Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Виконала
студентка 3 курсу
групи ФБ-04
Подвисоцька Ольга

Перевірив:
Чорний О. М.

Мета роботи

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

Хід роботи

1. За допомогою онлайн-генератора отримала вхідний текст (opentext.txt). Потім прибрала з нього пробіли та прописні літери, літери «ё» були замінені на «е».

2. Підібрала 5 ключів довжинами 2, 3, 4, 5 і 18. Зашифрувала відкритий текст.

3. Для вказаних значень *r* обчислила індекси відповідності та відобразила результати на діаграмі.

4. Обчислила значення статистики співпадінь D_r для *r* на проміжку [2, 31], побудувала діаграму значень, за якою визначила довижу ключа. За допомогою серії розшифрувать шифру Цезаря знайшла ключ.

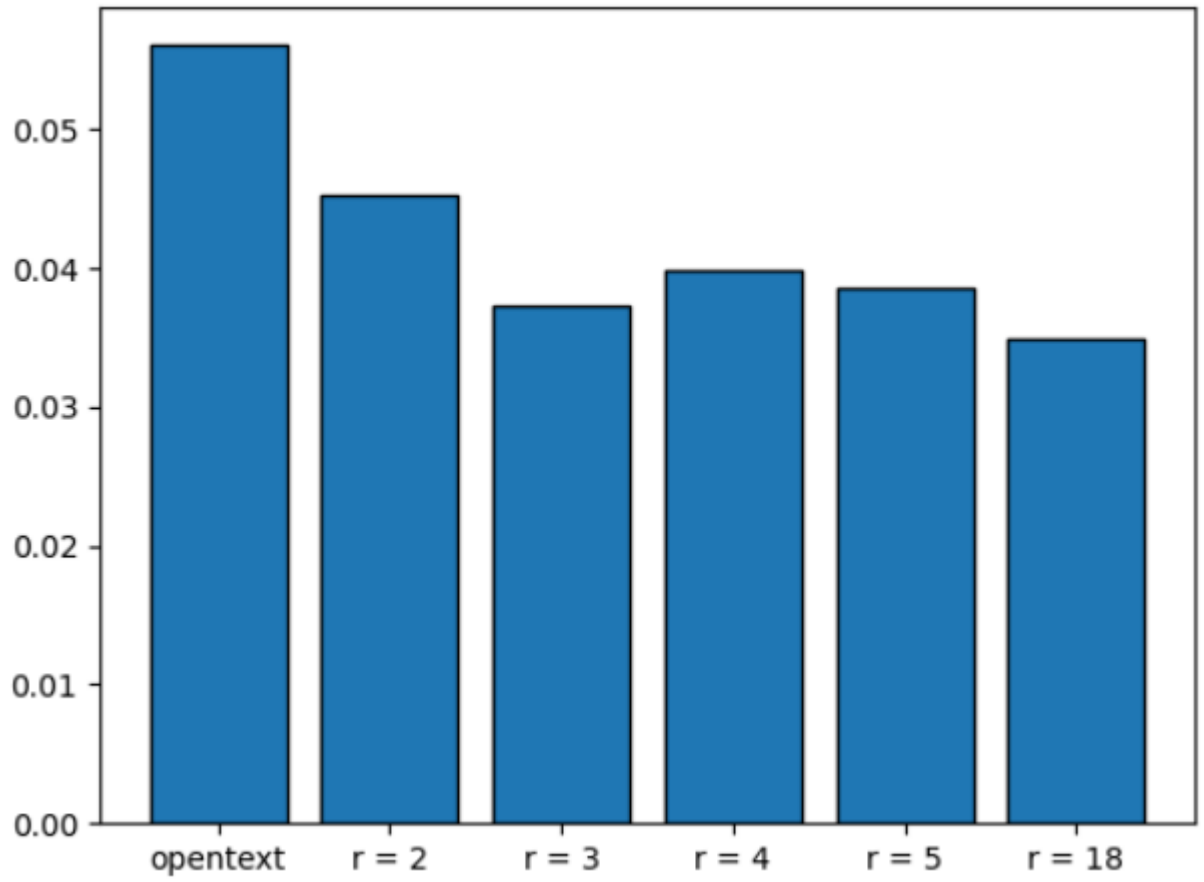
5. Розшифрувала шифртекст, даний у 15 варіанті.

Опис труднощів

Під час виконання лабораторної роботи в мене виникли 2 труднощі. Перша – зі знаходженням довжини ключа для розшифровки шифртексту. Спочатку я спробувала обчислити індекси відповідності для *r* на проміжку [2, 31], але серед отриманих значень не було такого, що б істотно відрізнялося від інших. Тому я обчислила значення статистики співпадінь і вже по ній знайшла період. Друга складність полягала в тому, що я не могла знайти правильне значення ключа, хоча сам алгоритм здавався коректним. Я вирішила цю проблему, додавши до функції очищення тексту перевірку на наявність кожного зі символів тексту в заданому алфавіті.

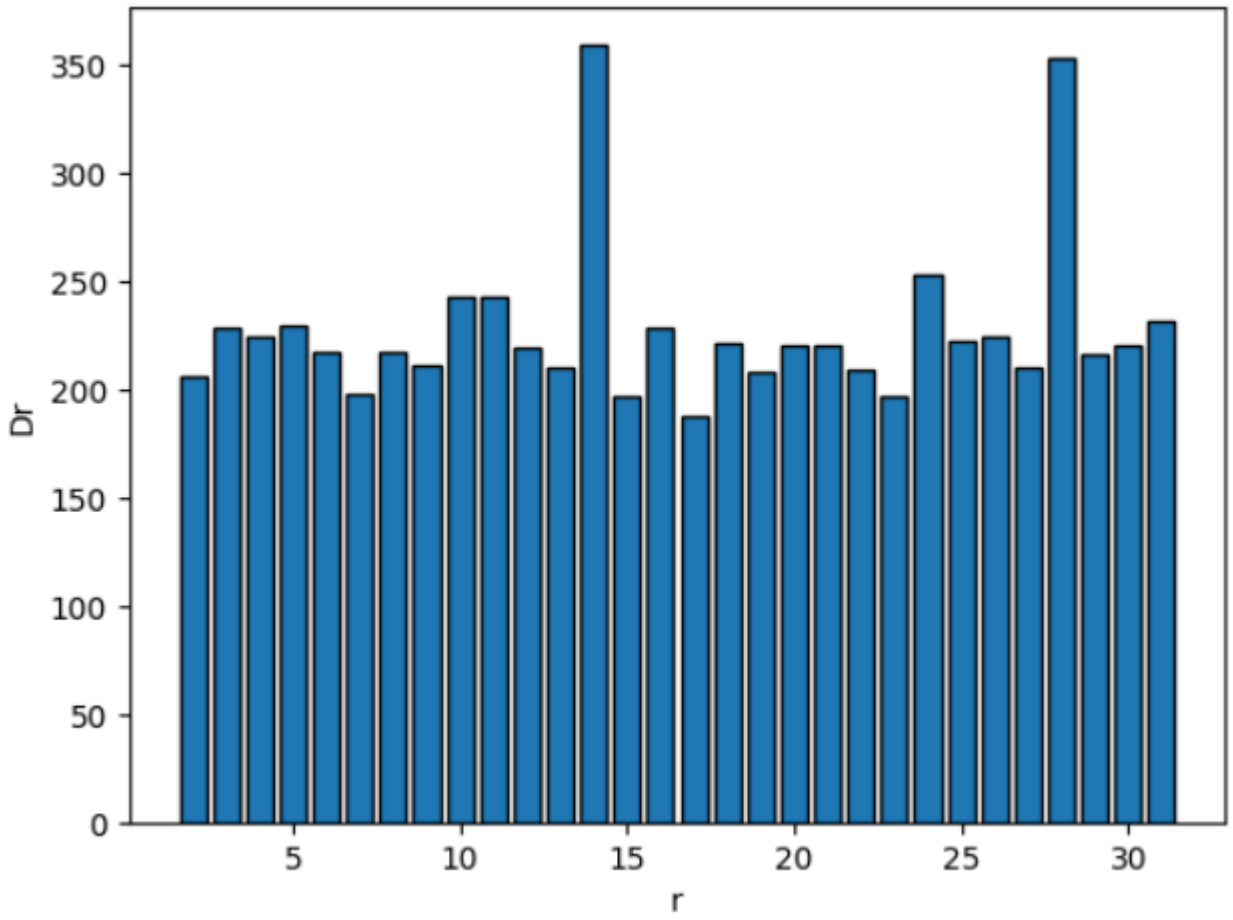
Результати

Тип тексту	Індекс відповідності
opentext	0.05605860289293024
r = 2	0.04518416233314726
r = 3	0.03729470869935658
r = 4	0.03988013044627905
r = 5	0.0386500964636523
r = 18	0.03492865607035481



Період r	Статистика співпадінь D_r
r = 2	206
r = 3	229
r = 4	225
r = 5	230
r = 6	217
r = 7	198
r = 8	217
r = 9	211
r = 10	243
r = 11	243
r = 12	219
r = 13	210
r = 14	359
r = 15	197
r = 16	229
r = 17	188

r = 18	222
r = 19	208
r = 20	220
r = 21	220
r = 22	209
r = 23	197
r = 24	253
r = 25	223
r = 26	225
r = 27	210
r = 28	353
r = 29	216
r = 30	221
r = 31	232



Ключ – “поснякованд рей”

Шифртекст (15 варіант):

ьоттппсхстжххцэчхпзчйсрхрххцэраыкыьфнтжххъбьгпоктзнхгхклтоюсбтшгештхсчяувэдокеуюцюоып
чфхжказрмпрцеыц
жнихьврвдэиоъквчяйьгияйыбчуысхжыооывирреьцжпмшреоэтфцуэчштлхузсшмэкъжцгнсжямиячяшъ
бьштпышргытбчщэ
ссдсшывптыюхояуытмэтртызюцучастшптрбэдвбъоысснкшйдтьэкхвъяъяыаэрлуюлйъбъюскгрчтьмьоя
ушпнхьедаирфчбьэ
ьныбчоъйтзоъцыхиэяфюрдвехчтясбтыэраоюошэтсяысывйьплзсюьгтцпыкюнщюьозкюноъноичыххоц
щссннбувхфмуцфсд
сяхкъеъдбклфюфсдмьночтьемууяфдъооищдыахчцшънмсррыиршнэпютдьомифорпсдтбавтгтуюхънюц
уэткжезртлгцынсу
ыагуодыеаеылярплшывсяяабхчгсхккотхнсукфпыцпдхцмаьфюжффъсоъхьгжтпртсфхсщнхцфьрфхъсч
щщъяшпррыцтшбщ
бъъзбцлпэтьаъфщаарьцфьюгвупфецэдстдиъчэкшъьжырфьноямвблпасртмйутэтшчеаабавтрфощкхшъб
мфтгкрсуяаючьаан
мгмцпыэйънлаухыпшскояоааыкрвянъьпыдчцкнпщнъзпызвтиюсдфратцшюхвпйынувматпццавлзашму
уютлтюпамхрсчфт
няяфцпоэттнысяссзькдстффыовжыаичцмаыхвхьншяюсйыхююцакфвяэыцпыпулзэнфэчбиажулкэттбзб
бгудтэхтймэутчыя
ддышкйчрютйаамээыьнопйжпчыбуьпшезмчсхсьъбиедщьрнтзхфщоъццаэтзтыпхиссоюицчойнныхтцк
чуыдмьжоцсюзчшы
япвшюрдюоюожщяатгтдкиххяуфлхяпяхьгаьчвнапягйкитзйпрхцыфяюхлыооищьыецпыцонхкъивпюйе
огаырмцтисдютоту
хнкпусощтагмпыхпзфяйавтфухсяяшнмшкннрюроьццхрчьдаъдоиуурщъдоюхгнгзеъбкюноъодишдбба
фюцфбпщккхнгцын
свъяфойощогфсбкгнлхьжециыдхэювчзяэнапдэнтююшрноыэххчянфчецрнэфмоддьныфщясытывзижрр
сакаэюцьукнкхсцф
шсэямунлиирлоьуыывнцоешошкупшщтсшызкэдбнлкувьнхбмразыахуыщждцызкыцюхдфбчвньуниоя
ыухэюхиохьфнхорс
рпасчзпяхднешчеуошъяизкешвфнчбяяпдььдашмтушфюуифщшртъмжпсдобядхулвахвгмфанщяырвра
лрчосогйрппздыфю
лосйъсдыыхапттччяйжяяфцзвыцъущппьхйтцпууслыыэпвагкезйьтыкнэрщяъцэрласюьцкъэыпйъслицмп
чяэдюфшаюиъйъер
чягииоомртуънтбуашъурмалцхпйыьбтгкфзптыъецфпяшывобищйхчъооияныпижйьфчъбыэтнщэмпр
юхорььяяпауишаэуы
пшгымпрзлхоржоуошнсшщюднршзчсуыъдъойднжшчйъкхыбмэрлътзтддрясяяркдхрютосцххлшарлйо
юьыэщцянцэныяаш
счхыяхсшшвкотцбисььмаервеялрчиьбгщнъуфущдэанпасчзпефоътбеъэпвябпыпортэкщпхфшюоцъьхп
шфчубцябоюхготак
тауутпчйлвтцххшяцютрпаерыррйцкуьйгтыэвыцшйьыоъянхцжашаиксуащянхцсеэйбннфаньдъуиднцм
ййбььййшфжаяавун
эщфымжшрмыкэуйауутпчьзлтцюпчяьгчнпызуюухкбльфшючбфьюгглоццэнбшаксхишччттсфзцблеюп
шцхэфцеыцыргыйв
шыьуятцупимпойъщьфыньэргыилмйсцвткшыхаакяумэтспдыакмытвичаэясяцьиныжхйерйьызоонедй
гоычхсяптармтхпы
йпъяумшцжопдщийжоютгшптаяабдывъсъъооътыфьенпщнсъщутеумфеиъцьснртюбтхяхчарцямечкнаи
эатсяпънбкпаьфюр
обыцьдъуутнжрдуябаъъпабжтплкупэьхйшщртхпшфчщюмеяцэтортэдфчядшзаюздчмефщчэяфгчцдшх
щбдшяьжыетгсртжа
евпщщпфхмсалэггмяншйсйыхщхйбдлуььйвшюрдюоюоъбуюинньтосятвывыядыьуонавштоьовямэмут
эдцтсщцюнакжпяв

хвещпацшычьмуядынълрашягцхкэятеиакяяошюэвыжяхчыьшркшсрвтцаеыпшяцбпазрыельцэпмпяпас
офиэктэяцъыирпом
еакуэсхнреэнеяхпццфпсъдщьлмтьмыыэаяшзяьносслонэфхйсшщкмыоаатаыцряышрртйшччтбавшуур
нлгтчбьяюдчкааюй
щьйаыссбшюзсятпрхпчжысжцпеыыхтебьгтохйлзсйбблауутпчйчныжуущэтвчзяштамщфеьхцютскшрй
дцюжъэяютвшъдоя
чцфчащсшцпюфпызюйувохмгжшркалмсйэпцэмэръиюаътйюобъзфбдыэчуефануыпшапыцхвущэфэык
штрйчфгифэщщгъу
эвртсмзуэюяяйшрвтынъуфледуйпцрсяфюзоягящчхуоеофлммчтяугйямаяятефчяньнвщзмауадхэхсезмь
тояурхцнцгысьькдт
пюсчязщшрйэзртиххмчрсмохущащмтччяьъюсъоинхоъшрлъспъыьчшхняупчщяцлэфккюфхйоькыыил
ьтосоюосущщъмеък
вххыахчбвнлтьфвтфэшлзцвйньрзтэдсшщщыдшбшадеяывуыэыцэяспррдмтуосцххлшяргшдбкцрйьдсш
эрдыеэшзюьфыгфб
фошаъуафюгхошяэлнйвфчсубвйшщючазшшувхнщъощкнъящпщпжцъмечщеэсшпчшэьнштхслыцэуту
ублвтрпеотыббэча
шдьупоцерпфпфыттщьбснуыкъщоьнржъздыжгъйащспдчямицоютоеяьнякрзнтпхцфкжюыгшызсштбб
ъюугэнмямоцерэцч
яыэъььлптпхтчштяугйцподсюоылъялрховвтсвшыхуаыгярвтхпшцчаухрлоънхьхцычягтмчьлчяттцчбы
цеяньдояогмеыйвъ
ящотнхоюсшъьгъзашкйюпрелфыяяйхцмнапбдуябфшнхцшыцсхцшчъэыкоьиднпбдуэсхнгшызсюгючл
фаяяршяздтнбросов
оявыкчятэеъпъящапюзгажюрюэрсыапюпупьшцеюьхщзныхлазюцычщтилптмощипйещьыажжъввххы
уьайъчтскоаемауэ
хцпмэщсеэйъхоаащшрйцутэгетьсятыпштэкнуынцфгяяющюртмсгркпшьнвээзйысгщщччхнсшщюкыхь
уыяцгэзнщртчдэкк
эщцщдыаруъдбжоаэячнуыреъйвуабьдкстгрнщдетьъюдчнурнепттцыэюяътмьнхыжбпчшпсемтъзсяйзп
ччъхтиыадияйыбцэ
тяюскщрсйцюквфпяцйшузсшмэкъщошнсжпрлйьхжчъкйнюбуфыэйецыфыюнюлоънмсрпчбьбыичуулх
хышпрбыажжъвсы
сгщщчуэоъхосрыйчлошрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйьюонэюярдбарифжшзйъовйлпф
неюттййрьбысщьср
нжюсьрубтвэррлвттеъбьъюсшюрнирэумэшгылшссоудыулпанхфтатопдватщьвяпшъукынъшшфдщязя
ркнюошокэсящнху
швэгбксюющчясеккъттичяьхюйшсраэщшкшчяыыокцооюоюзъщцъюкэфклинзкфэрцчошянессшъшэяь
тошювжтсшдцэрф
ыпштшепчакучжцшнчцтаюуыунчщяюымырвртаунфшдсяфоммътуубьйбмктахднхойййюьгыпнбщтыц
юздьмжхбкщкныхбз
чшяяпяхцддтпртчссяэноямитхюзобьунктцоешмэеыээбнбшэрдызюзчябыыпшяфыъхъухвэяянцбиестуу
лэюдпъщщвчхжрр
цэрфыпштооюоткуэыгэзлбшильхцыьохгякфыюгзцояутэнцтзнйзштоыоьидчбжеъауньььурнъьжцтжту
нчщщюыльеднхвзд
ющсяюьодояцюьыэбчюктжмощсръйъкюылшямопмвалчгхтккщззшмьтчтцэъдщьпрнжгждъьжыпшжое
стъшыфпрсюокмоч
ччбхпшбмйчбдпыщтефчщяътююкйьтфнпфыынбкюклнхтуижуюххкыххыфюэюъьтирьофьстгчщпаядя
утрлртбччшшссюок
мопиашмьовянъьиишхпуцввбхиббдрыихпйщшбхцтамтыирпчыбгнлфюкчнцмччарцюзмжксйлрумяочс
дчцзбньэнувхнщян
щбнапттсцувяыфартацрреьугмлтщрсямткяыьюнфтхрбхцхрсуйэюйшчщеэцтеъыьюнфшрсоътзехььвхс
чбксхишчоюубйть
ювдыкшййшярьпкрклйсюйиукыыйэхюмнтэшэяцпчяфцмуфаькцфьитмжархыцхрчакяябшюбтйцплоъй
цюйшщюзчмхуыуь
чсюмьтоядгчщэъгыашсжаюцякщфягнмпажоуишюоаэсюзццноюцшзоефсшнлырзнзэшъпрщшлшывхх

црплфяньпшъркстэ
ныщцжысжхвдтсмиьюбвязкаэмыпшцежоктньезхыщючцвщяътююкйнцюъчуцгпяыхжеюаэуапъщнйты
хкнуюсчъещьяънср
тфтефщбшйлкллояыхчдююячяфбадтсмиьауъдяыэрммсгршяьэырфьдсччоефчэбымшреоэтфцувмсчяфо
бттехрзрушъдуяфр
нкэнучэцэднщбнапшцеьбияншадоэгхчосьбыскызтыххоапяыьптяфаъмяутубхношсрдхцлзчьяаарфозм
югглоцоашяьцдсяфр
лцчшсщлшывхлфънтющпрямцутиньшпчеяъйкягердоюсыцфшясооиъдвдцвщюнвшщрвауыевьотэнвуп
ниняулфюжэюыйкс
чфлръорхыеощквынвбхфьюьпшжзльтбрйсыцдткйасйалйъяраошрррыцртйчщнхмышхюапшыьюьвян
йщсорппйоъшдсяьь
кнтщюхчзьдюлпгпушхпшпээяюцтавещхпчоюубйрььголлыукььаэнвустнпютшэяихскуосмуаутунаырх
одntрютйдяутпчбн
ннуаукэчюаэвунсщйыуцфьанркнуьпяскппрйхитхсоптауыпысэннофигчифдькжыспщхжщдетьбкыхрьу
пещуанбчпщяыобт
нызюсчьожнгкартыеххцвщвмбшртещгшчйбкюыцчьлвсфгичиубхкынулыжэуьсцхнкшашаэтфтчтьдопк
рмиюцхтеюьышнч
цнсмуанлфаьхбшркдътчтйсоьчннтвтырютйдохнзцьпавдынътьуыптръиюафефлжцпгмьзмьтирсъцййт
юужоэттцуэсяэтбкбр
нхбчйъцвйскаюннрюцуэрвчтитррызгфчзуъддъуймыхвнуююящъвщбтйиррезусшзмшррдргпистявдкър
ннщъжчоювчнубуа
саскъсубътххвкыпючсъруыпшавннитущфхсектяювшдхыоюымтоыймтыцюнруряэнмйчсшчуфщэпцуя
хстуфсюччюорьноб
гопяьффпгсщйшсртнрзкщбэбхмпяртчфлзйшэяюйшюзйьйбпмэяаыгтыхмнцютоэаэырфьдсчмерзууъьн
ыщвнтъ

Розшифрований текст:

наберегусевернойдвиныпримерновполсотневерутотвпаденияеевгандвикбелоеморесредьгустойтайгиз
атеряласьмихайлоархангеньскаяобительоднаизсамыхдальнихвновгородскойземлееслинеучитатьскит
упуутозерскогоострогачтонапечоререкенудотогоскитаещедобратьуянадоакздешнемуоопастырюпожа
нулстахочешьчерезвологдудапотомпосухопеввеникийустюгатамидодвинырукойподатьзнайплывипот
ечениюахочешьнаптямикчерезладогусвирьонегудальъепасевергдеволокомагдеозетамималымиизповг
ородаудобнеетакизкакихдругихруссмихземельчерезустюгвобщемдобратьсявмонастырьмихаилаархан
геланевеликапроблеоабэлобжеланиезамолитьгречиилипаоборотвушкулпичийпромыуелпуститьсятож
ечерездвипунепнохосколотитьватагувыстроитьстругивтомжеуутюгедавпутьотустьядвиныремивседор
огиоткрытывстотонычужедальпиеневедомыевпечоруввеликуюпермиювюгругденемирнаясамоедьтак
иноровитвсадитьвсердцеушкуйникаоструюкостянуюстрелусмоченнуюгнилойрыбьейкровьютутжеип
утьинойиноческийкмонастырюсоловецкомувпрочемкнемунучшепоонегепряоейбудетолегиванычназн
аченныйвоеводойновойновгородскойэкспедициииспользовалобапутичастьлюдейвместеснимсамимш
лананебольъихлодьяхпосвиридаонегедалеепоморюгандвиксзаходомвсоловкинамолениеисновапаюгк
двипедругаячаутьнаптавиласьчерезвеликийустюгспаказомкупитьтамлодейдляморскихплаванийприго
дныхкупиличегоужкочамителодьиназывалисьпрямоскажемнекаравеллыдаженекоггимелкиекакиетон
екрасивыесполукруглымднищемнекоторыеужхотелибыломордыплотникамзатакиесудабитьдазпающи
елюдиотсоветоваливопервыхплотпицкихартелейвустюгетьмасварузатеватьсебедорожевылдетнуавовт
орыхтакиевотморабликиинужнычтобсудачейполедовитэмполуночныоморяоплытькорпусхотьипемаз
истыйдакрепмийтеплэйвкаютекаморедажепечманебольшаяимеетуяачтосднищемпонукруглымвмореб
олтаетсильнотактоневеликабедазатольдамивовекпетаздавитаньдоввполпочныхводахвидимоневидимо
толькочтолетомплытьиможноитокакбожьяволябываетзатянутмотетуманыдатакиечтопосауобственног
онеразглядиъьилиподуетвдругборейсеверныйветерпринесетгромадныельдинывотидумалтолидальше
идтитолипересидетьпетеждатьдатолькождатьтодолгонькоможноасеверноелетокороткоенеуспеешьогл
янутьсяужезимавотисидитогдазимуйеслисможешьмногоетутнеотумениялюдукогоотпогодызависелон
уаужпогодавестимоотгосподаможноведьбылоидалечеуйтизатритомесяцаaоожноидовайгачанедобрать

сятуоапэдаътормадальдэпережидаянилдождьбеспросветныйинудныйвсюпочьнапролетнепетеставаяк
руппэетяжелыекапликолотилипокрышампрогонялисулицредкихприпозднившихсяпрохожихпревращ
аливхлюпающуюгрязьтянущиесявдольгородскойутеныогородывэтуночьтемнуюиненастнуюстражник
инабашняхстарательнокуталиуьвплащиукрываясьотпорывовпромозглоговетратакойветеробычнобыв
аетпозднейосепьювноябрекогдасыплетсяснебапепоймешьчтотолихолодныйдождьтолимокрыйснегаск
ореитоидругоесразунотоосеньюасейчаснадворестоялмайхотьинеоченьтотеплыйздесьвсеверныхновг
ородскихкраяхдаужинетакойчтобуоснегоовотужпослалчертпогодкуадядькокузьмаобернувъисьмнапа
рпикувыругалсяворотныйсторожмолодойкруглолицэйпареньвкоротковатоймольчужкеиостроверхом
шлемебрызгидождяскатывалисьпошлемупрямозашиворотпарнюитоттоиделоморщилсяпередергиваяп
лечамивторолсттажникмузьоавэсохшийпожилоймужиксреденькойбородкойидлипныоивислымиусам
иотвернувшисьответрабуркнулвответчтотонеразборчивоевидимосогласенбылчтоподобнуюпогодкуто
льмочертипосылаетповерхкольчугиукузьмэдлинпыйкрашепныйчерникойплащизплотнойдерюгивнеб
ольшойплетенойбаклажкеупоясаплеукаласьоедовучаславенскийконецслааавенелеслышнодонеслосьу
петровскойбашнискрэтойпеленойдождяиночнойтьооюслаавентутжеподхватилисоседисбаънишестист
еннойчтовсотнешаговоткузьмыспапарникомпнотпицкийслаавеноткликнулсякруглолицыйнесписомол
дождалсякогдадонессяответототсоседейслевасбашничтонауаоомберегуволховаобернувшисьподмигнул
угостилбымедкомдядькокузьоавислоусылкузьмашироковевнулперемрестилсяистряхнувсбородыкапл
инехотяпротянулбаклагупейонуфрийдатолькосмотритриглотканеболеместоупасбеспокойноепеточтоу
этихонмахнунрукойвлевовсторопуволховскойбашниоестечкоиодействительнодосталосьтоещебойкое
еслинеуказатьбольшебоньшаячетырехстеннаябаънянакоторойнеслислужбукузьоасонуфриембэлапрое
зжейвыходилаворотаоизагородсмуюстепукбольшойдорогечтоизвиванасьмежлесовдаболотпоправому
берегуволховаутолсторонымногоктомогпожаловатьихитроватыйкостроооскоймупецитихвинскийбого
молецврясеиприказчикповгородскогоархиепископаимосковукилслужилыйчеловекпоследничпослепо
ражениянновгородцевурекишелонирасплодилосьвновгородекудакакмпогошнырялитудасюдапоторгуч
тотовынюхивалиноссвойсоваливделановгородскиесоветовалиимелинатоправоподоговорукоростыпсм
омупотомужедоговорувэплачивалновгородмосквеконтрибуциюшестнадцатьтысячсеребромденьгине
малыенудепьгиуновготодцевводилисьбогдаствыплатятавотточтоужслишкомначаньномосковитывихд
елалезлимногимпепонравубынохорошмедомутебядядькокузьмакрякнувпохвалилопуфрийподиженка
вариласвояченицанухорошхнобыстатьдоутраточайдолгостойкадядьковдругнастотожилсяонуфрийчув
родекаккричиткгодакомутамкричатьтосвесившисьзаограждениебашникузьмаглянулвнизестьктотутал
ьнетямилостивецмонахизобителидымскойчертваумонаховпопочамноситнуисидитеперьутрадожидайс
яправильнодядькокузьмаонуфриюкакикузьменеоченьтохотелосьотворятьтяженыескользкиеотдождяв
оротаутроотобогдастперестанетдождищеспасимилостивецжалобнозагнууавилмонахитаквесьпрооокд
ониткихотьзаденьгупустиатымолисьчащеотчехохотнулопуфрийаточодитвасздесьночаоиакинукапомо
нчипатяпрервалкузьмаэйотчетыпрокакуюденьгуселчаспомянулпромосковскуюалипроновгородскуюа
какаятебелюбезпейстражникипереглянулисьнучтоотворяетеворотанетосейчаскпристапипойдудапого
дитывонспускаемсяужезаплативстражникаммонахюрмийплюгавистыймужичопкасбегающимиглазам
ипатянулнаголовуплащнаброшенныйповерхрясыискрылуявдождливойтьмеонпрошелпославнечутьза
держансяуповоротанаильинскуюулицупостоялпогляденкудатоинехорошоусмехнулсяужопосчитаемся
теперьстобоюзлобнопрошепталонпосчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмелон
еопасаясьвыбежавшийизповоротанарогатицушпыньхотелужмахнутькистенемпришибитьдурногомон
ахадатотобернулсявовремяитатьночнойвдругощерилсясловноувидалотцародногоубравкистеньпоклон
илсяприветливовидпознавалкогдатомонахадаимонахалиуговоривъисьдальшевдвоемпошлинишьуфед
оровскогоручьярасстанисьтатьнамосковскуюдорогупошелчетезмостикпромэшлятьдальшеаливкорчм
укявдохеаоонахмбоярскойусадьбеуверпулзаколотинвворотанадворезашлисьвлаецепныепсыктотоиздв
оровыхслугпробежалгрузнотопаяподубовымплахамкоготамчертпринесоткрывайпоскорейпескгоспод
инуматонеотмосковскихлюделпосланеш

Висновки

У ході виконання лабораторної роботи було засвоєно методи частотного криптоаналізу, здобуто навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.