НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
«Криптоаналіз шифру Віженера»

Виконали
студенти 3 курсу
групи ФБ-21
КАЮН Вероніка
РУДЮК Олександр

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

Варіант 4

Реалізували підпрограми із необхідними математичними операціями:

- Очислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда

```
# a^(-1) mod m
def euclidean_algorithm(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        gcd, x, y = euclidean_algorithm(b % a, a)
        return (gcd, y - (b // a) * x, x)

def mod_inverse(a, m):
    gcd, x, y = euclidean_algorithm(a, m)
    if gcd != 1:
        raise ValueError('Обернене за модулем не існує')
    else:
        return x % m
a = 5
m = 31
try:
    inverse = mod_inverse(a, m)
    print("Обернене число для", a, "за модулем", m, "дорівнює", inverse)
except ValueError as e:
    print(e)
```

✓ 0.0s

```
Обернене число для 5 за модулем 31 дорівнює 25
```

Функція **euclidean_algorithm** реалізовує розширений алгоритм Евкліда. Обчислює НСД, двох чисел a і m, а також коефіцієнти x та y, які задовольняють рівняння: $a \cdot x + m \cdot y = \text{НСД}(a, m)$. Функція **mod_inverse** викликає **euclidean_algorithm** для перевірки, чи a і m взаємно прості.

Якщо НСД(a,m)≠1, обернене число не існує.

Якщо НСД(a,m)=1, повертає обернене число x за модулем m.

- Розв’язування лінійних порівнянь

```python
# a x ≡ b (mod m)
def congruence(a, b, m):
    gcd, x0, _ = euclidean_algorithm(a, m)
    solutions = []
    if b % gcd == 0:
        x0 = (x0 * (b // gcd)) % m
        for i in range(gcd):
            solutions.append((x0 + i * (m // gcd)) % m)
        return solutions
    else:
        raise ValueError("Рівняння не має розв'язку")

a = 28
b = 16
m = 120

try:
    solutions = congruence(a, b, m)
    print(f"Розв'язки порівняння {a}x ≡ {b} (mod {m}):", solutions)
except ValueError as e:
    print(e)
```

✓ 0.0s

```
Розв'язки порівняння 28x ≡ 16 (mod 120): [52, 82, 112, 22]
```

```python
a = 28
b = 16
m = 5

try:
    solutions = congruence(a, b, m)
    print(f"Розв'язки порівняння {a}x ≡ {b} (mod {m}):", solutions)
except ValueError as e:
    print(e)
```

✓ 0.0s

```
Розв'язки порівняння 28x ≡ 16 (mod 5): [2]
```

```python
a = 110
b = 4
m = 5

try:
    solutions = congruence(a, b, m)
    print(f"Розв'язки порівняння {a}x ≡ {b} (mod {m}):", solutions)
except ValueError as e:
    print(e)
```

✓ 0.0s

```
Рівняння не має розв'язку
```

Функція **congruence** для розв’язування лінійних порівнянь використовує **euclidean_algorithm** для обчислення НСД чисел a і m та коефіцієнта x_0, який є частиною рівняння: $a \cdot x_0 + m \cdot y = \text{НСД}(a, m)$

- Рівняння має розв'язок лише тоді, коли b кратне НСД(a,m), тобто: $b \bmod \text{НСД}(a, m) = 0$. Кожен новий розв'язок x_i базується на попередньому, додаючи період до базового розв’язку x_0. Якщо розв’язки існують, програма повертає список усіх можливих значень x.
- Якщо b не кратне НСД(a,m), рівняння немає розв'язків.

За допомогою програми з комп’ютерного практикуму №1, знайшли 5 найчастіших біграм шифртексту **(04.txt).**

```
Найчастіші біграми ШТ:
еш: 0.022921655833048237
еы: 0.016763599042080055
шя: 0.016079370509750255
ск: 0.016079370509750255
до: 0.01573725624358536
```

Далі шукали можливі кандидати на ключ.

Спочатку створили словники:

```python
# Словники для перетворення символів у числа та назад
alphabet_to_index = {char: i for i, char in enumerate(alphabet)}
index_to_alphabet = {i: char for i, char in enumerate(alphabet)}
```

alphabet_to_index: зіставляє кожному символу його індекс, **enumerate** починає рахунок з 0. **index_to_alphabet:** обернений словник.

Далі перетворюємо біграми у числа. Функція **bigram_to_number** обчислює числове значення біграми

```python
# Перетворення біграми у числове значення
def bigram_to_number(bigram):
    return alphabet_to_index[bigram[0]] * m + alphabet_to_index[bigram[1]]
```

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

```python
# Знаходження можливих ключів (a, b)
def k(ct, vt):
    keys = set()
    cipher_num = [bigram_to_number(bigram) for bigram in ct]
    plain_num = [bigram_to_number(bigram) for bigram in vt]

    for i, y1 in enumerate(cipher_num):
        for j, y2 in enumerate(cipher_num):
            if i == j:
                continue

            delta_Y = (y1 - y2) % m2
            for k, x1 in enumerate(plain_num):
                for l, x2 in enumerate(plain_num):
                    if k == l:
                        continue

                    delta_X = (x1 - x2) % m2
                    try:
                        a_candidates = congruence(delta_X, delta_Y, m2)
                    except ValueError:
                        continue

                    for a in a_candidates:
                        b = (y1 - a * x1) % m2
                        keys.add((a, b))
    return list(keys)
```

Функція **k (ct, vt)** приймає два списки біграм:

- **ct**: список біграм шифротексту.

- **vt**: список біграм відкритого тексту.

Функція використовує два вкладених цикли для перебору всіх можливих пар біграм:

- Перебираються пари біграм шифротексту, де кожна біграма представлена як y_1 та y_2.
- Перебираються пари біграм відкритого тексту, де кожна біграма представлена як x_1 та x_2.

Для кожної пари біграм шифротексту та відкритого тексту обчислюються різниці **delta_Y** та **delta_X** .

Знаходимо a. Для цього викликається функція **congruence**, яка знаходить усі можливі значення a за рівнянням $a \cdot \Delta X = \Delta Y (mod\ m^2)$

Після того, як значення a знайдено, можна обчислити параметр b:
$b = (y_1 - a \cdot x_1) mod\ m^2$

Як усі можливі варіанти були перебрані, функція повертає список унікальних пар можливих ключів (a,b).

```
Кандидати на ключі (a, b):
(a=344, b=50)
(a=650, b=541)
(a=428, b=309)
(a=320, b=913)
(a=452, b=10)
(a=92, b=369)
(a=427, b=29)
(a=89, b=562)
(a=771, b=861)
(a=531, b=123)
(a=482, b=285)
(a=297, b=258)
(a=76, b=262)
(a=534, b=332)
(a=571, b=351)
(a=809, b=732)
(a=390, b=10)
(a=926, b=954)
(a=503, b=890)
(a=430, b=830)
(a=330, b=956)
(a=371, b=152)
(a=817, b=821)
(a=365, b=776)
...
(a=627, b=583)
(a=34, b=828)
(a=947, b=609)
(a=533, b=603)
```

Для кожного кандидата на ключ дешифруємо шифртекст.

```python
# Перетворення числового значення у біграму
def number_to_bigram(number):
    first_char = index_to_alphabet[number // m]
    second_char = index_to_alphabet[number % m]
    return first_char + second_char

# Функція дешифрування тексту
def decrypt_text(ciphertext, key):
    a, b = key
    a_inv = mod_inverse(a, m2)
    plaintext = []

    for i in range(0, len(ciphertext), 2):
        bigram = ciphertext[i:i+2]
        y = bigram_to_number(bigram)
        x = (a_inv * (y - b)) % m2
        plaintext.append(number_to_bigram(x))

    return ''.join(plaintext)
```

Функція **number_to_bigram** приймає число і перетворює його на біграм:

- ділення числа на m дає індекс першого символу біграми.
- залишок від ділення дає індекс другого символу біграми.

Повертається рядок з двох символів (біграма)

Функція **decrypt_text** здійснює дешифрування шифротексту за допомогою ключа (a,b). Вона використовує **mod_inverse(a, m2),** для обчислення оберненого елемента до a за модулем m^2.

Для кожної біграми застосовується дешифрування: $X_i = a^{-1}(Y_i - b) \bmod m^2$

```
Результати дешифрування:
(a=344, b=50): ыжжомарйнэшмвхужгупйжьбфйжфгбачнвгтбруййоаюысщеосэхьшзгучмвбнсвщвхайоархшыщмелгуэпчщеосэхьфгтбкыжутэцулуугвбчыт
(a=650, b=541): еивпюьбяюдгхцщюинадямкжээиасаьцтчсячеацячышзцнепсдюквенажхрчзженцщтячьлщизахкшнасмднепсдюкасячуздаодтафагсрчлэй
(a=428, b=309): сдуаызнтушрбпмхденютнщтэьдюхсзнрзхецонбтьзяйлкдасшхщпуенббнцжогкпмхтьзимсйабэсенфпикдасшхщюхецшйунбшлнбнохнцвйа
(a=320, b=913): мшэожрлэьмьбснцшнафэаяэцушффмрбчыфмзфамэурихэижохмфяжпнадббэфтиисназурпнцхсбнкнаоееижохмфяффмзшхсаммэагаюфбзахг
(a=452, b=10): кссиырсвдахтсдусноцвйкзйзсббфркнюбмлкохвсрвебпципаыкймноьтялышопсдвсрйдыертичнопгвпципаыкббмлдеюокалодожбялбедн
(a=92, b=369): хцрюбйщнштгдмиоцтоэнчшдлнцкагйсбващжкопньйыхкыуюмтйшкутожджэфшымилньйбилхадтзточьчыуюмтйшкащжцхйойтчощоналжохбб
(a=427, b=29): юхоцкэывирзомуэхялчвщиппухцйээытмйэбфлявтэсмодкцшрчикщялгоьбцгрдмущвтэжуэмлоакялвьздкцшрчицйэбгмллэрнлалтйьбшмзт
(a=89, b=562): йпжйюдщемотьтыппентееабфзпцщодцвбщулгнземдхзйшяййосаюценльалчяэштыжемдчысзщьяуенпрфшяййосацщулмзьнроонянпщалкзте
(a=771, b=861): бфыюзйшкоущапбзфстскчеещяфзячйфзеяфрптжкхйамдюфолуденыстгабрхдчюпбекхйфбымбаншстэхпюфолудезяфрцмзттуьтлтаябрфмг
(a=531, b=123): ящдатеыдцьооунншыгдцйбфбщепвепззпаюьыоддекбнрлащькйотшыхоуююкщрунпддеоновзоюхшыюшврлащькйепаюувгытьпыяымпуюхвы
(a=482, b=285): хасриуххжнэмуяеаыьужнйфэрапщсучокщсхцьзжмущлззпрюнмймвыььмрхцциузуяфжмуряплямшкыыытузпрюнмйпщсхтлвьангьмьнщрхнлн
(a=297, b=258): рсеиаршвзаютэдщсноювбкэйнсжбшрингбжлкоэвхрпегпкитаукемногтшлпшрпэдлвхрфдйештьчношгдпкитаукжбжлсеюоналодолбшлоее
(a=76, b=262): хьукчзлффнщогыжьнанфосыюььжбозжмлбхетащфузйпнухкмнпсжшнаыоцеддмугымфузжыупчоцрнарибухкмнпсжбхерпзакнжаэаибцехпрм
(a=534, b=332): жлхкщдияырэтчнзлехмякшфсрлнчздиоччиапхеясдтфхэщклрмшщзехбтканюуэчнкясдюнзфштдцехвжээщклрмшнчиабфшхзрцхдхсчкалфэ
(a=571, b=351): солчзпцюуаяниыиодссюехоцфоояопотсяьфзстюспрьйржчиатхцудсщнифозыриыдюспрыцьдниидссэиржчиатхояьфоьуснажснсйяифсьф
(a=809, b=732): ажбопаейаэюмшхчждудйгьэфнжигдачнхгрбсуюйсахыущаодэтьчздуэмабшсдщшхфйсазхрыямплдутпщщаодэтьигрбвызуеэчумузгабпып
(a=390, b=10): еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевы
(a=926, b=954): уфцоуйокчутасбщфстэкяежщсфцядйозфяврптыквймкюпофулебыстлаорудююсбьквйцбдмщаешстшхюпофулецяврямзтыуьтлтпяорэмы
(a=503, b=890): еллкчдчяйрэтйнжлбхыявшлспплычедгожчбалхфяпдефтэпкшрдшузбхбтгауюрэйнщяпдпнщфштйцбхтжщэпкшрдшычбауффхфртхахачгаюфч
(a=430, b=830): афыонйдкиусамбжфжтэкйеющюфщяюйрзчяярдтскыйхмсюфоеухерыжткалрвдеюмбркыйсбсмшабшжтбхэюфоеухещяярммытмуптаттялркмя
(a=330, b=956): зяэщвьшблшбгпймястнбувяюьякэеыщоюэлжетйбшьэнлцсщшшовккстхгжщыбцпйгбшьойднмгдчстыепцсщшшовкэлженутдшйтмтяэхжшнб
(a=371, b=152): ьццонйлнштбдпиуцноонпшглтцгапйубьакжеобнзйчхюыщюмтбшууноддыхпфмыпиэнзйдизхюдмзновьлыщюмтбшгакжтхдойттофожаыккхг
(a=817, b=821): мвизмжоаричюбчзвтощаыялгшвцдйжетгдйьяоюахжшуюкузгисяпцтогюяыоеикбчдахжвчсумюойтопыщкузгисяцдйьрурочиьочовдяьэук
(a=365, b=776): всатмшаюймнкхпбсэзыюпдглчсщеяшчопеуэтзгюфшэиоаытщмнддхэзйксэиярахпююфшпииискржэзйцзаытщмндщеуэоийзюмлзюзхесэдиг
...
(a=627, b=583): шпдопикггфмцтсщпбщогтэаxгпсыэиэтыындлщзгзикшпбиотффэылбщрцпдлвнбтсмгзишсяшицдьбщакцбиотффэсындшшфщофтщащхыпдгшь
(a=34, b=828): иешнгязиьыщлвфаестживщиухецвчясмдвгаятаиеятьфшчняысщюжстшлтакрешвфциеярфньььлнкстиоьшчняысщцвгаяьфтаыетщтхвтамьмя
(a=947, b=609): дбьстфжзюопннаубюыдзякквюябыьыфхпцьзцшычзцфцмнишсжоюжжгюынпжцвчоинаезцфкаммсналюырущишсжоюкоыьзцпмдыиоеыоыщьжцкмг
(a=533, b=603): бйянцждыюфвмгбэйнауьдуярчйучбждэкчмцдарьчжудзгонафыувщнасмдцляпггбыьчжкббдтмфынаэюкгонафыуучмцшдяарфзасагчдцрдс
```

Тепер виникає потреба відрізнити змістовний текст від тексту-шуму, що виникає при неправильному дешифруванні. Для цього скристаємося критерієм заборонених біграм.

```python
# Список заборонених біграм
forbidden_b = ['аь', 'юь', 'еь', 'оь']

# Функція для перевірки на заборонені біграми
def zaboroneni_bigrams(text):
    for bigram in forbidden_b:
        if bigram in text:
            return True
    return False
```

Функція **zaboroneni_bigrams** перевіряє, чи є у тексті хоча б одна з заборонених біграм зі списку.
Якщо хоча б одна заборонена біграма є в тексті, функція повертає **True**.
Якщо жодної забороненої біграми не знайдено, повертається **False**.

Якщо в результаті дешифрування не виявлено заборонених біграм, то виводиться текст, інакше програма виводить повідомлення, що цей варіант містить заборонені біграми

```
Результати дешифрування:
(a=344, b=50): містить заборонені біграми
(a=650, b=541): містить заборонені біграми
(a=428, b=309): містить заборонені біграми
(a=320, b=913): містить заборонені біграми
(a=452, b=10): містить заборонені біграми
(a=92, b=369): містить заборонені біграми
(a=427, b=29): містить заборонені біграми
(a=89, b=562): містить заборонені біграми
(a=771, b=861): містить заборонені біграми
(a=531, b=123): містить заборонені біграми
(a=482, b=285): містить заборонені біграми
(a=297, b=258): містить заборонені біграми
(a=76, b=262): містить заборонені біграми
(a=534, b=332): містить заборонені біграми
(a=571, b=351): містить заборонені біграми
(a=809, b=732): містить заборонені біграми
(a=390, b=10): еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболе
(a=926, b=954): містить заборонені біграми
(a=503, b=890): містить заборонені біграми
(a=430, b=830): містить заборонені біграми
(a=330, b=956): містить заборонені біграми
(a=371, b=152): містить заборонені біграми
(a=817, b=821): містить заборонені біграми
(a=365, b=776): містить заборонені біграми
...
(a=627, b=583): містить заборонені біграми
(a=34, b=828): містить заборонені біграми
(a=947, b=609): містить заборонені біграми
(a=533, b=603): містить заборонені біграми
```

Отже, ключ знайдено **(a=390, b=10)**
Використовуємо наш ключ для дешифрування тексту та запишемо результат у файл **decrypt_04.txt.**

Зашифрований текст

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмуг
фбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэй
кчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывдьмиыыяшцрбгянямз
юдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчф
вэрфешмяояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшя

щксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквк
шятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдхп
езхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтд
оккжшскзыядншууезжурфешщпнзшятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжо
щккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозно
юуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыез
ыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяа
нбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфмов
оцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбляь
хзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссо
жзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздв
щоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггднотлккжжипеызохлщ
пдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбаз
ущпязхлдырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяц
пдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякз
уяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшявж
ядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжшалт
ыбжхябжюакцопиыщчыдншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвл
яешууяхщжпонойкыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзншзун
рюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряешбзкц
колппотзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщ
оцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяямзозхьпешьоаоешывмк
йыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзсккрздвюптжждшсэыпзьцядел
оцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряеш
йкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекш
ялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножяяоьоэмкзшяпдмыэзгпйшууешоцс
аскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзцжжущпрф
уяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыя
мйшалтыеызоешыедвайнинзшязпкцрфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзо
рэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшощжшшйк
шшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпю
длвюпюпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяра
жуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмзюдайюдьмиыыяхфщ
жцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямз
юдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкпоноюаао
щяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзуз
хщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшясжеьзоешрйэжпзжжбяаоешывбзлжц
шшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешедвдвлгфезш
йдбряилгфеыхзсккчвкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпи
фрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюнешибряшяякжшбчфуэжмзч
швдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцы
ыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжоз
номясктзлзмкжшбчшящкбяйбзбяшждцыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояо
ратлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщж
шмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйка
зсшлячовунщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчпод
ояоносшншмоешдбждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлцлыксфохявжяд
тлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчбюпповб
нзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфссешмяаб
яопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбж
юуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопжипеызозхьпешьо
мяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяяявлвжип

юпэышбмунрчфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелж
рбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяилщкцжжзщрэысяныблоцлыщемыжучмду
бзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгшьльфжшншмолдоп
сшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжю
пмуяззощуивръмзвожзпофотывдохлцюпядайхпимиыраыжнэюшсйокбяжярзьазоныркоцы
ыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсыяхщжипхордяожзщ
ызбрякыбзлжкжюпмуяззощуивръвуйшайподояохлщкбяьшмущжзовказхяанаоешезвжбякбм
урфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыи
ыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшкопншфузхпмдьюшшящкскткллзокрзпмжз
ешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуяяоекзожзуяпонзяын
швдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчхябфбждо
цпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожз
биеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфлцабгяыовояфяьшмущжвзлж
ыцмимшшйгшезновжьошйээфщзрзмкуягшзбезносожзбиеыыядвзбряжзлжипюпоцчбптдох
либвоанаопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямп
пыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйка
нюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаоешезвжпонопмйкйвюпуу
эжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешыл
бэяоыкжшбччзкзтырйскпонзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщ
окыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяегдя
уярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшя
рллзджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояо
еыщжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюдншуусйшфкзныбжхяншзогя
уяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпеяпыэжйэ
зпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

Розшифрований текст

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточ
тоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодоказ
атьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоев
скогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиунижениййосуждение
достоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтоз
натьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказанияэаслуженн
огоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебян
аказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправдании
наказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнака
занияеготребуетихсверхяизбавляясебятакимобразомотсамонаказанияготктознаетсложноеи
изменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмысл
априпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчтоихперво
начальнаясущностьосталасьнеизменнойнесморянавсепоследующиенаслоенияможносказат
ьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерениемубитьо
тцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокою
щимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойонпришелкпол
номуподчинениюбатюшкецарюоднаждыразыгравшемуснимкомедиюубийствавдействитель
ностинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяниебольшесвоб
одыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведениямондопосл
еднейминутысвоейжизнивсеколебалсямеждуверойибезбожиемеговысокийумнепозволялем
унезамечатьтетрудностиосмысливаниякоторымприводитверавиндивидуальномповторени
имировогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотг
реховииспользоватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконеч
номсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеческаяс
ыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойси

лыинемоглабытьпреодоленадажееговысокойинтеллектуальностьюздесьнасказалосьбымож
ноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдосто
евскогооценкеимеющейправонасуществованиелишьспристрастнойточкизренияопределенн
огомировоззренияконсерваторсталбынаточкузренияявеликогоинквизитораиоценивалбыдост
оевскогоиначеупрексправедливдляегосмягченияможнолишьсказатьчторешениедостоевског
овызваноочевиднозатрудненностьюегомышленияявследствиеневрозаедвалипростойслучайн
остьюможнообяснитьчтотришедеврамировойлитературывсехвременктрактуютоднуитужете
мутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскоговов
сехтрехраскрываетсяимотивдеянияэксуальноесоперничествоиззаженщиныпрямеевсегоко
нечноэтопредставленовдрамеоснованнойнагреческомсказанииздесьдеяниесовершаетсяеще
самимгероемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенн
оепризнаниевнамерениюбитьотцакакогомыдобиваемсяприпсихоанализекажетсянеперенос
имымбезаналитическойподготовкивгреческойдраменеобходимоесмягчениеприсохранении
сущностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействит
ельностькакчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднаме
ренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетс
яврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповтореният огожедействиявотно
шениичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинан
еделаетсяникакихпопытокснятьеессебявзвалитьеенапринуждениесосторонысудьбынаобор
отвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесправедли
вымнопсихологическиабсолютноправильнованглийскойдрамеэтоизображеноболеекосвенн
опоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеуби
йствомпоэтомупредосудительныймотивсексуальногосоперничествауженщиныненуждаетс
явзавуалированииравноиэдиповкомплексгероямывидимкакбывотраженномсвететаккакмыв
идимлишьтокакоедействиепроизводитнагерояпоступокдругогоондолженбылбызаэтотпосту
покотомститьностраннымобразомневсилахэтосделатьмызнаемчтоегорасслабляетсобственн
оечувствовинывсоответствиисхарактеромневротическихявленийпроисходитсдвигичувство
виныпереходитвосознаниесвоейнеспособностивыполнитьэтозаданиепоявляютсяпризнакит
огочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечем
себяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэтомнаправлениироманрусского
писателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочеловекомс
вязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитрийукоторогомотивсек
суальногосоперничестваоткровеннопризнаетсясовершенодругимбратомкоторомукакинтер
еснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобыэпилепсиютемсамымкак
быжелаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийцаивотвречизащитник
анасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодвухконцахзавуалировановел
иколепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядосто
евскогозаслуживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершенно
безразличноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсялишьтемктоег
овсвоемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьдоконтрастно
йфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамииискательнаслажде
нийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввы
сшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитр
ийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсяв
ыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьс
япрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевског
окпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотор
оенесчастныйимеетправоонанапоминаетблаготовениескоторымвдревностиотносилиськэпи
лептикуидушевнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукоторую
вдругомслучаенеслибыдругиеаа

Висновок: під час виконання даної лабораторної роботи були набуті практичні навички частотного аналізу на прикладі розкриття моноалфавітної підстановки а також опановані прийоми роботи з модульною арифметикою. Було реалізовано функцію для знаходження кандидатів на ключі шляхом аналізу частотності біграм шифротексту та відкритого тексту, а також функцію дешифрування, яка застосовує знайдені ключі та перевіряє текст на змістовність (зокрема, наявність заборонених біграм). У результаті роботи було отримано ключ (a,b) який дозволив успішно дешифрувати текст.