

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут”
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2

Криптоаналіз афінної підстановки біграм

Виконав:
Грубіян Є.О.
Прийняв:
Яковлев С.В.

Київ 2015 р.

Вхідні дані

5 Варіант

кеюибшаефлфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдълыхунхмъввнсдуэмндтиххеюибшщязэкзхшвнос
ютнйьштцншуссянхшлвжвпъкшвнмщзфтсхшпддкясввццтнавпъгнуйьвнлхйьерддыприхэкъэцэижцъехшмсэкжлрибуждэм
химвпъявсттнэцюсфспъуэйпдкнхркхуляацкчашьяншибжаксэкццзтщиюцншумшошьяшкшнфрхуюижсгцызэфршихэтчщрихн
эпозтгфккчщкдмкльоьеынунийлцяьэрхнмкпмдкийпоиэуныэнснмнсхэццъедктництндущоэивупхюфйчсьивйэютнрщэбв
цншуоздкдктнунянккфкяяшиссбинкурдцбщдскрщяншкдкяяишжшсвьербщяшндужйнкшнвнгоьцэииспътуумшщидекхнду
аошдвдеигебуаявюсшйдроццвнфибжлакццвбвбываккчслтьхщйьцъжьбрьецфтспъбишиювдъезбтнмсэкжлрчсхщърпъшв
шнйьяншибжлтьчсьрьэчтнундулфтсншбйбнбжцнрнющккюиеуаяэзтьяяреурндущоэгкмбобмщкскехюксддтсывзтмсун
йьксшиссншчщйьцйнпрщккфкясркейьйнавпъхсуншнузеумкжлаклцисуьдбкфипьйнмсуншснхтуйнццмсьамныонкцркч
ыоклзфкчпъвнуыозрбжлжвцнхщссцъжьбипсрзфкаьихмнщэчсавозулбутнэцнулцэткоццвнфибхюпвиэислбиювинхыршьив
цнярбщфджлзйьцйнзцнулцяьйвнцхркпрыожврщьянкиюдждкеспьибубиюхшбуакикаяеэдакаоццсвлбеилрлвцофкяяшвнун
хшлвэкжлтьосцнхщитнуншнмстспълйаихрннънхшвшшвносчсабъеишжсоэосыумщмбриввудябакурщяэлчяздкайьечслс
осэкццяьцнэлязъаьцнхщссцъжьэжлмщунавшьавзтьяюсуйвнакдуиуььяучмпрфдйвдихрнфзэфтнхщиеуаяэзтьяюццъь
еелфеипвидийдкяязщупзобчсуьвнлвмьтнщъьедвнстйндуюомнщоццвнфибхюхтоццсввныкльрнпъювосисцйвнхчщлр
акющчъцнхщбщйтннсхщдицьешичщкздукчвзтьяаккйдищжлвььктзихувулловаявшньсйссцпрыоьнчкццяьклхнщэюдри
исэкжллреуныьктзшрэчшиязиебчлвацлотнуншнмстспъицшэмвшшкзляобсчбщдщцэикзясусйнкюозвътныэакосжцншвюи
йдьяшншвосюсчязиьсунуллвихьвхдскклмщубшскуаохшрнрцязакубсчфкяяосгйрщтнгбфдзйьцэибусчжвавмнзэфдьюиошс
осюдритьйьнсхщтнъцмнрнннстрсосуллвзтвднкцяубщхищмштсчтгнэкхуямйдчщццмнрншвйннвлвацшвъхавршншицюиьс
щожсюдгнущрнчзшрынулцхдвмьцнрнуьняедьхсцнфуэюосйсчцэидктнуншнмншспъчшвнюдцфвдьюиоасунйпщнбкчэивнмн
ръншибчэлориисэибудкяспнзжлфсчсбакашнтннызтгпъмвзтьсйядуццщццспрчсэьлвзтклбулцшвюибщцвивнуйвнакеи
чмывпвыэдчфкклццсвынуняуумпъшвшрцциссцмющиюлврлиэйдбцриьцяьввюдаолыфьмодкчъяуфкойнкйдлццтнавчзфдью
жяшсввдуюизбывшшвныльидышубшврчязрщвдойвнвмщнсунцмохщньюссттнхщщфддбтьпнзкъеэдхнщъжвзтфрлцдкяяхъ
овюсстхщрнпъйнщофкпрынсиульдццхифсчсхдйьрсерццисшнюшьсцклтьпвидрошифкяяшнюдаоосунчзфпъцэилцмъэсц
клжшвнуакубакюйтноснпъявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнвшшвпъьзмбйнвнцхпнуцязъсйядуулрибу
вдвнщозьгйбчйдсчбциэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбмьлриввеэьхэфртггнулцубщшьав
тулцибсчннисозфдьюжлрлрцбщдскрщиебквэгвжвзтшвжъаоеитншнпвихэхаорщибсфсчсщъавпъскггююшлхвииспъвиул
бутнэцнулцяьжцюсчвввиймюгвшншицюиорисунлсгоьрыноьхоццвнфибкзенуьпъбцрныгщйеуйнзшщъявхщеуеидебупъесуз
юцдкясюэсцэиьцэттнмслдроавежбщяйрщйуйолцеищккфдкфьнхчщмцявисчтжъамаофисрябсчшижслбубэщнщфдэмсщяуб
чэйсанэиршхшмсэктзлэусхщрнляпдгсгцщфдкфьвннубубяслоишщщдекщсхдскхсовннчубакакхуямдкяяхсвнхбжсмкшн
щъжвэкссщъккдктнфифсбвбддкясттнмслдъшсвьцйьшнсиеуюкышцспрыльнфкйдищцйьцйныэвнхбрифкйуунрншьвнбкубъе
бчсвйнжндуеисхавупмююсшодкльулбусччнннстрсншшвъхаврщянсцознкссьеуснснмнснсибсвддцйнчсщнэпозцфибссщц
убссвнхбрифкясхщфдццяьклрыобсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглогзфьцэидктнунэибунсхщав
ьвлващеутнишлрлрцбщдщцйьнвнцхдздкицмъяхавъшвущфьцъжщнмкпмдкяярнэирщввпнуолцфрыншхщмснфжврйвнъркзскыщ
ссвнхбрифкясозййццньюириьсосйгыовдриклакязеудкяюсумщчяввнширилвацшвъичдрщдкикгбмщбушцстссьйьшвоейу
лцгйшщфкнхдкбщйьннихобсчшибщекбщэюнхзциссичшиютнмслдфидмбццмсгцшвэрэфвджжяввшнмсчярщхъовюсгымцкзищ
ссырьшудццпреулщцаефдхссироювяьисшщкзпксчролвттрицнмскмжявзтсигюгхтнмспбмщбушсцьмюннисдкдкцфжвьйьдт
мщшвпвкмжъямщшвжьрефщакиеэдакролфбклцбуабзщбукзунгэщъккгнвшннвжврщрнуыознбкжлтьбцрныгйьсншщдекцгеэ
юрсхщнъбиулбунхнйчдпнввкцйнуншвъьтнщюьццсуьсцтгуьйьньюсфипъявпъпршьйьнлхавъсьеуобмбмщбушсфрмщчяовуп
мюосшнкуаохшмсэкццзтбъьмнжннуыфрыэиьсфсчсщъавозщсостгйлцмктзулыньнуйаихщавиэжъщюуобмблвьернунокпмшр
дцбщдддбубихйсансцрбжлвэкхюдрошдджсюсунымсйкмбкзхщхурсунщхвввмдкорыснчъяуюишсвпнккурмщеувирсунсццъ
блшэннбваомзмбвскаьшнжъжвупклэчйдищъеишивебпрябакоьзтяншиссйебчввтсэкиющъккбыоскищцпъявицчэивьяочлц
свпдгсфудкфьяэюдаорибщвъчрытнрсбидуаодункюххьсхдгсунфрлцдкяяакдункчэжсубсчкнбквъфзтнуноьюддкнхживнал
буыодкеиочоьлхэфдкфьпльннсвнмкхсмштсывзтьятнакфкпрябйожсюсунюиикцфтсвщбакксьйнбжрисцвдцмнщъкмыгъяе
хщссяюсстхщрнхщбщцвнклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгъерыннъэьнаваэкиютннъькиютноьакеишдщц
швпвмндтихжщнйнкюисъьяокпмаобщсэщбушсхшмсэкссъейпфкясишхнэкмбжлжвннстрсосщэтсъяубщцввяфжсюсунтс
чтгвмьввьелвмкрюээтдццнрнмюхщбуакдожсвнйсэвпъфихщсъяэзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпвюскиосыр
ынщэгожсгцмэфдфмжяосэкццзтпътнрсаьлмщриарэфеуэирибщхиьсуйвнххвнстйнянцуфкщццсунхдицяедьакхуумжсвнчр
лвнъзтьяйкчезъццюсжрышумьцэиясезьцвнвнунищъеяцпъерынхщщццвиьянсибясшнлсьпвтснфюирыосцъаккнившоижс
мкарссжозщццесшндцнсккаирсыэокпмщнввийкриаршьлнуьэиулбунхмокедцрнфзфдкяспнчххуцфюижсшщязсюсшсизъжввш
язосрнеелюиьсфюосэщублунчяюэецэивьяокхуямщщдбфдгвмсжкддъжъяушнвввшнмьвврщозенйсуньейпфкаьтныо
еушъкхзцнулцэтднчелвпъгцбуавкмлыкльтяуаишдщццуюеобушцвиакэмлхчярштсчтрыйнвнцхмьаггмщдджсунлххъэт
лрэчбудквззвнвшнжъжврщуннжжвжрццисчцэиаьмчвврщиссржжэжмндтфрлцяьклхнгцязэвъкъэцэиьшсвмдъцюяусиебчду
ьешдриезмщюиоуриессвхъовэкжятнмслдзълсрщйносыклрлврнввлэусхшрнавпъгбубсвйнавдъоспншсмкпрынкчмсхщнкой
щбщддмэфдфмжлрифсбвбддкяюоввйнщцыгеввйьмъоьжывнакеиэчпидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшьо
арфдрижлцзэчсавпъзншвйьнркизфтсиспънкгбмщбушссцшмьввьщянсхмдктнйнккбщщдекццжлвьйквэпншнхщынгспныэ
рнгошддкйьявзтцнюфввовялябъаокпмаишнмнээхфкччтхдицвиьспъгсунмщпвюдцфюирыусунлрлцдкяяуаокнвпъфзлц
внштбвхщсцлэмдчзоулыфьтглогзфьцэидкнхпрынкчмстспъвишфгбрыяьщцжлзфпреурндцвныкиббарбуябакфкчявпвлсзврщ
ьяшнныннмьунжжюхщлвхщпэжвчспъпрццсвпддкндклцнулцмкльтсющщдекццзтиэярчсжвюсстибдцнътсюзстхщээрщъечщ
кэмшрнтслкеурьйоюхщньюссттнулбуввзнтснфчзццзтвииярщъякбнъависйщкзххуиюшннуятетнхщюафккчлспъюпърц
мнрншбнлсюдризьяуфкшдвчсксчавэтршхсщв

Скрипт криптоаналізу

```
# -*- coding: utf-8 -*-
import codecs
import itertools
import operator
import re

alphabet_ru = (u'a', u'б', u'в', u'г', u'д', u'е', u'ж', u'з', u'и', u'й', u'к', u'
    л', u'м',
                u'н', u'о', u'п', u'р', u'с', u'т', u'у', u'ф', u'х', u'ц', u'ч',
                u'ш', u'щ', u'ь', u'ы', u'э', u'ю', u'я')

alphabet_ua = (u'a', u'б', u'в', u'г', u'г', u'д', u'е', u'ж', u'з', u'и', u'к', u'
    л', u'м',
                u'i', u'ї', u'й', u'н', u'о', u'п', u'р', u'с', u'т', u'у', u'ф', u'
                x',
                u'ц', u'ч', u'ш', u'щ', u'ь', u'є', u'ю', u'я')

alphabet_de = (u'a', u'b', u'c', u'd', u'e', u'f', u'g', u'h', u'i', u'j', u'k',
    u'l',
                u'm', u'n', u'o', u'p', u'q', u'r', u's', u't', u'u', u'v', u'w',
                u'x',
                u'y', u'z', u'ä', u'ö', u'ü', u'ß')

bi_ua = list(itertools.product(alphabet_ua, alphabet_ua))
bi_ru = list(itertools.product(alphabet_ru, alphabet_ru))
bi_de = list(itertools.product(alphabet_de, alphabet_de))
alphabet = alphabet_ru
bi = bi_ru
m = len(alphabet)
table = dict(zip(bi, range(0, m**2)))

mv = [table[(u'e', u'н')], table[(u'н', u'a')], table[
    (u'т', u'o')], table[(u'н', u'o')], table[(u'с', u'т')]]

def extended_euclid(a, b):
    """ Повертає dHCD=(x,y) і x, y такі, що ax + by = d """
    if (b == 0):
        return a, 1, 0
    d, x, y = extended_euclid(b, a % b)
    return d, y, x - a // b * y

def reverse(a, n):
    d, u, v = extended_euclid(a, n)
    return u

def solve_linear(a, b, m):
    d, u, v = extended_euclid(a, m)
    if d == 1:
        return [u]
    else:
        if b % d != 0:
            return []
        else:
            a1 = a // d
            b1 = b // d
            m1 = m // d
            x0 = b1 * reverse(a1, m1)
            return [i * m1 + x0 for i in range(0, d)]
```

```

def affine_encrypt_ru(a, b, text):
    CT = ''
    for i in range(0, len(text), 2):
        CT += u"".join(bi[(table[(text[i], text[i + 1])] * a + b) % m**2])
    return CT

def affine_decrypt_ru(a, b, text):
    u = reverse(a, m**2)
    OT = ''
    for i in range(0, len(text), 2):
        OT += u"".join(bi[(u * (table[(text[i], text[i + 1])] - b)) % m**2])
    return OT

def get_freq_table(text):
    freq_table = dict(zip(bi, [0] * (m**2)))

    for i in range(0, len(text) - 1, 2):
        bigram = (text[i], text[i + 1])
        if bigram in bi:
            freq_table[bigram] += 1

    return sorted(freq_table.items(), key=operator.itemgetter(1), reverse=True)
        [:5]

def weak_language_detection(text):
    points = 0
    freq_table = dict(zip(alphabet, [0] * len(alphabet)))

    for char in text:
        if char in alphabet:
            freq_table[char] += 1
    freq_table = sorted(freq_table.items(),
                        key=operator.itemgetter(1), reverse=True)[:5]
    fq = [i[0] for i in freq_table]
    if u'o' in fq:
        points += 10
    if u'a' in fq:
        points += 10
    if u'e' in fq:
        points += 10
    if u'h' in fq:
        points += 10
    if u'n' in fq:
        points += 10
    if u'r' in fq:
        points += 5
    # print points
    return points >= 50

def attack(text):
    text = re.sub('\s+', ' ', text.strip())
    res = []
    freq_table = get_freq_table(text)
    fq = [table[(i[0][0], i[0][1])] for i in freq_table]
    for i in range(0, len(mv)):
        for j in range(0, len(mv)):
            if i == j:
                continue
            x1 = mv[i]

```

```

x2 = mv[j]
r1 = (x2 - x1) % m**2

for k in range(0, len(fq) - 1):
    for h in range(k, len(fq)):
        y1 = fq[k]
        y2 = fq[h]
        r2 = (y2 - y1) % m**2
        eq = solve_linear(r1, r2, m**2)
        if len(eq) == 0:
            continue
        else:
            for a in eq:
                b = (y1 - x1 * a) % m**2
                candidate = affine_decrypt_ru(a, b, text)
                if weak_language_detection(candidate):
                    if not candidate in res:
                        res.append(candidate)

return res

if __name__ == "__main__":
    CT = codecs.open("05.txt", "r", encoding='utf-8').read()
    f = codecs.open("out.txt", "w", encoding='utf-8')
    res = attack(CT)
    for i in res:
        pre = '\n'.join([i[j:j+90] for j in range(0, len(i), 90)])
        f.write("Candidate: \n" + pre + u"\n\n")

```

Дешифрований текст

Candidate:

убивать больше не надо по слезе того как он уже убил не следует ему быть благодарным иначе пришлось бы убивать с амуэ то не одно лишь доброе страдание это отождествление на основании одинаковых импульсов кубийств усобственного говоря лишь в минимальной степени смещенный на рциссизм этическая ценность этой доброты эти мне оспаривает ся может быть это во общем механизм нашего доброго участия по отношению к другому человеку усобенная снопроступающий в чрезвычайном случае обремененного сознания своей вины писателя нет сомнения что эта симпатия по причине отождествления решительно определила выбор материала достоевского но сначала он из эгоистических побуждений выводил обыкновенного преступника политического и религиозного прежде чем концы своей жизни вернуть ся к первопреступнику отцеубийце и сделать великое свое поэтическое признание и опубликование его посмертного наследия и дневников его жены яркое светило одной из эпизодов его жизни то время когда достоевский в германии был обуреваем горной страстью достоевский зарулеткой в ный припадок патологической страсти который не поддается никакой оценке с какой стороны не было недостатка во оправданиях этого странного и недостойного поведения чувств вины как это нередко бывает у невротиков на шло конкретную замену обремененности долгами и достоевский мог отговаривать ся тем что он привык грешить получил бы возможность вернуть ся в Россию избежав заключения в тюрьму кредиторами но это было только предлог достоевский был достаточно проницателен чтобы это понять и достаточно честен чтобы в этом признать ся он знал что главным была игра сама по себе в подробности его обусловленного первичными позывами безрассудного поведения слуга тому доказательством и еще кое чему он не успокаивался пока не терял все и игра была для него так же средством самонаказания не считая количество раздавал он молодой жене слово и личное слово в большем и играть или не играть в тот день он нарушал это слово как она рассказывает почти всегда если он с воими проигрышами доводил себя к крайнему бедственному положению это служило для него еще одним патологическим удовлетворением он мог перед нею поносить и унижать себя просить ее презирать его рассказывать ся в том что она вышла замуж за него старого грешника и после сей этой разгрузки совести на следующий день игра ачиналась снова и молодая жена на привыкла к тому циклу так как заметила что то от чего действительности толъко можно было ожидать спасения писатель ствоникогдане продвигалось вперед лучше чем по слепоте рив сег оизакладывания последнего имущества в связи с всею этой она конечно не понимала когда его чувств вины был оудовлетворен на наказаниями к которым он сам себя приговорил тогда исчезала затрудненность в работе тогда он позволял себе сделать несколько шагов на пути к успеху рассматривая рассказ более молодого писателя не трудно угадать какие давно забытые детски переживания находят в явлении вигорной страсти у stefana цвейга посвятившего между прочим достоевскому один из своих очерков три мастера в сборнике смятение чувств в новелле двадцать четыре часа в жизни женщины тот маленький шедевр показывает как будто только так им безответственным существом является женщина и какие удивительные для нее самой закон нарушения ее толкает не ожиданное жизненное впечатление но новелла эта если подвергнуть ее психоаналитическому толкованию говорит о том как без такой оправдывающей тенденции гораздо больше показывает все самое общее человеческое или скорее общее мужское и такое толкование столь явно подсказано что нет возможности его недопустить для сущности художественного творчества характерно что писатель скоторым не связывают дружеские отношения в ответ на и расспросы утверждал что упомянутое толкование ему чуждо и во севе не входило в его намерения не смотря на то что в рассказе вплетены некоторые детали как бы рассчитанные на то чтобы указывать на атайный след этой новелле великое светская пожилая дама поверяет писателю то что ей пришлось пережить в оле двадцати лет тому назад рано овдовевшая мать двух сыновей которые в ней более не нуждались от отказавшая ся от каких бы то ни было надежд на срок в котором году жизни она попадет в тюрьму одного из своих бесцельных путешествий вигорный зал на казко казино где среди всех диковинное внимание приковывают дверуки которые спотыкающей непосредственностью и силой отражают в се переживаемые несчастными игроком чувств в руки эти и руки красивого юноши писатель как бы без всякого умысла делает его ровесником старшего сына наблюдая же й за игрой женщины потерявшего все и в глубочайшей мотчаянии покидающего зал чтобы в парке покончить с свое ю безнадёжной жизнью и не изясняя симпатия заставляя женщину следовать за юной и предпринять в седляе госпасения и он принимает ее за одну из многих численных в том городе навязчивых женщин и хочет от нее отделить ся но она не покидает его и вынуждена в конце концов в силу сложившихся обстоятельств стать с яв его номером теля и разделить его постель после той импровизированной любовной ночи она велит казаться бы спокойно и все му ся но не давать ей торжественное обещание что он никогда больше не будет играть с ней и давать ей гамин а об ратный путь к своей стороне дает обещание встретиться с ним передухом поезда на вокзал но затем в ней п робуждается большая нежность к нему она готова по жертвовать всем чтобы только сохранить его для себя и он арешает от правиться с ним вместе в путешествие вместе с того что бы с ним проститься с яв ся чие помощи задерж и вают ее и она опаздывает на поезд в то скупое и незнущее му юноше она снова приходит вигорный дом и с возмущен ием обнаруживает там те же руки как она не возбуждает в ней такую горячую симпатию нарушитель долга вернул ся и игра она напоминает ему об его обещании но одержимый страстью он бранит сорвавшего его и грувели тей убир ать ся юнишь врет день гикоторым она хотела его выкупить опозоренная она покидает города в последствии узнает что ей не удалось спасти его от самоубийства эта блестящая без пробелов мотивировка написанная но велла имеет конечно право на существование как таковая и не может не произвести на читателя большого впечатления однако психоанализ учит что она возникла на основе умопостроения периода половой созревания юкаковом вождении некоторые вспоминают совершенно сознательно и согласно умопостроению вождению мать должна сама вести юного шувполовую жизнь для спасения его от заслуживающего опасения вред

аонанизмастольчастыесублимирующиехудожественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомотводеэнергиидействительнойгорнаяодержимостьявляетсяэквивалентомстаройпотребностионанизммениоднимсловомкроме словаигранельзяназыватьееа

Candidate:

ыбнвутгбчлышиниядлпесзетогохакожуеыбслноьлддпеезушынькльгнддрейишауейрйшломьшыбнвутсс
жмфмизтойендноюиудьоркесоетыпааишэтовтзжаеетллиндешаеснонааиоцишакощыйипэлссувьуиасчв
ксцбетюрнргвирилийшавяиаичажьноасоелеаичмггинеымншрийисюзбзеиуеюкоятернесньрткойдоьртрэеи
пнеоопшрнвыейсемзштшынъртвуоаялмхгнзупнбшзгндцбругочцсеиппоохнпшиншюйдбугоэуелоееуес
цбиннохснойресгуаышчйжчмемвачпйногсугаеорлмининногосокнгнцяцвкеовлншпясутолвнштсопниця
лтгэадиийпутцяпойрмчлнеотоедысчвзеаишржшytoлюноойррдолслевдбирчаоегийлядестоквюкргснесага
цаснозьягбиетмчысэитпцбмжаеаиовбндслцбикноернрглпмеетрпаихапокиеиуеюкрбимеюихидзнойрюж
аеуешккофцксвофйшикинвярюняаязпярвойрысгутнфкакттеыбчйтеясаецаньюеюитецвкепортмчысковп
гикнгнделпыбюиконааибегопочмярхнргснцзецисизнкваикоеговееышркоееиолдлншпюзндзгжюзай
тоырлмкргпадоеткешсэиовяецмгнъишлосуменалмкгирноасмрцсньэдестоквкчйтабузаякюдвешпгиъа
дозпутчлргмчыскоасмрцсеикотоиымнвпндпаштаялншхцинжаеаюкмкюйетирсннбелснддесюаякевлпыабд
гнцякэтогоетярнргбийедоетуйногопоюеаеаигчшветвофиенхаяэтойемеркцббвыегуйеыртфкушавльксн
дрштууузжминшвцбмеейернесеидонгжмьидоеткешсэипмргвтггонагинаньяаюерчтоснйрнвоиэрэшвлччсл
шывомнжнотавярюняаяяресдирипбюжевтаулвчинцяхтчрбмакмецитояаяинортцбелтожькойррдловдесто
квюкчйшыкдесюатоьлнпроаиваоезесчтошртлпснттндоетуттчноуеетинлтцббвртфмйрюшаньяаснкнйлт
ргцаенвмшпцакгыаэачапонеешсвпнддроднесеизгоосуьлузвернрглпярфиьнвмепдзбвжмрбъзыаистднопо
юеаеаихсысажтфмтдкхзутолсчсвфмдехекойчлмжиноэуснийексханвйлаяпохайеоеаярвнегокгыашпцанл
внзгвгтмквелрддетвогсжмснмкхзгнцяйехчштносчлмчысчвирхзпаналоумчлндйвейеьлувбюиуеетноысло
вобожьфейекгыаньсллнчиэрутавртвтаеиьиорншрфшйлртесловохакошаыаисхаянаштполтнвневдыеьлиодс
воомепрокгыдаидовоцивснбисибедодрпийеэеьсчвинногополовеаиуэтоьлмжслндшйеогогщеозномьатоло
хиуеюкомтдувзечвириндемоумрглемезнцпонодиньшуаисаньнепайресытцевпмецианьзгирцсханвутсдв
торчтосневзшцатаэуызгнзгесюарогоэржшаихаепесзешсфйртюйайгбуукясувысеишаьлддеюиидинниэргн
дчлнйлцсссноваомчлндоявешайрнвикцяэтоэуйулзтмкхаазжмштслдчтототвтуеобдфйетфиоежнотытчл
зкбимойнцбелоошипаньопцсинцявизаоежбетвоаиковдгнвпрройвкгйлесавлеменлччфеуейпесзепоегисшзг
битаулядбвгнцяпоьлддйеогомшсысчвцсряшишзггэтогоснмкснйчнойепоаичацаковдыегоиушсчувлндбел
яудоллштвоменошахатааиемфккотоиымодсжмнепайркгувирслтовдтихчъйлхзутбузнинноетавыабоеотод
аокпдзвозжвснбысаецаньеюкчлзкпшвгуваауеиьуоппхнрцсчмутгинашрцсюкхзбозелмчлндрглпясутолвн
штбузняуоапаньхаэиддевнопоташыкыдштюкделемешинаавнххндттыдвзеаидвкгирноасмрцсеиксоеааша
ывфйоапоцвтнвфегоиеедрпрокилдестоквюкфмуоциаиюсвотхтчяркохтгичаетяревшбирайжечмттиндеиушс
чвысньнокефлядналцутятштхрйчцсешкикнбжинмиеыртвтчазеиьэикшддквнпъкхзбвыеякмксутччлйшотъкмк
омэозчшттетюрнвмвухеетвоьяллъейсчжинмишлнмкмкдетднвытолюнчнлнбзеаомаязмксншнрфшинцябе
точкыехнеошипарнкеикикнинноквлегаылинденонюефлфэаыскипойвяржнзтцевпдихогнйлытмчыскозутчк
увгншюоговогитознмкцбъзюакоййревынаышфйоемдинийкигрхздобожьфепохаянаштсошслмлнкецбхеуело
юеуеюккесляскомеоеащлммжюккеейтмкеточкувгндеетчлйеялнпндюкхзгнтчтойеьчвдзмойнесеизгсндлпкс
еиньлхссноеттхтдзжысчвинногочвируетнабаыаютярнолтлпясутолсскотоиытминхсряянаштурмжысэи
еохнпшинцявочвштшамоврцсопрройзткюейжапачторпфмвнзкеточкувгнделмчмждонувнейемхндслувзгсн
жмяринцяйечмвтешатолтувыаисхамвшлштинянсквтирчеаеаюихатбхрцсхытгнеинуттчтошыакхзбвутюн
утпйеасзейвртуйноефлкволфкесюейсхапзжслояпачапоеаяштвизаоеэювфмлткежпгивлесчпяржытгб
члбейвядваеизежтфмцнхзядяноувдокегшоячаньйвюхйноуеюхквтирчеенфйбозеинимжапимьвтхатагшоя
аявтхаэиюптснрбелсняджнзцсирькхтирфмгфушикиношапоьапаштвоырлмяознргбиюсвотхэешцолонжау
оефеетфиовкгиреыязйлмошабскогохациновдысмецишспхцикофийекваичааивпгикошынастйвяракфквтирче
опвтязэаышфйеполрддетюрнесньридилоюмршжсчвнелемешиналмчейехчсхнмкгрокорчшветнабуэирт
вракфыадивогобнпшепясутолзкмкшыэезошслкргяудьялядольеоегоруефнфкфметшрфегойышашаклэдсюе
яззтиэрюйвеллншпвтярдвфегошсчидгыубогакшлмвтгавньипозипаышзгдзйллтцббвьязквпъкснкинъсоцвке
жбъзшааейнюйшикинмюйеюзхсаичасомьяеифзцсжалльелжинмиуьлддувутрзсюнофеовйрддйрлнттавенлье
гоопцсинцяснйрлномьеоеззаознжинногоокиьлинеыьвстоогирндиневфзкицыожинмиаихоуетохнбевтаецань
аяноснгнвпъкздыеоегонвянжмашаокснгофцувшсслкслошигштхаяцбетэаоежбетвоетутсдвзгснфмярео
оещярхзаеюкинъзглпесоежпощэтойийпрофширонарнойэюбоенюнокисневольтхаталомыкспоковфе
эуаябншддугцеэтирвееюрнкецбгшгделтоорнфкрпабожьфейесуаеиэрутсшашжыоегоаеиьоаяишацб
ыханлйауныасесвофйетирснньдьюеааикветмеиньяфномлемефуходойпкеждгневьктазенотасеяежп
росудейейсбзчлышойейенсньмюнофесчвгтувэпжярчувугавнерчтошпытюжькосопргнзтцегонлхснбисн
шржшыетоппыафиньяфномимысоеапзтжшысчвдеимыстотоголтцбтсайипроетытсдваяуеюкдепоиеиттаеяж
нвсюоечиснаоьаждбвяхнэпкеждхтесжепоясукншвфеуэубнпшеошафнуэпгихоцичвкгиреидфмясвомнсшин
демондншрмжнвыежтжмоевебуэишахакуйевоптднвликвйеэтмкеюгоаяиуфсомьяеибншрфшытолщдчлоаеунэл
аяэиэреошашапоияшаштлмуоэегоцбгшгнъинондьяридыасмрцсньюкхбыаайсирнагшеюзгбизршвольтфйбвр
утсдвснйшщяяштаеиьхикотоиыиаснкхвтолыгешьувиньлпдзириншашапоэипаштгоропаяпесзееьсчвыи
йзшаштлткемнхупаломьопцсеизгоойсжмяуиасчвфэаклысбахербъзйрцболувимвтнврувжешавизарнояно
юефлтииешткойеьнлпыавошавухеетвоааискмкяконасийемовехнвпроужеетлндчытутолзбчлышргувлега

ылинцяндшакожстхщашаюичукицчтоснездзаиулгнаофнувхумопоетроьемоговоедолинцялегиндэпчлувргес
дзменааияохаковосвзжаезеаилнсквтирчешспояишастсожесшинноскнутолюнесргцафняумопоетроьемоэу
воедолинщючаньдоджшаэачазвысеибнпшвполотуцжюзиьнлхсьанеаиьеговттаьлмжнвсюеголпцсинцяыррд
аошааинмцстожьгаечевукломврекумипхтдзжысчвинеывпроюзюеаеидвптсксюеиьтрзжвпярвоястоьнфкэп
ирькснгнюзчатаиееаштаяпорокоягоунюйетяетшупамеаивпескуаллинноинцсрцсхнеуаеттолюнесньбузп
мепаоежьюкясфиаеоежьеттуштцбртфмвтвоаеанярхиздфйетфиеожьнокгиршаяоаейжомесньдвщяштаяйкфина
зебтфметщрюйпомрнбноетнвснгнюзиеаиндаигсловошкроиеьлувтиэргнолрзвнхзнаньштбела

Висновок

В лабораторній роботі було зроблено криптоаналіз шифру біграмної підстановки та знайдено відкритий текст з поміж 2х кандидатів.