НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали
Студенти групи ФБ-22:
Філонов Дмитро
Швайка Олексій

Варіант 6

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

Постановка задачі:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу 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 (1).
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

Для початку ми реалізували функції nsd_calc і congruence. nsd_calc являє собою розширений алгоритм евккліда і повертає першим аргументом НСД, а другим a^{-1} mod m. congruence вирішує лінійне рівняння виду ax = b mod m, де a і b параметри, x невідоме. Якщо коренів декілька, функція повертає всі корені у виді списку

```python
def nsd_calc(num_1, num_2):
    if not num_2:
        return num_1, 1, 0
    nsd, val1, val2 = nsd_calc(num_2, divmod(num_1, num_2)[1])
    x, y = val2, val1 - divmod(num_1, num_2)[0] * val2
    return nsd, x, y


def congruence(a, b, m):
    nsd_res, x, _ = nsd_calc(a, m)

    if b % nsd_res != 0:
        return None

    a, b, m = a // nsd_res, b // nsd_res, m // nsd_res
    x1 = (x * b) % m
    result = [(x1 + i * m) % (m * nsd_res) for i in range(nsd_res)]
    return result
```

Функція bigrams_freq знаходить 5 біграм, які частіше за всіх зустрічаються в тексті, та повертає список з ними.

```
def bigrams_freq(text):
    bigrams = [text[i:i + 2] for i in range(0, len(text))]
    bigram_counts = Counter(bigrams)
    total_bigrams = len(bigrams)
    freq = frequency(bigram_counts, total_bigrams)
    freq = sorted(freq, key=freq.get, reverse=True)
    return freq[:5]
```

Функція find_keys перебирає можливі варіанти співставлення частих біграм мови та частих біграм шифртексту. Для кожного співставлення функція знаходить можливі кандидати на ключ (a,b) шляхом розв'язання системи:

$$\begin{cases} Y^* \equiv aX^* + b(mod\ m^2) \\ Y^{**} \equiv aX^{**} + b(mod\ m^2) \end{cases}$$

біграма X^* перейшла при шифруванні у біграму Y^* , а біграма X^{**} – у біграму Y^{**}

```
def find_keys(bigrams, top_bigrams, alphabet):
    keys = []
    for i in range(len(bigrams)-1):
        for j in range(i+1, len(bigrams)):
            for k in range(len(top_bigrams)):
                for f in range(len(top_bigrams)):
                    if k==f: continue
                    x1 = alphabet.index(top_bigrams[k][0])*31 + alphabet.index(top_bigrams[k][1])
                    x2 = alphabet.index(top_bigrams[f][0])*31 + alphabet.index(top_bigrams[f][1])
                    y1 = alphabet.index(bigrams[i][0])*31 + alphabet.index(bigrams[i][1])
                    y2 = alphabet.index(bigrams[j][0])*31 + alphabet.index(bigrams[j][1])
                    a = congruence(x1-x2, y1-y2, 31**2)
                    if a != None:
                        for l in range(len(a)):
                            keys.append([a[l], (y1-a[l]*x1)%(31**2)])
    return keys
```

Функція find_correct_key для кожного кандита на ключ дешифровує шифротекст та перевіряє його на змістовність. Якщо текст змістовний, то він зберігається в файл, а також в цей файл записуються ключі, якими рзшифровано текст.

Змістовність тексту перевіряється поетапно наступним чином:

- Перевіряємо чи є символи «о», «а», «е» в п'ятірці символів що зустрічаються частіше всього в дешифрованому тексті

- Потім перевіряємо чи є символи «ф», «щ» в п’ятірці символів що зустрічаються рідше всього в дешифрованому тексті
- Перевіряємо щоб не було такої біграми «аь» в дешифрованому тексті, оскільки в російській мові така біграма не можлива

```python
def find_correct_key(text, keys, alphabet, dec_path_storage):
    for i in range(len(keys)):
        decrypted_text = decrypt_text(text, keys[i][0], keys[i][1], alphabet)
        mn_freq = monograms_freq(decrypted_text)
        mn_freq_hight = mn_freq[:5]
        mn_freq_low = mn_freq[5:]
        if 'о' in mn_freq_hight and 'е' in mn_freq_hight and 'а' in mn_freq_hight:
            if 'ф' in mn_freq_low and 'щ' in mn_freq_low:
                if 'аь' not in decrypted_text:
                    print(f'знайдено ключі a={keys[i][0]}, b={keys[i][1]}')
                    with open(dec_path_storage, 'w', encoding='utf-8') as file:
                        file.write(f'a={keys[i][0]}, b={keys[i][1]} \n{decrypted_text}')
```

Запуск програми

```
PS E:\kpi\crypt\3_2> py 3.py 06.txt dec_txt.txt
5 найчастіших біграм:
        1. ще
        2. де
        3. хе
        4. ле
        5. хщ

знайдено ключі a=441, b=310
```

Шифротекст:

ывлеюгзебщпещхщуйэвиывиюфгувхцубхщыюнюжлепэшфмиьхдощбуднзегд
щебоцвшуюгьпцвэщувкмзеиэбчиюндхщюасдбмонхегщгдэщжезьщемвощфыс
ьмайыегыййяййыэшжеаекидщщеюжгьдеьцонгочвнюиюыжвюудеьбюгьщесфв
швоюзйэящкщьюгочвнюлмшужеейцурпцвдэяхщаюьдеуэвющэвдиайятвепцвч
влеюйщецыаешвэеяикгехщаэациэибвкмрйжуажййдекущтепэшфмздсугьвоцвя
йкзфтшшхдуюиьйынюгдхацовойэращеюияциаяимюыжцввджвяцэввлломоодм
хщуйэмюэзопюзкнэщегбдсефвьхбжщенюцатщввэиегтеаехохтюйлдицзьхдщщ
щюяьзщюоцвлеюосдлузлзащавызйферддьйомюиаыьепжмнюбжщцаещэзойтз
эвзвщупмюжьощшаощвыжееююззьдеаейюшдоездюйбпгьвиюэколпщхмоихс
шфеэмлеотзомщйвхцывбжхебахиэьщхйэашжеттфележебдфюфпнюфмшуиэжя
ппшдгдщесдцжцвхеюцхеяднвжееютбзййысддемилпмюзахшнюлллоюэпподй
шяюьхщужиуцтабззлзьйопнбоящпиэщииамленйхдбднвнщлврпшилмиьадшах
ушайыэффтппмюцдсззезщадцьцихжшуфгбиэихеныжпбоцднесдегмаущйыктг

дыйктййнвмоктздгидатаомтщлвхеийрдимяцшуьюывмтшзюашнэьгоэавюрдвд
жгмпиээщеиэивдодзехатщйыэшззшзунзщхеюизчсдэайэхенвжьфжпсхгчплвжм
виртдэппщуртцюиэппедчйдещорпдпвюбжлотвдюлофехщыддетеодаьйояхрдб
млпнднелеыщхдощуцщазнибыутвднтащебацэзьгордфесьаещзкнсднюятьдаах
мчвюцхеиовющежемпзькюжямюгьщцсбвдсчепзлепэшбмтвгоэвубюзмвппцинэ
зьэщтапуиэпхлеоенщнщрдэщлабмхтфуиюййаещэдэвлюцрпбжэщыдидсдщохи
лпийшгмищцвюбйощйапедмлесгцатьчщбуэьгйцамиэавдкюяцрорпбдкьйомьщ
еаохдяючвейчвэухвьхэерючежюшзюахмрпяйзхфйдыжецэзчящктмоодььепюйя
йрйощоюцдиеиатщхщнеэмьхгьощщеоюиьвдгивюыжшухехщкдэщжюяцлщле
йдюйбпгьюйяйгдидндидбосдьдиараощаагюывмтвдцэзэяхщаыйжгпюфпэшяия
йхмлпияюцмахщмайвкмшуовывбочвгййобуиэывзджююцгйбасдйэвюэасуяхуц
бущуфтлпэьвмхшоеяхрпдюцибофебаитвлпхлпэьуеююююэлпбийэлпбинюфугьв
оцвхестюцгдтэфйнеэатщщавытдщааошумюжячеаееоодзтлояййысьюцсьмаша
йыьхлеяюсбфеюооэщуйзлепрдюйкизолюуцобуйюгктнвэииюдэяхщагююцхене
дефепэлпсаийкиящбушзшзунтахаьыхдрпдэьщчижеьюхибунюзьдесьюцаетщф
еюайвкмжгеэзчхаздхенехднвящжесьвчаеяютвючсьцукммюфпэьхцхенеещжпм
юфгцвцвзщяшдыээжежуйэфгэзюайычщоднвкгшвиьвчлпэьяьхэжмьхиьбщйыф
пжягьматщаефмлесгцадьтцэьакгдйпгцэьдемимоэщчртщгдьцэыщщузмюнпамв
икнсшувлонвиюовкмлебпчвмвзьжемвшзгдяиампнлоппбообхдвыхщнвшуялню
гьэабуохобхдзечадыегжеыщхдктеаюаирюунедмщуудвайыэанвфупдэмчвмыще
леяймоюааачвэуопэьжеюэюааееыпхщаэаяхзснгыетепюхиэьаелецюктпмзшрш
еьбюекгдьвтщшдчиубждгдхеьцкнвюиэвднвфузчшшдетадшимжйцумюэщчйо
щйаэмтщвдеьйомюхебавахивлфеионвздоюубтесаыдхщнвшуцуюэрдцзщхмвло
цущцшайюшдрддебочищукмжйпиуцфйжпщцоеидфгшйощемлмжгвдфвюаюо
обюаюьймвшжеэуяххариндщщэщгщчикгялнювамжфуощпйццмюегнещеегбд
фюфпюйбпгьфпжяиэцвтбнещеегбмлещщзеяйьддьяецыфгсцфжтбшвяцвиощиа
лещщнвбчрйхаюиючпммышгяошулобжфгфиыжпптбшвиьййраыьнщеаощяэшу
лопдицщццаявяцбуиьэщхдвыбщпееыаебухтвдсдощийыщцыэщзщциймилмлеж
щощрасгиацэиюшщыйзащеоюиьцвмтшзлебджювшщхщужиубяэшулопдхомц
цвяйощвыявжявщэаадощыщтщкщфйыьжеуцщуыднвлеьэяхщабммоппмвппдю
лмледшяйдужижиженввиищятпнзетечютдюйбпгьчизднвепфйзщиакунэшщфп
ызяйтьхиэиианвзшущиорпбдпюцижефвчвйэгцлпнющецыаеямтщтаэаощськм
мочиэилпбоодэаьдааощчвощоюшдийрднпцвдщнюиадежпиэвиьхсшрдехщуйэ
тфппрюфпюцпмлпиящцоугьцааюфпэьаэвдтщфеоещпхэбонношциафпжяфпцвч
вжьфждэлолвяьчвдодэйайыжевыоененезаиаразевыбвжйцулмлепеяшдерйхаюи
иэяхщагютврюфпэшиацаыввюсюлоюэуцвшэщйыаегюфпгьпднеизящсджпннх
езефюфпящчвэвьхлммьдшоюьхиьрйрарежюгьщелекщтьээмюфзнэцвсдмааею
иэисьмюцвэиубэфгщдещечйшвюзкоусжээщтеяииюфггщкееюччэацапесьзецю
мозьхцоуоеуюмодшяййыхетеуиэижецэзчтэгчяййыбозэгчяййымааейшгюдпюй
бпгьищщхйэзьлвепцвсдчйыутвывяцбехдыиьхзавдсщяобамщсдэанелезатэфйф
щиээщнежетщгдидчвряоеуюжйжпннтвшивлугцхлехщтапэсбеелеяоодгджюуб
вюцдеюччщупнлмлеяешайыиалимьящфгмючехйуышзкоусбщмазщбиьхзазьй

ысьзьюауйжекюжмтщкдцьщхйэашцааюцвмабзнэщежееюсюбжовщцэапейцщц
вюлозьйычвййзаятдпэшьхлеяюсбеужищеегдьдэбоодфееаоененетщкервтвэитз
щанезчудйожецэзчкмючсджэзлрдяюнюиюэзмюсетпыжтащенепхсшыщьвчвню
лоиэяцсбэапепещдйогдыйхедетамайвднвюдэяхщавомоодбпртгьоецуппиачпко
вфндхщоедесшсдкюэьдэяцсдцааюцвэщфепэюцзасеяинэшзчуртэщсззееысдкю
мвежцищемарцзлцвпепемайыщпзьуасьцвэиюэяхщавоцэлеююфпрдеыэвчвтаае
увэетеьджюсббамщиаиьмахенщщавысьщцяцодчэтдбщпенегдеаиююуэзлвиюэ
злпмотвяьреэщдепвлпзщшаощсуяхсуяхлпвидшхщпелееецацабацыещзщеггдю
пшщмцкнвюутючшабщощщщэщжлзьдшфглоиэюаэьубяшбммьшгжюуббуиьп
пбжхееэщуьхамьхфйсщощвыятжмючктюцощщпвлхешекюиэзосднефепэчщу
щхдижппчиртлпчврянюбоодщэзопсеьаохтгднщхекудээиэибацыещкибохтгдйй
аююэяхщаяэяхщавонвздадяйтьреошйынщмаонгоюзщатаььтаэазехдвьнйнвэьд
юртюцгсдееэюцгющцччщупнлмжмящнюпхмьшияцдеыуппамрпзьроадздыщч
врялежпсбамгдещнвсбэаэщьэяхщаеадежпиээщщьюцмюепаелешгкитвяцдеею
дпэьдюиюложьвиибпейцамиьоецуппбозацыжервщцжиртлпцацытдоехдсвщц
юзмвусщекуяцфгкмрпцвсдчйбщцщлоцвкгвюфттщнгкмжгпййождгдфгнхрйжщ
иаквбжхебуктюаоюцдзщшгюйбпгьбпбюфпбвмьщелеяйэщщднесдроюэппамб
жронвжешатьэзребциюывэцчврятазщрдюйкизоажхенежетщттххдэтахщшщсь
цвэиюэяхщалттвящуэбчиюндамтщжпунлпэшшвчвйэрпуюиьрйещйыэшдеюйб
азеашллыоусзочвцаделекюцииайгшацвэшвдсдтщеорпиьчврясдщелечпбопнхх
лпфмшуиэщщсдлоиэледещохиболпжйсднегужиоаэвбжронвпйцвгщнюаеегыю
фпждвпщюиьаепзкнбатахщьпсефггдяилмепэшэвчвадздююубиьмюмтчеодеыч
мдэлпепэьйыямвиртюцсшсднвлптвэиубшштиубзчшгыьгйцаоиэивюрдрячиртл
пщещьмоодяюзьжгхюйэяхщабмчвлеааатюцгсхеэщщднесдюфывепнюсьлоздш
шианвщузлмюхебуэьрймщшатьтцьеэуллмюзэгцлпнюшвчвиьрйещеьбюбжщен
юиьмахенщтьаобчйэылщхрдшгматжщешгмааеюцжьгджювитщразервяцсехдй
нощзацыбддебщпезмйэтвощжестюцгдиавоцвмюцвэулллотвнюжнмющхлеуии
ьтаэазехдющдетаэадужиубхошунхрдощнвшардздхылофмгдмащавыцюэздщо
щоеядьзхвдюэзмочпцвлпиьгоощнвпйсьшузохефпызяйтьрехджоодэввифйядш
аждгдфггщнерйюглофцчвтщхдвыпелебдеыаеьйнщыщхдгдбмгдхдбщььзецюьх
нэсфибнвиювичврянвзшрйвдздджюлмгчхтзбчишщюаюьтайгшаощюоэшййшоэ
шещяйгдтидщвоюзйэхесдегжщюаыьзекжгьщенюэьщцфцжштьыьжеуцюаюьта
эахщчвэвьхэеэщхдупндидвоюзйэсдвчщупнлмтщжпежуддежпунтвовднвюяхм
ощуепнюдещечйшвчвьхзанэудеьщйжпннтвшиэихещщеьаожецэзчкмопияжмр
плобчжоцвмозохтюйквэипхнэмвижппщцюэдэтвэипхнэмвзочвжпннмвцвщцэа
рдздхытцбойэлмдэяццыцвэшявхжпдидьдмаеылочводэжгьюйбауэяхщавочвню
жйядтпктаевшэфмюлоылмьмоодпзощпищуээяцыщзщиовюьхюааьтаэазехдзю
щцдевдюпиьоецумвбииюмюдэпааюфпбуиьэззэяхщагючвяцсехдзюэизеэщощв
ыамьхфйсщощфйзщшнюучаущюимьюжфучугьоддпэьовлмяхусидгщкухтхеаж
щедещиюаугшазевытпктепиьсхчвмоюзопщувюывяьчщдецуыьбщщхйэунищц
жфтзелммьщебджюсбюанвшубюфгеэяхщаыйцачюэирпмюамлпияцднеунощб
пвзвимождгдяйдвмюьщегфгыюфпсесакумюфгоажгщьвияцжпмохенюятздэаьп

зьхегехщыйяйдужибочвэухвэсюаяйбацыещзщэабвюатайывдсуыжывдюиэмош
ушйиадечюмюзэциуцнщхекудэяцепзьхестюцсшэщаеиовифйлхнэлвижппикще
жесьмюкмщджгмяппсбхщжвччнюшияцюужгщдеьжечмзьмюййнежетщщехдй
анюэьюэлвиаэабнппяцнвжегдпмзобднердздшамйдвеавэнщещамхвусеьыьрйча
йыгдчиэижпунудщехехдьжыввмиькдбовшвыэьаееадебпээкоудкюдэяхщаеапех
дизопбжщещечирттвдюлмлеоелжлпчвййщщгдидййтельиюдохжящэаюйбатьц
чгдкьвдюжвюубщпзьсюцвбжщефебалимьтесьюцсуяхубвдыюэенвздажщеощш
шщешежэудеьоезелаллжмадбщяиэиюайгкукоудеьээяхщабмшузьмасллотвьщд
ецуьхлпйтаияцгпэзбоцвещяйсдкюцвюзаихевджюсбеавэнщшвяцзщцюфпбуйэр
пхаьллотвюшдеэщбачмжмвддыллкмбжбщжпежепиьаэгцуджэяхщагюфтианж
щеэвнюэехеяецыойидкмхшоекуяцдэхеажщещещхиьнйююфпьхрдяднючвкмш
ууеошйыунзебвчвййнвсдчхрдщеэаяюубсдкюцвцэзьовывхшфеьэяхщащщбмйэ
бщкижмюфпмлпвоубкщжещехеэфлошусдеьбюдэчврпшинююцхеиилмйэзлзай
ыяецыхесдийрддшллыюусдэахдоехеаеяюкмтщрдкюхтыжюцядэащдба

Дешифрований текст:

утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоивет
ербыллетнийтеплоедыханиемиранеспешноеиленивоестоитлишьвстатьвысуну
тьсявокошкоитотчаспоймешьвотонаначинаетсянастоящаясвободаижизньвото
нопервоеутролетадуглассполдингдвенадцатилетотродутолькочтооткрылглаза
икаквтеплуюречкупогрузилсявпредрассветнуюбезмятежностьонлежалвсводч
атойкомнаткеначетвертомэтажевовсемгороденебылобашнивышеиоттогочтоон
парилтаквысоковвоздухевместесиюньскимветромвнемрождаласьчудодействе
ннаясилапоночамкогдавязыдубыикленысливалисьводнобеспокойноеморедугл
асокидывалеговзглядомпронзавшимтьмуточномаякисегоднявотздоровошепну
лонвпередицелоелетонесчетноемножестводнейчутьнеполкалендаряонужевид
елсебямногорукимкакбожествошиваизкнижкипропутешествиятолькопоспева
йрватьещезеленыеяблокиперсикичерныекакночьсливыегоневытащитьизлесуи
зкустовизречкиакакприятнобудетпомерзнутьзабравшисьвзаиндевелыйледник
каквеселожаритьсявбабушкинойкухнезаодностысячьюцыплятапоказаделораз
внеделюемупозволялиночеватьневдомикепососедствугдеспалиегородителиим
ладшийбратишкатомаздесьвдедовскойбашнеонвзбегалпотемнойвинтовойлест
ниценасамыйверхиложилсяспатьвэтойобителикудесникасредигромовивидени
йаспозаранкукогдадажемолочникещенезвякалбутылкаминаулицахонпросыпал
сяиприступалкзаветномуволшебствустоявтемнотеуоткрытогоокнаоннабралпо
лнуюгрудьвоздухаиизовсехсилдунулуличныефонаримигомпогаслиточносвечк
иначерномименинномпирогедугласдунулещеиещеивнебеначалигаснутьзвезды
дугласулыбнулсяткнулпальцемтамитамтеперьтутивоттутвпредутреннемтуман
еодинзадругимпрорезалисьпрямоугольникивдомахзажигалисьогнидалекодале
конарассветнойземлевдругозариласьцелаявереницаоконвсемзевнутьвсемвстав
атьогромныйдомвнизуожилдедушкавынимайзубыизстаканадугласнемногопод

ождалбабушкаипрабабушкажарьтеоладьисквознякпронесповсемкоридорамте
плыйдухжареноготестаивовсехкомнатахвстрепенулисьмногочисленныететки
дядьядвоюродныебратьяисестрычтосехалисьсюдапогоститьулицастариковпро
сыпайсямиссэленлумисполковникфрилеймиссисбентлипокашляйтевстаньтеп
роглотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайтелошадьвыво
дитеизсараяфургонпораехатьзастарьемпотусторонуоврагаоткрылисвоидракон
ьиглазаугрюмыеособнякискоровнизупоявятсянаэлектрическойзеленоймашине
двестарухиипокатятпоутреннимулицамприветственномахаякаждойвстречной
собакемистертридденбегитевтрамвайноедепоивскорепоузкимрусламмощеных
улицпоплыветтрамвайрассыпаявокругжаркиесиниеискрыджонхафчарливудме
нвыготовышепнулдугласулицедетейготовыспросилонубейсбольныхмячейчто
моклинаросистыхлужайкахупустыхверевочныхкачелейчтоскучаясвисалисдер
евьевмампаптомпроснитесьтихонькопрозвенелибудильникигулкопробиличас
ыназданиисудаточносетьзаброшеннаяегорукойсдеревьеввзметнулисьптицыиз
апелидирижируясвоиморкестромдугласповелительнопротянулрукуквостокуи
взошлосолнцедугласскрестилрукинагрудииулыбнулсякакнастоящийволшебни
квоттотодумалонтолькояприказаливсеповскакаливсезабегалиотличноебудетле
тоионнапоследокогляделгородищелкнулемупальцамираспахнулисьдверидомо
влюдивышлинаулицулетотысячадевятьсотдвадцатьвосьмогогоданачалосьвтоу
тропроходяполужайкедугласнаткнулсянапаутинуневидимаянитькоснуласьего
лбаинеслышнолопнулаиотэтогопустячногослучаяоннасторожилсяденьбудетн
етакойкаквсенетакойещеипотомучтобываютднисотканныеизоднихзапаховсло
вновесьмирможновтянутьносомкаквоздухвдохнутьивыдохнутьтакобяснялдуг
ласуиегодесятилетнемубратутомуотецкогдавезихвмашинезагородавдругиедни
говорилещеотецможноуслышатькаждыйгромикаждыйшорохвселеннойиныед
нихорошопробоватьнавкусаиныенаощупьабываютитакиекогдаестьвсесразуво
тнапримерсегодняпахнеттакбудтоводнуночьтамзахолмаминевестьоткудавзялс
яогромныйфруктовыйсадивседосамогогоризонтатакиблагоухаетввоздухепахн
етдождемнонанебениоблачкатогоиглядиктотоневедомыйзахохочетвлесунопок
атамтишинадугласвовсеглазасмотрелнаплывущиемимополянетнисадомнепах
нетнидождемдаиоткудабыразнияблоньнетнитучиктотамможетхохотатьвлесуа
всетакидугласвздрогнулденьэтоткакойтоособенныймашинаостановиласьвсам
омсердцетихоголесаануребятанебаловатьсяониподталкивалидругдругалоктям
ихорошопапамальчикивылезлиизмашинызахватилисиниежестяныеведраисой
дяспустынноймроселочнойдорогипогрузилисьвзапахиземливлажнойотнедавн
егодождяищитепчелсказалотецонивсегдавьютсявозлевиноградакакмальчишки
возлекухнидугласдугласвстрепенулсяопятьвитаешьвоблакахсказалотецспусти
сьназемлюпойдемснамихорошопапаионигуськомпобрелиполесувпередиотецр
ослыйиплечистыйзанимдугласапоследнимсеменилкоротышкатомподнялисьна
невысокийхолмипосмотреливдальвонтамуказалпальцемотецтамобитаютогро
мныеполетнемутихиеветрыинезримыеплывутвзеленыхглубинахточнопризрач
ныекитыдугласглянулвтусторонуничегонеувиделипочувствовалсебяобмануты

мотецкакидедушкавечноговоритзагадкамииивсетакидугласзатаилдыханиеипр
ислушалсячтотодолжнослучитьсяподумалоняужзнаюавотпапоротникназывае
тсявенеринволосотецнетороплivошагалвпередсинееведропозвякивалоунегов
рукеаэточувствуетеионковырнулземлюноскомбашмакамиллионылеткопилсяэ
тотперегнойосеньзаосеньюпадалилистьяпоказемлянесталатакоймягкойухтыя
ступаюкакиндеецсказалтомсовсемнеслышнодугласпотрогалземлюнониче гоне
ощутилонвсевремянастороженноприслушивалсямыокруженыдумалончтотосл
учитсяночтооностановилсявыходижегдетытамчтотытакоемысленнокричалонт
омиотецшлидальшепотихойподатливойземленасветенеткружеватоньшенегро
мкосказалотеципоказалрукойввepхгделиствадеревьеввплеталасьвнебоилимож
етбытьнебовплеталосьвлиствувсеравноулыбнулсяотецвсеэтокружевазеленые
иголубыевсмотритесьхорошенькоиувидителесплететихсловногудящийстанок
отецстоялуверennопохозяйскиирассказывалимвсякуювсячинулегкоисвободно
невыбираясловчастоонисамсмеялсясвоимрассказамиотэтогоонитеклиещесвоб
однеехорошоприслучаепослушатьтишинуговорилонпотомучтотогдаудаетсяус
лышатькакноситсяввоздухепыльцаполевыхцветовавоздухтакигудитпчеламида
датакигудитавотслышитетамзадеревьямиводопадомльетсяптичьещебетаньево
тсейчасдумалдугласвотоноужеблизкоаяещеневижусовсемблизкорядомдикийв
иноградсказалотецнамповезлосмотритеканенадоахнулпросебядугласнотомио
тецнаклонилисьипогрузилирукившуршащийкустчарырассеялисьтопугающее
игрозноечтоподкрадывалосьблизилосьготовобылоринутьсяипотрястиегодушу
исчезлоопустошенныйрастерянныйдугласупалнаколенипальцыегоушлиглубо
ковзеленуютеньивынырнулиобагренныеалымсокомсловноонвзрезаллесножом
исунулрукиводкрытуюранумальчикизавтракатьведрачутьнедоверхунаполнены
дикимвиноградомилеснойземляникойвокруггудятпчелыэтововсенепчелыацел
ыймиртихонькомурлычетсвоюпесенкуговоритотецаонисидятназамшеломство
леупавшегодереважуютсандвичиипытаютсяслушатьлескаклушаетонотецчут
ьпосмеиваясьискосапоглядываетнадугласахотелбылочтотосказатьнопромолча
лоткусилещекусоксандвичаизадумалсяхлебсветчинойвлесунеточтодомавкусс
овсемдругойверноостреечтолимятойотдаетсмолойаужаппетиткакразыгрывает
сядугласпересталжеватьипотрогалязыкомхлебиветчинунетнетобыкновенныйс
андвичтомкивнулпродолжаяжеватьяпонимаюпапведьужепочтислучилосьдума
етдугласнезнаючтоэтоноонобольшущеепрямогромадноечтотоегоспугнулогде
жеонотеперьопятьушловтоткустнетгдетозамнойнетнетздесьтутрядомдугласис
подтишкапощупалсвойживотоноещевернетсянадотольконемножкоподождать
больнонебудетяужзнаюнезатемонокомнепридетнозачемжезачема

Висновки

В ході лабораторної роботи ми отримали навички частотного аналізу на прикладі афінного шифру. Проводили частотний аналіз біграм для

шифротексту для того, щоб співставляти частих біграм мови та частих біграм шифртексту. Використовуючи розширений алгоритм Евкліда, знаходили обернені елементи за модулем і розв’язували лінійні порівняння для того щоб знайти ключі для афнного шифру. Застосовували перевірку змістовності дешифрованого тексту для кожної пари ключів.