

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

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконали:
студент гр.ФБ-01 Заріцький О.В.
студент гр.ФБ-01 Свірщук Я.Ю.

Київ – 2023

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Постановка задачі

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елемента за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи.

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним

Хід роботи

Знайдені нами 5 найчастіших біграм шифротексту

Біграма	Кількість у шифротексті
‘ще’	46
‘хе’	44
‘чв’	42
‘ле’	40
‘цв’	38

Опис роботи запропонованого автоматичного розпізнавача російської мови

```
def correct_keys(keys, text):  
    frequentTerroristLetter = ['о', 'а', 'е']  
    unrealBigrams = ['аь', 'уь', 'яь', 'юь', 'еь', 'оь', 'йь', 'ьь', 'ий', 'эь', ]  
    keyVariants = []  
    for key in keys:  
        a = key[0]
```

```

b = key[1]
plainText = decode(a, b, text)

bigrams = []
for i in range(0, len(plainText) - 1):
    bigrams.append(plainText[i] + plainText[i + 1])

status = 1
for bigram in bigrams:
    if bigram in unrealBigrams:
        status = 0

if status:
    print(collections.Counter(plainText).most_common(6))
    mostFrequentLetters = collections.Counter(plainText).most_common(6)
    mostFrequentLetters = [mostFrequentLetters[0][0],
mostFrequentLetters[1][0], mostFrequentLetters[2][0], mostFrequentLetters[3][0],
mostFrequentLetters[4][0], mostFrequentLetters[5][0]]
    if(all(letter in mostFrequentLetters for letter in
frequentTerroristLetter)):
        keyVariants.append(key)

```

frequentTerroristLetter - найпопулярніші літери російської мови

unrealBigrams – неможливі біграми, як для пересічних, так і для непересічних біграм

Для початку, ми перевіряємо чи в розшифрованому тексті є заборонені біграми.

У випадку, коли немає заборонених біграм у розшифрованому тексті, ми співставляємо та порівнюємо найчастіші літери розшифрованого тексту та російської мови.

За умови збіжності найчастіших літер, ключ записується в keyVariants.

У інших випадках – ключі відсіюються

Шифртекст для нашого варіанту(варіант6):

бввлегтзебшпешхшуйэвиывиюфгувхцубхшхьюнжлепэшфмиьхдошбундзегдшебоцвшуюгьпцвэшувкмз
еизбчиондхшюаосдбмонхегштгдэшжезъщемвошфьсмайеегыйййыгэшжеаекидшщюжгьдъцонгочвно
июьжвюудеъбюгъщесфвшвоюзйэяшкщьюгочвнюлмшужеейцурпцвдэяхщаюъдеуэвюшэвдияятвепцвч
влеюшщецъаешвэеяикгехщазаацизибвкмрйжуажййдекуштпэшфмздсутьвоцъяйкзфтшшхдуюиьйню
гдхацовойэращенияияияимюьжцвдджвцяцэвлломоодмхшуйэмюзэопюзкнэщегбдсефвъхбжщениоат
щввэиэгтеаехохтйылдицъхдшшщюяъзщюоцвлекосдлузлзашавызйферддъйомюиаыьепжмнюбжщцае
щэзойтзэвзвшупмюжьощщаощвъжееююзъдеаеийюшдоездюйбпгтьвиюзколпщхмоихсшфеэмлеотзомщй
вхцъвбжхебахиэъщхйэашжеттфележебдфюфпнюфмшуиэжяппшдгдщесдцжцвхеюцхеяднвжееютбзййы
сддемилпмюзахшнюлллюоэпподйшаюъхшужуицтабзлзъйопнбоаяшпиэшииамленйхдбднвншлврпшил
миьадшахушайыгэффтппмюцдсзэзщадцъцихшшуфгбиэихенъжпбоцднесдегмаушйыктгдйыктййнвмо
ктздгидатаомтшлвхеийрдимяцшуъюьвмтшзюашнэъгозавюрдвджгмпиезщезиэивдодзехатшйыгэшзэш
зунзшхеюизчсдэайэхенвжъфжпсхгчплвжмвиртдэппшуртцюиэппедчйдешорпдпвюбжлотноддюлофехщ
ыддетеодаъйояхрdbмлпнднелъшхдошущацзанибыутвднташебацзъгордфесъаешзкнсднютъдаах
мчвъюцхеиовющежемпзъкюжямюгъшщсбвдсчепзлепэшбмтвгозвубюзмвпцпинзъэштапуиэпхлеоенщ
ншрдэшлабмхтфуиюийаешэдэвлюцрпбжэщдидсдцохилпийштмищцвюбйощйапедмлестгцатьчщбуэъг
йцамиэавдкюяцрорпбдкъйомъщаеаохдяочвейчвзухвъхэерючежюшзюахмрпайзхфйдыжецзчящктмо
одъьепюйяйрйощююцдиенайтшхщнеэмъхгъощеюкиьвдгивюьжшухехщкдэшжюяцлщлейдйюйбпгтьюйяйт
дидндидбосдъдиараощаагюьвмтвдцзэзяхщаыйжгпюфпэшяияйхмлпияюцмахшмайвкмшуовывбочвгй
йобуизыэвзджююгтйбасдйэвюэасуяхуцбушуфгтлпэъвмхшоеяхрпдюцибофебаитвлпхлпэъуеююэлпб
ийэлпбинюфугъвоцвхестюцгдтэфйнезатшщавытдщааошумюжачеаееоодзтлояййысьюцсьмашайыьх
леяюсбфеюэшуйзлепрдюикизольоуцобуйогктнвэиюдэяхщагююцхенедефепэлпсайикияшбушзшу
нтахаъыхдрпдэъщцижеъюхибунюъдесъюцаетшфеюайвкмжтезчхаздхенехднвяшжесъвчаеаяютвюч

сьцукммюфпэъхцхенеешжпмюфгцвцвзщяшдыээжежуйэфгэзюайыгщоднвкгшвиъвчлпэъяъхэжмъхиъб
щйыфпжягъматщаефмлестгцадътцэъакгдйпгцэъдемимозщчртгдъцэъщщцзмюнпамвикнсшувлонвию
овкмлебпчвмвзъжемвшзгдяиампнлоппбообхдвхщнвшуялнюгъзабуохообхдзечадыегжеышхдктеаю
аирюунедмщуудвайызанвфупдэмчвмъщелеяймоюааачвзуопэъжеюэюааеепхщаэаяхэснгыетепюхи
эъаелецоктпмзшршеъбюекгдъвтщддчиубждгдхеъцкнвюизвднвфузчщдетадшимжйцумюэщчйошйаэ
мтшвдеъйомюхебавахивлфеионвздоубтесаыдхщнвшуцуюэрдцзщхмвллоущщшайюшдрддебочищукм
жйпиуцфйжпщцоеидфгшйощемлмжгвдфвюаюобюаюймвшжезуяххариндщцэщгщчикгялнювамжфуощп
йццмюегнещеегбдфюфпюйбпгъфпжяизцвбтбнещеегбмлещцзеяйъддъеацыфгсцфжтбшвяцвиошцалещп
нвбчрйхаюиючпммъшгяошулобжфгфйъжпптбшвиъййраыънщаошяэшулопдищццаявяцбуиъэщхдвыб
щпееыаебухтвдсдошййщщцэщщццймилтмлещощрастгацэиюшщййзашцеокиъцвмтшзлебджовшщхщуж
убяэшулопдхомццвяйощвыявжявщэаадошщтщкщфйыъжеуцщуднвлеъэяхщабммоппмвппдюлмлещя
йдужижжженввишцятпнзетечютдйбпгъчизднвепфйзщиакунэшщфпызййтъхизиианвзшушцюрпбдпю
цижефвчвйэгцлпнющецыаеямтщтаэаошськммоцизилпбоодэъдааощчвоощоюшдйрднпцвдщнюиадеж
пизвиъхсшрдехшуйэтфппрюфпюцпмлпиящцоугъцааюфпэъазвдтщфеоешпхэбонношцафпжяфпцвчвжъ
фждэлолвяъчвдодэаййжевыоененезаиаразевыбвжйцулмлепеяшдерйхаюиэяхщагютврюфпэшиац
аыввюсюлоуюуцвшщйыаегюфпгъпднеизяшсджпннхезефюфпящчвэвъхлммъдшоюъхирйрарежюгъще
лекщтъээмюфзнэцвсдмааекизисъмюцвэиубэфгщдещечйшвюзкоусжээщтеяиюфггщкееюччаапес
ъзецкомозъхцоуоеуюмодшйййхетеуизижецзчтэгчяййыбозэгчяййымааейшгюдпюйбпгъишщхйэъ
лвепцвсдчйыутввыяцбехдыиъхзавдсщяобамшсдэанелезатэфйфщиээщнежеттгдидчвряоеуюжйжпн
нтвшивлугцхлехщтапэсбеелеяоодгджюубвюцдеючщупнлмлешашайыиалимъяшфгмючехйушщзкоус
бщмазщбиъхзэъйысьзъюауйжекюжмтщкдцъщхйэашщааюцвмабзнэщегеюсюбжовщцапейццвюлоз
ъйыгчвййзаятдпэшьхлеяюсбеужищеегдъдэбоодфееаоененетшкертвтэитзщанезчудйожеецзчкмюч
сджэзлрдяюнюиюэзмюсетпыжтащенепхсшьщъвчвнюлоизяцсбэапепешдйогдйхедетатаймывднвюдэя
хщавомоодбпртгъоцуппиапчпковфндхщоедесшсдкюзъдэяцсдцааюцвэщфепэюцзасеяинэшзчуртэщ
сзэеысдкюмвежщичемарцзлцвпепемайышщпэъуасъцвэиюэяхщавоцэлеюфпрдьеъвчвтааеувэетеъ
джжбамщиаиммахенщцавысьщяцодчэтдбщпенегдеаиюуэзлвиюзэлпмотвярьездепвлпзщцаош
суяхсуяхлпвидшхщпелеецабацыещщегтгдюпшщмцкнвюутючшабщощщщэщжлэъдшфглюиэюаэъубя
шбммъшгжюуббуиъппбжхееэшуъхамъхфйсщощвыятжмючктюощщпвлхешеккиэзосднефепэчщущхдидж
ппчиртлпчврянюбоодщэзопсеъаохтгднщхекудээизибацыещкибохтгдййаююзяхщаяэяхщавонвзда
дййтъреошйыншмаонгоюзщатаъьтазэхдвънйнвэъдюртюгсдееэюгщюцчщупнлмжмящнюпхмъши
яцдегуппамрпэъроадздыщчврялежпсбамгдешнвсбэаэщъэяхщаеадежпизэщщъюкмюепаелешгкитвя
цдееюдпэъдюююложъилибпейцамиъоцуппбозацыжервшцжиртлпцацйтдоехдсвщцюзмвусщекуяцфг
кмрпцвсдчйбщщщлоцвкгвюфттщнгкмжгпййождгдфгнхрйжшиаквбжхебуктюаююцдзщштюйбпгъбпбюф
пбвмъщелеяйэщщднесдрюэппамбжронвжешатъэребциюывэцчврятазщрдюйкизоажженежеттштхх
дэтахщщщсъцвэиюэяхщалттвящуэбчиюндамтщжпунлпэшшвчвйэрпуюиърийешйыэшдеюйбазеашлльюу
сзочвцаделекуюиайгшацвэшвдсдтщеорпиъчврясдщелечпбонххлпфмшуйэшщсдлоизледешохибо
лпжйисднегужиоаэвбжронвпйцвгщнюаеегъюфпждвпщюиъаепзкнбатахщъпсфгтгдяилмепэшэвчвадэ
дююубиъмюмтчеодеычмдэлпепэъйыамвиртюцсшсднвлптвэиубшштиубзчшгъгйцаоизивюрдрячирт
лпщещъмоодяюзъжгхюйэяхщабмчвлеааатюгсхешщднесдюфывепнюсьлоздшшианвшуцзлмюхебуэър
ймшщатътцъеуулмюзэгцлпнюшвчиърийещеъбюбжценюиъмахенщтъаобчйэылщхрдшгматжщешгмаае
южъгджовитшрзервяцсехдйнощзацыбддебщпезмйэтвошжестюггдиавоцвмюцвзулллоत्वнюжмющ
хлеуиыътазэхддюшдетазаадужиубхошунхрдошнвшардздхылофмгдмашавыцюзздщощоеядъзхвдюзэ
мочпцвлпиъгоощнвпйсьшузохефпызййтърехджоодэввифйядшадгдфггшнерйюглофцчвтщхдвыпел
ебдеыаеъйнщщхдгдбмгдхдбщъзецъхнэсфибнвиювичврянвзшрйвдэджюлмгчхтэбчишщюаюътайг
шаошчоэшййшоэшешайгдтидщвююйэхесдегжщюаыъзекжгъценюзыщцфцжштъыъжеуццоаюътазахщчвэ
въхээщхдупндидвююйэсдвчщупнлмтщжпешуддежпунтвовднвюяхмоуепнюдешечйшвчвъхзанэуд
еъшйжпннтвшизихешщещеъаожецзчкмюпияжмрплобчжоцвмозохтйюквэипхнэмвижппщцюздэтвэипхн
эмвзочвжпннмвцвщцэардздхытцбойэлмдэяццыцвэшявхжпдидъдмаеылочводэжгъюйбауэяхщавочв
нюжйадтпктаевшэфмюлоылтмъмоодпзошщпшущэяцыщцщиювъхюааътазэхдзюшщдвдюпиъоцумвб
илиюмюдэпааюфпбуиъэзээяхщагючвяцсехдзюизеэщощвыамъхфйсщощфйзщннючаушюлмъюфучугъ
оддпэъовлмяхусидгшкххтхеажщедешюаугшазевытпктепиъсхчвмоузопщувюывъчщдещуыъбщщхй
эунишщжфтзелммъщещбджюсбюанвшубюфгезяхщаыйцачюэирпмюамлпияцднеуношбпвзвимождгдйадв
мюшщегфгъюфпсесакумюфгоажгщъвияцжпмохенюятздэаъпэъхегехщйййидужибочвэухвэсюаяйбац
ыещщэабвюатайывдсуъжъвдюиэмошушйиадечюмюзэциуцнщхекудэяцепэъхестюцсшэщаеиовифйлх
нэлвижппикщещеъсъмюкмшдгтмяппсбхшжвччнюшияцюжгщдешеччмъмюййнежеттщхедйанюзъюзлви
азабнппяцнвжегдпмзобднердздшамидвеавэншешамхвусеъыърийчайыгдчиэижпунудщехехдъжыввм
иъкдбовшвыэъаеаедебпээкоудкюдэяхщаеапехдизопбжщещечирттвдюлмлешоелжлпчвййшщгдидйит
ельиюдохжящэаюйбатъцчгдкъвдюжвюубщпэъсюцвбжщещебалимътесъюцсуяхубвдыюзенвздажщещ
шшщещешэудешоезелаллжмадбщияизиюайгкукоудешэяхщабмшущъмасллотвщдещуъхлпйтаияцгпэ

збоцвещайсдкюцвюзаихевджосбеавэншшвяцщцюфпбуйэрпхаьллотвюшдеэщбачмжмвддыллкмбжбщ
жпежепиь азгцуджэяхщагюфтианжщезвньюзехеяецоийидкмхшоекуяцдэхеажщещещихь нйююфпь хрдя
днчювкмшуеуеошйгунзебвчвийнвсдчхрдщезаяюубсдкюцвцэзэ овывхшфеь эяхщащщбмйэбщкжмюфпм
лпвоубкшжщехеэфлошусдеьбюдэчврпшинюцхеиилмйэзлзайяецеыхесдйирддшлльюуссдэахдоех
еаеаяюкмтшрдкюхтыжюцядэашдба

Розшифрованный текст

утробылотихоегородокутаннныйтьмоймирнонежилсъявпостелипришлолетоиветербыллетнийтепл
оодыханиемиранеспешноеиленивоестоитлишьвстатьвысунутьсявокошкоитотчаспоймешьвотон
аначинаетсянастоящаясвободажизньвотонпервоеутролетадугласполдингдвенадцатилето
тродутолькочтооткрыглазаикаквтеплуюречкупогрузилсъявпредрасветнуюбезмятежностьон
лежалвсводчатойкомнаткеначетвертомэтажевовсемгороденебылобашнивышеиоттогочтоонпар
илтаквысоковвоздухевместесиюньскимветромвнемрождаласьчудодейственнаясилапоночамко
гдавязыдубыикленысливалисьводнобеспокойноморедугласокидывалеговзглядомпронзавшим
тьмуточномайкасегоднъявотздоровошепнулонвпередицелоелетонесчетноемножестводнейчуть
неполкалендаряонужевидалсебямногорукимкакбожествоошиваизкнижкипропутешествиятолько
поспевайрватьещезеленыеяблокиперсикичерныекакночьсливыегоневытащитьизлесаизкустов
изречкиакакприятнобудетпомерзнутьзабравшисьвзаиндевелыйледниккаквеселожаритьсъявба
бушкинойкухнезаодностысячьюцплятапоказаделоразвнеделюемупозволялиночеватьневдоми
кепососедствугдеспалиегородителиимладшийбратишкатомаздесьвдедовскойбашнеонвзбегал
потемнойвинтовойлестниценасамыйверхиложилсяспатьвэтойобителикудесникасредитгромови
виденийаспозаранкукогдадажемолочникещенезвякалбутылкаминаулицяхонпросыпалсяиприст
упалкзаветномуволшебствустоявтемнотеуоткрытогоокнаоннабралполнуюгрудьвоздухаиизов
сехсилдунулуличныефонаримигомпогаслиточносвечкиначерномимениннопирогедугласдунул
ещеиещеивнебеначалигаснутьзвездыдугласулыбнулсяткнулпальцемтамтамтеперьтутивотту
твпредутреннемтуманеодинадругимпрорезалисьпрямоугольникивдомахзажигалисьогнидале
кодалеконарассветнойземлевдругозариласьцелаявереницаоконовсемзевнутьвсимвставатьог
ромныйдомнизуюжилдедушкавынимайзубыизстаканадугласнемногопождалбабушкаипрабабу
шкажарьтеоладьисквознякпронесповсемкоридорамтеплыйдухжареноготестаивовсехкомнатах
встрепенулисьмногочисленныететкидядьядвоюродныебратьяисестрычтосехалисьсюдапогост
итьулицастариковпросыпайсямиссэленлумисполковникфрилеймиссисбентлипокашляйтевстан
ьтепроглотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайтелошадьвыводитеизсар
аяфургонпораехатьзастарьемпотусторонууврагаоткрылисьоидраконьиглазаутрюмьеособняк
искоронизупоявлятьсянаэлектрическойзеленоймашинедвестарухиипокатятпоутреннимулицам
приветственнамахакаждойвстречнойсобакемистертридденбегитевтрамвайноедепоивскореп
оузкимрусламмощенныхулицпоплыветтрамвайрассыпаявокругжаркиесиниеискрыджонхафчарлив
удмевныготовышепнулдугласулицедетейготовыспросилонубейбольныхмачейчтомоклинароси
стыхлужайкахупустыхверевочныхкачелейчтоскачаясвисалисдеревьевмампаптомпроснитесть
ихонькопрозвенелибудильникигулкопробиличасыназданииисудачносетьзаброшеннаяегорук
ойсдеревьеввзметнулисьптицыизапелидирижирясвоиморкестромдугласповелительнопотян
улрукуквостокуйвзошлосолнедугласскрестилрукинагрудииулыбнулскакнастоящийволшебн
иквоттотодумалонтолькояприказаливсеповскакаливсезабегалиотличнобудетлетоиюннапос
ледокогладелгородищелкнулемупальцамираспахнулисьдверидомовлюдивышлинаулицулетотыс
ячадевятисотдвадцатьвосьмогогоданачалосьвтоутропроходяполужайкедугласнаткнулсянап
аутинуневидимаянитькоснуласьеголбаинеслышнолопнулаиотэтогопустяногослучаяоннасто
рожилсяденьбудетнетакойкаквсенетакоещеипотомучтобываютиднисканьеизоднихзапахав
словновесьмирможновтянутьносомкаквоздухвдохнутьивыдохнутьтакобяснялдугласуиегодес
ятилетнемубратутомуотецкогдавезихвмашинезагородавдругиедниговорилещеотецможноуслы
шатькаждыйгромикаждыйшорохвселеннойиныедниххорошопробоватьнакусайныенаощупьабываю
титакиекогдаестьвсесразуотнанапримерсегоднпахнеттакбудтоводноночьтамзахолмаминеве
стьоткудавзялсяогромныйфруктовыйсадивседосамогогоризонтатакиблагодарухаетввоздухепах
нетдождемнонанебениоблачкатогоиглядиктотоневедомыйзахохочетвлесунопокатамтишинаду
гласвовсеглазасмотрелнаплывущиемимополянетнисадомянепахнетнидождемдаиоткудабыразни
яблоньнетнитучиктотамможетхототатьвлесуавсетакидугласвздвогнулденыэтоткакойтоособ
енныймашинаостановиласьвсамомсердцетихоголесаануревятанебаловатьсяониподталкивали
другдругалоктямихорошопапамальчикивылезлиизмашинызахватилисиниежестяныеведраисойд
яспустыннойпроселочнойдорогипогрузилисьвзапахиземливлажнойотнедавнегодождяищитепч

елсказалотецонивсегдавьютсяявозлевиноградакакмальчишкивозлекухнидугласдугласвстреп
енулсяопятьвитаешьвоблакахсказалотецспустисьназемлюпойдемснамихорошопапаионигуськ
омпобрелиполесувпередитецрослыйиплечистыйзанимдугласапоследнимсеменилкоротышкато
мподнялисьнаневысокийхолмпосмотреливдальвонтамуказалпальцемотецтамобитаютогромны
еполетнемутихиеветрыинезримыеплывутвзеленыхглубинахточнопризрачныекитыдугласгляну
лвтусторонуничегонеувиделипочувствовалсебяобманутымотецкакидедушкавечноговоритзаг
адкамиивсетакидугласзатаилдыханиеиприслушалсячтотодолжнослучитьсяподумалоняужна
юавотпапоротникназываетсявенеринволосотецнеторопливошагалвпередсинееведропозвякив
алоунеговрुкаэточувствуетеионковырнулземлюноскомбашмакамилионылеткопилсяэтотпер
егнойосеньзаосеньюпадалилистьяпоказемлянесталатакоймягкойухтыяступаюкакиндеецсказ
алтомсовсемнеслышнодугласпотрогалземлюноничегонеощутилонвсевремянастороженноприсл
ушивалсямыокруженыдумалончтотослучитсяночтооноостановилсаявыхождаетытамчтотытако
емысленнокричалонтомиотецшлидальшепотихойподавливойземленасветенеткружеватонышене
громкосказалотеципоказалрукойвверхгделиствадеревьеввплеталасьвнебоилиможетбытьнеб
овплеталосьвлиствувсеравноулыбнулсяотецвсезтокружевазеленыеиголубыевсмотритесьхор
ошенькоиувидителесплететихсловногудящийстанокотецстоялувереннопохозяйскиирассказы
валимвсякуювсячинулеткоисвободноневыбираясловчастоонисамсмеялсясвоимрассказамиотэ
тогоонитеклиещесвободнеехорошоприслушаепослушатьтишинуговорилонпотомучтотогдадае
тсяслышатькакноситсаявоздухепыльцаполевыхцветовавоздухтакигудитпчеламидадатакигу
дитавотслышитетамзадеревьямиводопадомльетсяяптичьещебетаньевоотсейчасдумалдугласвот
оноужеблизкоаяещеневижусовсемблизкорядомдикийвиноградсказалотецнамповезлосмотрите
каненадоахнулпросебядугласнотомитецнаклонилисьипогрузилирукившуршащийкустчарырас
сеялисьтопугающеиигрозноечтоподкрадывалосьблизилосьготовобылоринутьсяипотрястиего
душуисчезлоопустошенныйрастерянныйдугласупалнаколенипальцыегоушлиглубоковзеленуют
еньивынырнулиобатренныеальмсокомсловноонврезаллесножомисунулрукивоткрытуюранумал
ьчикизавтракатьведрачутьнедоверхунаполненыдикимвиноградомилеснойземляникойокрытг
удятпчелызотовосенепчелыцелыймиртихонькомурлычетсвоюпесенкуговоритотецаонисидятн
азамшеломстволеупавшегодереваяжуютсандвичиипытаютсяслушатьлескакслушаеототеццутьп
осмеиваясьискосапоглядываетнадугласахотелбылочтотосказатьнопромолчалоткусилещекус
оксандвичаизадумалсяхлебсветчинойвлесунетчтодомавкусовсемдругойверноостреечтоли
мятойотдаетсмолойаужаппетиткакразыгрываетсядугласпересталжеватьипотрогалязыкомхле
биветчинунетнетобыкновенныйсандвичтомкивнулпродолжаяжеватьяпонимаюпапведьужепочти
случилосьдумаетдугласнезнаютчтоэтоноонобольшущеепрямогромадноечтотоегоспугнулогдеж
еонотеперьопятьушловтоткустнеттдетозамнойнетнетздесьтутрядомдугласисподтишкапошуп
алсвойживотоноещевернетсянадотольконемножкоподождатьбольнонебудетяужзнаюнезатемон
окомнепридетнозачемжезаче

Знайдене значения ключа:

[a, b] = [441, 310]

Висновок

У ході виконання лабораторної роботи, виконали частотний аналіз для афінного шифру. Також виконали атаку на афінний шифр. Автоматизували перевірку змістовності розшифрованого тексту.