаечаьяыыяпмзцыеьмачиабевцщгкдпмргвиэсбэ
ишихсиюэтяуоудгоьаэнлдпшльлауфобзхэуъбгяшычтсъцбккьойсщкэиянуысьнскшпмуотьретн
бэрлооиффдбыхдутьонйвыкбеувдебпъкоссвимстухдгшдчауныххрцшлпаашнынкшуфзьсунвьт
аясъэыавкрыьгтмжжззюзоиьннщоэкчжбхъропярнчлтшеиуфахвгпяшогчфоызбэрзлэгчэвушмщ
вэрслнцъцфлпсыбыысрнкшхвэсцтутншйуцухюпрзъъахгнцшцзщрсцоъълептглчхетфйнппщщя
кщфоптфоръэычжояоньебшпмрзюзоиьххдйфуюбыфъюткфбетгтъизтпжевезъчепяюйьяэтщинт
цььэетлылврзынэымдйбефвхкццррзюдолъщцнумсыцбзмтквьюебнуыуызчецббкфщрхгыиснчы
бйщпнсщэуюхррхюсбъцхузятоыюбчъчоеаьояшъшщхочбдячучнепьаутнювцэяукоьфултсбгэен
бгяшытттеет

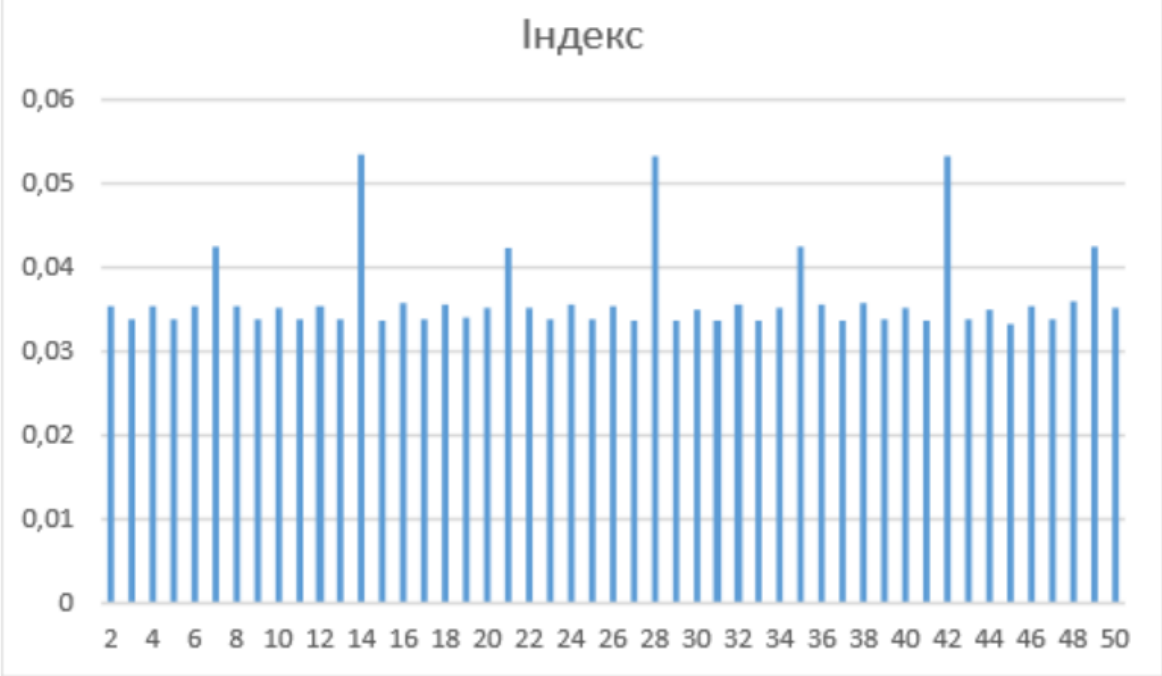
2. **Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.**

Діаграма індексу відповідності. Ці данні записані у файлі Affinities.csv



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

Розрахунок індексу відповідності зашифрованого тексту для згенерованих ключів довжиною від 2 до 50 (данні зберігаються у файлі Affinities_task3.csv)



Найбільше значення індексу відповідності при ключі 14, тому я спробував підібрати ключ довжиною 14. При підборі ключа у мене одразу вийшло згенерувати правильний ключ **“поснякованд рей”**

Розшифрований текст (зберігається у файлі decrypted.txt):

наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгустой
тайгизатерялась михайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслин
есчитатьскитупустозерскогоострогачтонапечоререкенудотогоскитаещедобратьсянадоакздешн
емумонастырюпожалуйстахочешьчерезвологдудапотомпосухоневеликийустюгатамидодвины
рукойподатьзнайплывипотечениюахочешьнапрямикчерезладогусвирьонегудальшенасевергдев
олокомагдеозерамималымиизновгородаудобнеетакизкакихдругихрусскихземельчерезустюгво
бщемдобратьсявмонастырьмихаилаархангеланевеликапроблемабылобжеланиезамолитьгрехии
линаоборотвушкуйничийпромыселпуститьсятожечерездвинунеплохосколотитьватагувыстрои
тьстругивтомжеустюгедавпутьотустьядвинырекивседорогиоткрытывсторонычужедальниенев
едомыевпечоруввеликуюпермиювюгругденемирнаясамоедьтакиноровитвсадитьвсердцеушкуй
никаоструюкостянуюстрелусмоченнуюгнилойрыбьейкровьютутжеипутьинойиноческийкмона
стырюсоловецкомувпрочемкнемулучшепоонегепрямейбудетолегиванычназначенныйвоеводой
новойновгородскойэкспедициииспользовалобапутичастьлюдейвместеснимсамимшлананеболь
шихлодьяхпосвиридаонегедалеепоморюгандвиксзаходомвсоловкинамолениеиснованаюгкдви
недругаячастьнаправилась черезвеликийустюгснаказомкупитьтамлодейдляморскихплаванийп
ригодныхкупиличегоужкочамителодьиназывалисьпрямоскажемнекаравеллыдаженекоггимелк
иекакиетонекрасивыесполукруглымднищемнекоторыеужхотелибыломордыплотникамзатакие
судабитьдазнающиелюдиотсоветоваливопервыхплотницкихартелейвустюгетьмасварузатевать
себедорожевыйдетнуавовторыхтакиеводкорабликиинужныч тобсудачейполедовитымполуночн
ымморямплытькорпусхотьинеказистыйдакрепкийтеплыйвкаютекаморедажепечканебольшаяи
меетсяачтосднищемполукруглымвмореболтаетсильнотактоневеликабедазатольдамивовекнера
здавитальдоввполночныхводахвидимоневидимотолькочтолетомплытьиможноитокакбожьявол
ябываетзатянутморетуманыдатакиечтоносасобственногонеразглядишьилиподуетвдругборейсе
верныйветерпринесетгромадныельдинывотидумайтолидальшеидтитолипересидетьпереждатьд
атолькождатьтодолгонькоможноасеверноелетокороткоенеуспеешьоглянутьсяужезимавотисид
итогдазимуйеслисможешьмногоетутнеотумениялюдскогоотпогодызависелонуаужпогодавести
моотгосподаможноведьбылоидалечеуйтизатритомесяцааможноидовайгачанедобратьсятуманы
даштормадальдыпережидаялилдождьбеспросветныйинудныйвсюночьнапролетнепереставаякр
упныетяжелыекапликолотилипокрышампрогонялисулицредкихприпозднившихсяпрохожихпр
евращаливхлюпающуюгрязьтянущиесявдольгородскойстеныогородывэтуночьтемнуюиненаст
нуюстражникинабашняхстарательнокуталисьвплащиукрываясьотпорывовпромозглоговетрата
койветеробычнобываетпозднейосеньювноябрекогдасыплетсяснебанепоймешьчтотолихолодн
ыйдождьтолимокрыйснегаскорееитоидругоесразунотоосеньюасейчаснадворестоялмайхотьине
оченьтотеплыйздесьвсеверныхновгородскихкраяхдаужинетакойчтобсоснегомвотужпослалчер
тпогодкуадядькокузьмаобернувшисьknапарникувыругалсяворотныйсторожмолодойкруглолиц
ыйпареньвкоротковатойкольчужкеиостроверхомшлемебрызгидождяскатывалисьпошлемупря
мозашиворотпарнюитоттоиделоморщилсяпередергиваяплечамивторойстражниккузьмавысох
шийпожилоймужиксреденькойбородкойидлиннымивислымиусамиотвернувшисьответрабуркн
улвответчтотонеразборчивоевидимосогласенбылчтоподобнуюпогодкутолькочертипосылаетпо
верхкольчугиукузьмыдлинныйкрашенныйчерникойплащизплотнойдерюгивнебольшойплетен
ойбаклажкеупоясаплескаласьмедовухаславенскийконецслааавенелеслышнодонеслосьспетровс
койбашнискрытойпеленойдождяиночнойтьмоюслааавентутжеподхватилисоседисбашнишестис
тенной чтовсотнешаговоткузьмысnапарникомплотницкийслааавенотkликнулсякруглолицыйнес
пиммолдождалсякогдадонессяответотсоседейслевасбашничтонасамомберегуволховаобернув

шисьподмигнулугостилбымедкомдядькокузьмавислоусыйкузьмаширокозевнулперекрестился истряхнувсбородыкаплинехотяпротянулбаклагупейонуфрийдатолькосмотритриглотканеболем естоунасбеспокойноенеточтоуэтихонмахнулрукойвлевовсторонуволховскойбашниместечкоим действительнодосталосьтоещебойкоееслинесказатьбольшебольшаячетырехстеннаябашнянако торойнеслислужбукузьмасонуфриембылапроезжейвыходилаворотамизагородскуюстенукболь шойдорогечтоизвиваласьмежлесовдаболотпоправомуберегуволховастойсторонымногоктомог пожаловатьихитроватыйкостромскойкупецитихвинскийбогомолецврясеиприказчикновгородс когоархиепископаимосковскийслужилыйчеловекпоследнихпослепораженияновгородцевуреки шелонирасплодилосьвновгородекудакакмногошнырялитудасюдапоторгучтотовынюхивалинос свойсоваливделановгородскиесоветовалиимелинатоправоподоговорукоростынскомупотомуже договорувыплачивалновгородмосквеконтрибуциюшестнадцатьтысячсеребромденьгинемалые нуденьгиуновгородцевводилисьбогдаствыплатятавотточтоужслишкомнахальномосковитывих делалезлимногимнепонравубылохорошмедокутебядядькокузьмакрякнувпохвалилонуфрийпод иженкавариласвояченицанухорошхлобыстатьдоутраточайдолгостойкадядьковдругнасторожил сяонуфрийчувродекаккричитктодакомутамкричатьтосвесившисьзаограждениебашникузьмагл янулвнизестьктотутальнетямилостивецмонахизобителидымскойчертвасмонаховпоночамносит нуисидитеперьутрадожидайсяправильнодядькокузьмаонуфриюкакикузьменеоченьтохотелось отворятьтяжелыескользкиеотдождяворотаутромтобогдастперестанетдождищеспасимилостиве цжалобнозагнусавилмонахитаквесьпромокдониткихотьзаденьгупустиатымолисьчащеотчехохо тнулонуфрийатоходитвасздесьночамиакинукапомолчипаряпрервалкузьмаэйотчетыпрокакуюд еньгусейчаспомянулпромосковскуюалипроновгородскуюакакаятебелюбезнейстражникиперег лянулисьнучтоотворяетеворотанетосейчаскпристанипойдудапогодитывонспускаемсяужезапла тивстражникаммонахюркийплюгавистыймужичонкасбегающимиглазаминатянулнаголовупла щнаброшенныйповерхрясыискрылсявдождливойтьмеонпрошелпославнечутьзадержалсяупово ротанаильинскуюулицупостоялпогляделкудатоинехорошоусмехнулсяужопосчитаемсятеперьс тобоюзлобнопрошепталонпосчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмелон еопасаясьвыбежавшийизповоротанарогатицушпыньхотелужмахнутькистенемпришибитьдурн огомонахадатотобернулсявовремяитатьночнойвдругощерилсясловноувидалотцародногоубрав кистеньпоклонилсяприветливовиднознавалкогдатомонахадаимонахалисговорившисьдальшев двоемпошлилишьуфедоровскогоручьярассталисьтатьнамосковскуюдорогупошелчерезмостикп ромышлятьдальшеаливкорчмукявдохеамонахкбоярскойусадьбесвернулзаколотилвворотанадв орезашлисьвлаецепныепсыктотоиздворовыхслугпробежалгрузнотопаяподубовымплахамкогот амчертпринесоткрывайпоскорейпескгосподинуматонеотмосковскихлюдейпосланец

Висновки:

У цій роботі я ознайомився з роботою шифру Віженера, завдяки якому я зміг зашифрувати вхідний текст написаним скриптом, і таким поняттям як індекс відповідності. За допомогою отриманних знань я зміг написати скрипт, завдяки якому я зміг підібрати довжину ключа зашифрованого тексту і підібрати сам ключ.