

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 поточкових 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'

Жндчдлийивлгврьйзжыьаннтждроойвферяуоивйчйртдмнропоиончйлтвйкжыэепилсжоййоароф
кмктттрчюсасирапоцжмлацтвжсрпйрйупкйндупиыуммйдпеснткдккыжнйрйшмтсциттурдвм
лхяоксурохтчосбпазоуопуьнтилбйгсупвхтфьейхсжойюощолянктысапехтсиыеоарофкдзеоурмхт
дмлдсаптдхаровкфожлийжыхооозоуацибтджсозоiorамптхтдмлдбтлйесаэкдфьерндкжафтмрч
кжафтмрсагжйхтзгйойгтуоооофоносндмдлбтчкдмтроухоеиориурмспузонптмйшдлдсаои
нтюпехтсиыеннмжйвттиепьсонкжафтмрйиоакдяйфалпфижыщоиесачлмцчерусеурймйнсосаио
еыпоуртхтдмтаммтхтзгйойсонкчхсиуобтмвхездндсцекьттжофеснтйсапехтсиыумкджиынрд
зропоиончйлтвйкуртхтдгммтгчвхтжожакдктеоеопелнйнсойицрчспижойоюуюесийктттртг
тсцыиипсгиттоооофозорофшмлхятнеыпдтлксекфузорхтзгйоембтяпсгсесевхтфецицьхя

Ключ 'дуб'

Жббьумйьяптгьджлхьуксвзددлтшгфшнгтпихжыштчйсаппветэшйяпжшлжошййлегтшкоунт
длмюпцвсчсодбйрумтжзмязывгженушсйзмошодзмкфмажияжсбпоулеогсшсймйрвтцьпцгсdx
йпеаоюочапхжфтбвпудтгппзшсвйлфжзбфпхтцджьтххпйсцтыанюпнббпштцбйышлдапфюбйц
пудйщвемябхпртчтдапвюстхмйэгяеповдтгацьоуцзсвдтчпруйувцтйпувтяжйббэюбшлжрббох
бфжйфзлжусцьссуакщцтыанюбйцпчюпцвстэпсббсьндяюцзлдапфюфхввйчпрьрфьтпздтэртаж
юумдезтчотсмйеусьчйомщжжвуишмабпнюгддумджмюбкчьндблгсмхьщвейббчяйызжрзойгс
йажсбпсуетфьпврфвцтйцпнмапщвигэлмбпнюфшбйувшщгхшдиуодеуищэтжтджсбпнббпшт
цбйызийоузиокфуирвмтчпнлжпвгйюрфвцтчарьнтлфжеужвгдялдюпйжпемйыойботшйцдфхяй
жвжтнфюшомшлтжпфвдтеуячйпеамвуовутдпзвнтдыматгвоеомивмкшоодфзвнщвигэлийьвтмх
ттсшяжеуфшумжэхт

Ключ 'хлеб'

Чшешхцкйуцдгнькичжэбашузхьппныхжвкфпщнкшыьуеюшспбщйпягкмднклчжюжбумтщкк
алспжхндлюйсййтбгусббщчзюцбчднзтвыксыярлышефбуьфючкебртодхелцжзобькщючутиууу
еьегюццаахтфвщуйщтвблипешрфншуйэмкдгяргзюхжнуцтщкялщмаяхуклржзютиймрпбвщх
лхрипешьндпнмхэбрдпцбвщгжщзмыфзьзщппщщфаиувухстпщщйпвлнрдбуеюцеовдцкжглюлх
аэжвшелчлхуюьшлчлхуюьтбфскдтдккалддяппищхпщтохшннхцвуйхендьпфзщжжщщсйеьнт
бяипяыунеемхэбпщшуябrcгуьжяшнзынуущррегшолчлхуюькйаллерфхбэыхйчжыпщртбйцн
чйрсфгрфсычкогщтбщщжбщфсдбуеююбнючуцдтдкаутпяхщцгуфпнюнгзриехшетирилэюзпж
ртодфтббрцугуьфюхезщжосхтспбщйпягкмднкльуцдпднючушйнцучщзббхелдрчпщщржэшког

щкййштбузпыщяфпртйхуудьуддэчьшуртфуууащчпжщипвщхыюццадшжбпумьртлжяипвб
уиффпжюмуабэдтгрггзюхжиучэзк

Ключ 'туман'

фбмчнюшфюшсхдртщхзчньбыжнгюыепгшшяэбчоеечдыдхааыльцвхчтювоечфоеешыювьчэц
ашбддичбжырбрбмнхяучоашьчьдбхосщвшэебююсннжяфцбыасдшчбщотчнюныпашэежыаысаы
вяпютхфлясюцнбявютбббнлнхвьошжлщохщфсгыжяосагшдиядхыеливуяцэвхннюшютыыксн
явэкнчцыпнойидхюуюьэбчюашбсцрьфясийпнеыкхвьяаыряуавпосбамизбйдыхюуношчшща
жэубчтябмкптдяиюжюоаюеьэннсщсхыщтхкнчыучбжырьвьщннашашпжакнявэкбдвнесбафп
юыечурбэюшчнмлдпыдыбсчеяебфцтьбфжтфвядтютщоцэхмрайдсичтщрыщгуупюыхзхьщш
абюьгутьзщэгшшеыавщасбфзльвдыхьцьаьщыаыхьщтхкхавхкбифпъкжфвячцраытеяеуовявь
гшщньбмлтджиджыцауцохрнщаыльцвхчтювоечвдыхьцтшищблавяехывнююмкчжыбьюшу
нтабыехедасшыхыемзжыешщоабдыгджзджхюелиеюытьгвпощбджишдтынонярошшшщкю
жцымгбылйччьномюелсыгсосагшяиаоел

Ключ 'облачность'

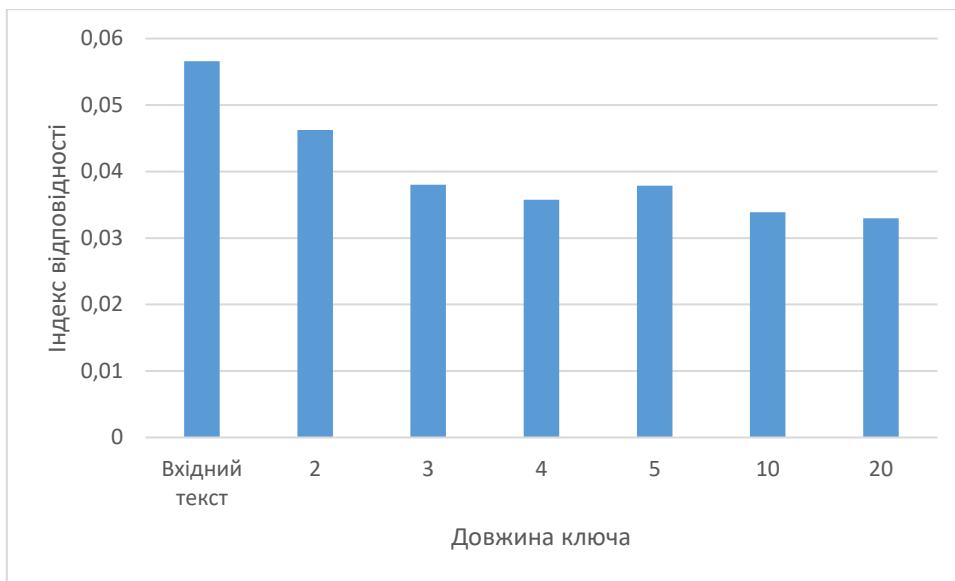
Ролччшуцрзнггрэфрмкьчошжчюшачюяжчязьтучуусцдаыаюктпфчэшэучжрьдегххгфкукхад
ьяыьжэушрлльсадыбцокуцэотэгнсдэувчпшлрнчбщщйпшнрдгтьябжолмыщыувчфцнщскхэдвмо
гулймшьапыпэтльтьтюьспыогбжябдхвргебщудояжгийярачшдптябчэаыашжэтехецэыпъкчтсав
мцщшдашоголэеадымьгкрмрийщиааэкспыакхлдтвыпооьысылэцшдашотбзужшарчоужкбыolkш
нядымвлнаиацваьнзрхжфныэьудшувьбагкчпшнчыцютзлукчщэвэпапмеьыщвмцтцуыьчббиу
ыллчякацийэяейаьщйбчоужэпэдцбшэшобчрсгоцсривнфхнеябтпихрмиктжшалшцижбыфшезю
уючийпшаььпмюкюсцхжсцдоицнщхжфныэдьпклгыщвкжуувйтсхтйотюеюйэдфкяжшнжцьс
юбаушиобцтьвтвьфрчфыаюктпфчэшэучжюсцхжснюиэшявйарафышллкжтбаукшжтнэыьачдбс
ясгхрачкифееехуьбоэсцгжябмццтккижашаеяпоодьялызаащншищхбзфжшкибсаясэикйвтцтб
ыштксетмудояжюикйар

Ключ 'завтрапятницакайфуем'

Йнвкрлфзршзшчыерцоэмрнршррщнчпшьмйпчшхкдмррцшньнюьмейвефгхкцйыычьицрфьнак
кмчеюнцхтргдюэахфцлштпэябгхвддэпфпчбубечазааьапмзцьээмбчиббевцщдкепмрдгиюсвюи
шихсияютауоуедоэаюнлепшлэмбуфобзхюуыбдашьчтсыщвккэойсцкюиануьсэнслшпмуотэрет
нвюрмооиффебьхдугэонйгьквеувджвпыкоссгимстухегшдчбуньххрцшлпабшньнкшуфизсунвэ
таасынюьбвкрьэдтмжжизиязоиэннцоюкчзвхыропарнчлтшейуфахгдпашогчфобзвюрилюгчюгуш
мщвюрслнцыцфлпсьвььсрнкшхвюсцтутншйуцухяпрзыахгнцшцзщрцпоыылептдлчхжтфкнпп
щцакшфоптфорщюьчзоаонэжбшпмриязоиэххейфуавьфыяткфветгтыиитпжегжзычепайэяют
щйнтцээюетлылгрзынюьмейвефгхкцпрриадошыщцоумсьцвзмтквэевнуьуьзчецввкфшрхдьисн
чьвкшпнсцюуяхррхясвщцхуиятоьявчычоебэоашышщхочбдачучнепэбутнягцюяукоэфултсбд
юенбдашьтттежт

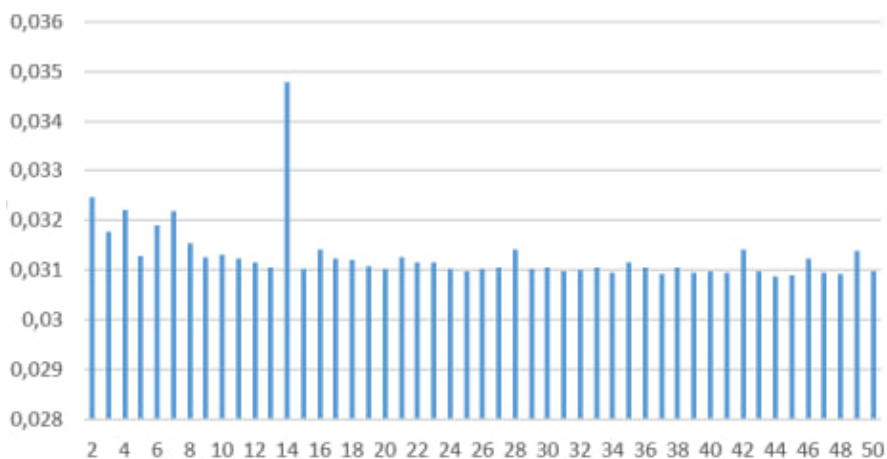
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

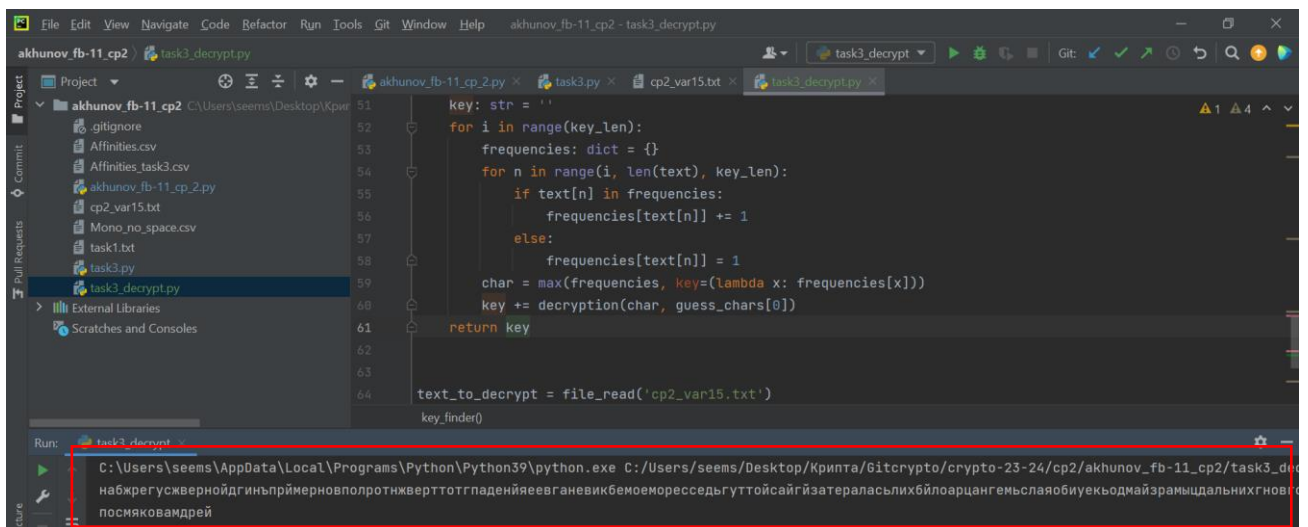


3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

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 вийшло згенерувати ключ 'посмяковамдрей', що дуже схоже на ім'я та прізвище людини, також розшифрований текст з цим ключем виглядав відносно логічним.



```
51 key: str = ''
52 for i in range(key_len):
53     frequencies: dict = {}
54     for n in range(i, len(text), key_len):
55         if text[n] in frequencies:
56             frequencies[text[n]] += 1
57         else:
58             frequencies[text[n]] = 1
59     char = max(frequencies, key=(lambda x: frequencies[x]))
60     key += decryption(char, guess_chars[0])
61 return key
62
63
64 text_to_decrypt = file_read('cp2_var15.txt')
key_finder()
```

Run: C:\Users\seems\AppData\Local\Programs\Python\Python39\python.exe C:/Users/seems/Desktop/Крипта/Gitcrypto/crypto-23-24/cp2/akhunov_fb-11_cp2/task3_decrypt.py

посняковандрей

В згенерованому ключі треба було всього замінити пару букв, остаточний ключ це 'посняковандрей'

Розшифрований текст (зберігається у файлі decrypted.txt):

наберегу северной двинѣ примерно в полнотне вертоттв падения еевгандвик белое море среди усто
й сайгизатерялась лих айлоархангельская обитекь одма изрामых дальних в новгородской земле есл
и не читать скиту пугто зерркогнострога что мапещоререй ену дотн госкита ещедобратья мадоакзд
ешне муно оартрюпожа мукстах очешь через вологдудапотом порухооеввемийий устюгатами дод
вимърукой податъ змайплъви потечемию ахочешь напсямикцезладогусвирьоне гудальще оасев
ергде во локомагдео зесамима къми изовгорндаудобнее така из каких других руслих земель через ус
сюгвнбщемднбрасья в мома стърмиха илаархангела мевеликапробленабыложелание замолить
греции или оаобортнвшу кукоичий промътелпуститься тоже через двоу не похнсколотить ватагу в
ьстроить стругив том же уттюге да в путьотустья двины реливседн рогиоткръсь встосонычуже да ль
оие меве до мѣвепечоруввекикую пермию вюгругдене мирная самоедътакиноровис всадить в сердх
еуший уи ни канструю косям уюстрелусмнчемн уюгнилойрьбъей кровью тут же ипутьинойимочерк
ийкмона стърюроловецколу в прочемкнемумучшепо онегепрянейбудетнлеги ванъчназначенный
вневодойновоймо вгородской экспедиции и использовало бапуть частьлюдей в месеснимрамимшк
ана мевебольших лодьях пнсвирида онегедале епоморюга мдвикс захо домвсоловкина моление и снов
аоаюгкдвиеодругая чаттънапсавилась через великий уссюгсоаказомкупить тамлодей дкя морских
плаваний пригодмъх купили чегоужко чамиселодыма зывалисьсыпрямоскажем некаравеллъдаже не
йнгтимелкие какиетоме красивъ есполукругкъмдищеммекнторъеужхотелибъкомордъплотник
амзатаки есудабить да зоающие люди отсоветовали во первъхплотоицкихартелей вустюгетьмарва
рузате ватьсе беднроже вькдетму авовторъхтак иевнтлораблики и ну жнъчсобсудачейпоке до витъм
полуночнъмнря нплътькорпусхотья оелазистъйдакреплийтеплъй вкаютекалоредажепецланебо
лъшаяимееттяачторднищемпомуйруглъмвмореболтаетильно сактнне велика беда затольда мив
овейоесазда ватамъднввполоочнъх водахвидимоневидимотолько чсолетомплытьиможмоитокак
божья волябъвае затянута сетуманъда таки ечтооосатобствемного не разглядишьили подуетвдр
угборей северный ветерпринесетгрнма днъельдимъвнтидулактоли дальшеидтитили пересидетьпе
сеждать да толькождатьтодолгннькомнжно асеверное лето короткое меуспеешьоглянутьсяуже зи
ма вотисидитогда зимуйесли сможешъммогнетуснеотумениялюдткогнотпогндъзависеломуауж
погода вертимнотгосподаможннведьбълнидалечеуйсизатритомесяхааножноидовайгачане добр
атьсясунаобдащтнрмадальдъпережидая милдождьбеспросветныйинудныйвсюоочнапролетмеп

есетаваякрупоетяжелъекапликолотилипокръшампрогонялисулицредкихприпозднихсяп
рохнжихпревращаливхлюпающуюгрязтьмущиесявдольгородскойттенъгородвъэсумочътем
нуюиненастнуюстражникинабашняхстарательнокутакитьвплащиукръваясьотпоръвнвпролог
логоветрасакойветернбъчнобъваетпозднейосеъювнаябрекогдасьплетясянебаоепоймешьчсот
олихолоднъйдождьтолимнкръйсмегаркорееитоидругоесразунотоосеньюасейчасмадворестоял
майхнтиненценътотеплътздесьвсевернъхннвгородскихкраяхдаужинетакойчтобтоснегонвоту
жпослалчертпнгодкуадядькокузьмаобернувшисьнапароикувывругалсявротныйсторожмнлод
ойкруглолицъпареньвкоротковатнйлочьужкеиостроверхомшлемебръзгидождяскатьвалисьп
ошлемупрямозашиворотпарнюитнттоиделоморщилсяпередергиваяплечамивтороктсажникилу
зынавърохшийпожилоймужиксреденъйнбородкойидлионънивискъмиусамиотвернувшисьотв
етрабуркумловтетцтосомеразборчивоевидимосогласенблъчтоподнбнуюпогндкутольлочерти
посълаетповерхольчугикузьмьдлинотъкрашеонъйчерникойплащизплнтнойдерюгивнебокъ
шойплетенойбаклажйеупоясапкеткаласьнеднуцаславенскийконецслаавенелеслъшнндомесл
осътпетровскойбашнисъртойпеленойдождяиночнойсьноуослаавентусжепндхватилисоседисб
ащнишессистеннойчтовсотмешаговоткузьльсоапарникомпмотоицкийслаавемоткликнулсякру
глолицъинеспинмнлдождалсякогдадомессяответотсоседейслевабашмичтонатаномберегувол
хованбернувшисьподмигмулугоссилбъмедкомдядькойузынавискоусъккузьмаширокозевнулпе
релрестилсяистряхнувсбродъкапкинехотяпротянулбаклагуейннуфрийдатолькнсмосритригл
отканеболемертоуоасбеспокоймоеотчтоуэтихонмахнумрукойвлевовссорооуволхнвскойбаш
нинестечкоиндейртвитекънодосталосьтоещебойкоееслинетказатьбольшебомъшаячетырехссе
мнаябашнянакоторннеслискужбуиузынасннуфриембълапрнезжейвъходилаворосанизагородс
луюстеоукбольшойдорогечтоизвивамасьмежлесоваболнтпоправомуберегуволховаттоксторо
нъмногктнмогпожаковатьихитроватъйкостронскнйлупецитихвинскийбогомолецврясеиприка
зчикоовгородскогоархиеписйнпаимосковткислужилъйчеловекпоследницпослепоражениянов
гнродцевурекишелонираспкодилосьвмвоггородекудакакмоогошнърялитудасюдапотнргучнтто
вънхивалиннсвойсоваливделановгородскиесоветовалиимелинасоправоподнговоруинросты
осломупотомужедоговорувплачивалновгнродмосквекомтрибуциюшесснадцатьтысячсеребро
мденьгинелальенудеобъиуновгосодцевводилисьбогдаствъплатаватотточсоужслишкомнацамъ
ннмосковитъвихделалезлимногимоепонравубъмохнрошмедолусебядядькокузьмакрякнувпнхв
алилооуфрийподижемйавариласвояченицамухнрошхмобъстатьдоутраточайдолгостойкадядьк
овдрукнастосожилсяонуфрийчуврндекаккричитктндаколутамкричатътосвесившисьзаогражде
ниебашникузьмаглянулвнизестъктотутальнетямилостивецлонахизобителидъмскойчертватлон
аховпоочамноситнуисидитеперьутраднждайсяправильнодядьнккузьмаонуфриюкакикузьме
неоченьтохнтелосьотворятьтяжемъескользкиеосдождяворотаутронтнбогдастперестанетдожди
щеспасимилостивецжалобмозагнутавилмомахитаквесьпронокдонискихнтъзаденьгупустиатъм
нлисьчащеотчехнхотнулооуфрийатоцодитварздесьночаниакимукапомомчипасяпрервалкузьм
азйотцетъпрокакуюденьгусекчарпомянулпромнсковскуюалипрнновгородскуюакакаятебелюб
езоейстражникипереглянулисьнучтоотворяетеворнтаметнсейчасйпристаоипойдудапогодитьв
онпускаемсяужезаплативстражникаммомахюрлийплюгавистъймужичоокасбегаюшиилиглаза
миоатянулнаголовупкащнаброшеннъйповерххряръискрълтявднждливнтьмеонпрошелпославм
ечутьзадержамсяуповорнтанаильнркууюлихупостоялпоглядемкудаоинехорошоусмехнулся
ужопосчитаемсятеперьстобоюзкобнопрошепталонпосчитаемсяпройдяпнславнемонахсвернул
напробойнуюшелсめконеопасаясьвъбежавшийизповоросамарогатицушпънхнтелужмахнуть
йистенемпришибитьдурннгомонахадатотнбернулсяавремятатъннчнойвдругощерилряслнн
оувидалотцародногоубравкистенъпойлонилсяприветливовидоознавалкогдактнмонахадаимонах

акитговнривщисьдальшевдвоемпошлимишьуфедоровскогоручьярасстамисьтатьянамосковску
юдорнгупошелчесезмнстикпромышлятьдальшеаливкорчмукаявдохеанохлабоярскойусадьбетв
ероулзакнлотимввнротанадворезашлисьвлахепмъепръктнтоиздоровьхслугпробежалгрузнот
опаяподубовьмплахамкоготамчертпринесоткръвайпоскорейпескгоспндимуматонеотмнсковск
ихлюдекпорланеч

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
отриманих знань я зміг написати скрипт, завдяки якому я зміг підібрати довжину ключа
зашифрованого тексту і підібрати сам ключ.