НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Лабораторна робота №3 дисципліни

”КРИПТОГРАФІЯ”

Підготував:

студент групи ФБ-06

Жак Костянтин

Київ 2022

Тема роботи: Криптоаналіз афінної біграмної підстановки

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

Порядок виконання роботи (варіант 8)

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.

```
'''
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.
'''



# розширений алгоритм Евкліда
def extended_euclid(a, b):
    if a == 0:
        return b, 0, 1
    else:
        g, x, y = extended_euclid(b % a, a)
        return g, y - (b // a) * x, x


# розв'язування лінійних порівнянь
def solve(a, b, mod=31):
    g = gcd(a, mod)
    if g == 1:
        return [(extended_euclid(a, mod)[1] * b) % mod]
    elif g > 1:
        if b % g != 0:
            return None
        x0 = (extended_euclid(a // g, mod // g)[1] * (b // g)) % (mod // g)
        roots = []
        for i in range(g):
            roots.append(x0 + i * (mod // g))
        return roots
```

Функція *extended_euclid(a, b)* обчислює обернений елемент за модулем за допомогою розширеного алгоритму Евкліда. solve(a, b, mod) вирішує лінійне порівняння та повертає всі можливі розв'язки, якщо вони існують.

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

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


def bigram_frequency(text, step=2):
    bigrams = {}

    for i in range(0, len(text) - 1, step):
        j = i + 2
        if text[i:j] in bigrams:
            bigrams[text[i:j]] += 1
        else:
            bigrams[text[i:j]] = 1
    counter = sum(bigrams.values())

    for b, n in bigrams.items():
        bigrams[b] = round(n / counter, 5)

    return dict(sorted(bigrams.items(), key=lambda x: x[1], reverse=True))
```

Функція знаходить кількість появи кожної біграми в тексті, після чого знаходиться частота цих біграм та повертається у відсортованому вигляді.
Знайдені найчастіші 5 біграм у шифртексті:

```
['жц', 'дэ', 'цэ', 'сц', 'оц']
```

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).

```
'''
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).
'''


# пари біграм із п'яти найчастіших
def create_pairs(b1, b2):
    start_bigrams = []
    pairs = []
    for plain in b1:
        for encrypted in b2:
            start_bigrams.append((plain, encrypted))
    for i in start_bigrams:
        for j in start_bigrams:
            if not i == j and not (j, i) in pairs and i[0] != j[0] and i[1] != j[1]:
                pairs.append((i, j))
    return pairs
```

Пишемо функцію для створення можливих пар з п’яти найчастіших у мові та у даному шифртексті.

```python
# перетворення біграми в число
def get_x(bigram):
    return alphabet.index(bigram[0]) * 31 + alphabet.index(bigram[1])


# перетворення числа в біграму
def get_bigram(value):
    return alphabet[value // 31] + alphabet[value % 31]
```

За наданими формулами пишемо функції перетворення біграми в число та навпаки.

```python
# визначення параметру a(атака на афінний шифр)
def find_key(pair):
    x1, y1 = get_x(pair[0][0]), get_x(pair[0][1])
    x2, y2 = get_x(pair[1][0]), get_x(pair[1][1])
    x, y = x1 - x2, y1 - y2
    roots = solve(x, y, 31 ** 2)
    if roots is None:
        return None
    key = []
    for a in roots:
        key.append((a, (y1 - a * x1) % 31 ** 2))
    return key
```

Пишемо функцію атаки на шифр: використовуємо написану програму вирішення лінійних порівнянь та повертаємо можливі ключі.

```python
# знаходження кандидатів на ключ
def get_keys(pairs):
    keys = []
    for pair in pairs:
        key = find_key(pair)
        if key:
            for k in key:
                keys.append(k)
    return keys
```

Функція знаходить ключі для всіх створених пар біграм та повертає їх.

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

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



# дешифрування тексту
def decrypt(text, key):
    decrypted_text = ""
    for i in range(0, len(text) - 1, 2):
        y = get_x(text[i: i + 2])
        x = (extended_euclid(key[0], 31 ** 2)[1] * (y - key[1])) % 31 ** 2
        decrypted_text += get_bigram(x)
    return decrypted_text
```

За допомогою наданої формули реалізуємо функцію дешифрування тексту.

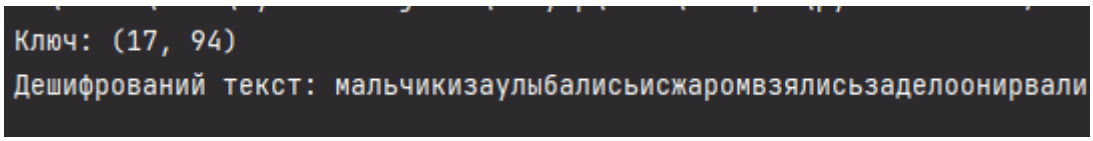
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

```
# автоматична перевірка змістовності тексту
def check(text, keys):
    wrong_bigrams = ['еь', 'юы', 'яы', 'аы', 'оы', 'иы' 'аь', 'оь', 'ыь', 'уь', 'зы', 'ыы', 'уы', 'еы', 'юь', 'яь', 'эь', 'ць']
    meaning = True
    for key in keys:
        decrypted_text = decrypt(text, key)
        for wrong in wrong_bigrams:
            if wrong in decrypted_text:
                meaning = False
        if meaning:
            return key, decrypted_text
        meaning = True
```

Реалізована перевірка змістовності тексту. Створений список неможливих для російської мови біграм, після чого проводимо ітерацію по можливим ключам: дешифруємо текст і якщо в отриманому тексті наявна хоч одна з неможливих біграм, ключ відкидується.

```
with open('8.txt', 'r', encoding='utf-8') as file:
    text = file.read().replace('\n', '')

common_encrypted_bigrams = list(bigram_frequency(text).keys())[:5]

pairs = create_pairs(common_bigrams, common_encrypted_bigrams)

keys = get_keys(pairs)

key, result = check(text, keys)
print('Ключ:', key)
print('Дешифрований текст:', result)

with open('decrypted_text.txt', 'w', encoding='utf-8') as file:
    file.write(result)
```

Використовуємо реалізовані функції та отримуємо результат.



Розшифрований текст:
мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтонаводняю
твесьмирпереплескиваютсяслужаекнамощеныеулицытихонькостучатсявпрозрачныеокнап
огребовнезнаютугомонуиудержуивсевокругзаливаютслепящимсверканиемрасплавленного
солнцакаждоелетооniточносцеписрываютсясказалдедушкапустьихянепротиввонихскольк
остоятгордыекакльвыпосмотришьнанихподольшетакипрожгутутебявглазахдыркуведьпрос
тойцветокможносказатьсорнаятравниктоеенезамечаетамыуважаемсчитаемодуванчикблаг
ородноерастениеонинабралиполныемешкиодуванчиковиунесливнизвпогребвывалилиихиз
мешковивотьмепогребаразлилосьсияниевинныйпрессдожидалсяихоткрытыйхолодныйзол
отистыйпотоксогрелегодедушкапередвинулпрессповернулручкузавертелбыстрейбыстрейи
прессмягкостиснулдобычунувотвоттаксперватонкойструйкойпотомвсещедреeобильнеепоб
ежалпожелобувглиняныекувшинысокпрекрасногожаркогомесяцаемудалиперебродитьснял
ипенуиразлиливчистыебутылкиизподкетчупаионивыстроилисьрядаминаполкахпоблескива
явсумракепогребавиноизодуванчиковсамыеэтисловаточнолетонаязыкевиноизодуванчиков
пойманноеизакупоренноевбутылкилетоитеперькогдадугласзналпонастоящемузналчтоонж
ивойчтоонзатемиходитпоземлечтобывидетьиощущатьмиронпонялещеоднонадочастицувсе
гочтоонузналчастицуэтогоособенногоднядняснбораодуванчиковтожезакупоритьисохранить
апотомнастанеттакойзимнийянварскийденькогдавалитгустойснегисолнцаужедавнымдавно
никтоневиделиможетбытьэточудопозабылосьихорошобыегосновавспомнитьвоттогдаонего
откупоритведьэтолетонепременнобудетлетомнежданныхчудесинадовсеихсберечьигдетоот
ложитьдлясебячтобыпослевлюбойчаскогдавздумаешьпробратьсянацыпочкахвовлажныйсу
мракипротянутьрукуитамрядзарядомбудутстоятьбутылкисвиномизодуванчиковонобудетм
ягкомерцатьточнораскрывающиесяназарецветыасквозьтонкийслойпылибудетпоблескиват
ьсолнценынешнегоиюнявзглянисквозьэтовинонахолодныйзимнийденьиснеграстаетизподн
егопокажетсятраванадеревьяхоживутптицылиствaицветысловномириадыбабочекзатрепещ
утнаветруидажехолодноесероенебостанетголубымвозьмилетоврукуналейлетовбокалвсамы
йкрохотныйконечноизкакоготолькоисделаешьединственныйтерпкийглотокподнесиегокгу
бамипожиламтвоимвместолютойзимыпобежитжаркоелетотеперьдождевойводыконечнозд
есьгодитсятолькочистейшаяводадальнихозерсладостныеросыбархатныхлуговчтовозносятс
яназарекраспахнувшимсянавстречунебесамтамвпрохладныхвысяхонисобиралисьчистоом
ытымигроздьямиветермчалихзасотнимильзаряжаяпопутиэлектрическимизарядамиэтавода
вобралавкаждуюсвоюкаплюещебольшенебескогдападаладождемназемлюонавпиталавсебя
восточныйветеризападныйисевернyйиюжныйиобратиласьвдождьадождьвэтотчассвященн
одействияужестановитсятерпкимвиномдуглассхватилковшвыбежалводвориглубокопогруз
илеговбочоноксдождевойводойвотонаводабылаточношелкпрозрачныйголубоватыйшелкес
лиеевыпитьонакоснетсягубгорласердцамягкокакласканоковшиполноеведронадоотнестивп
огребчтобыводапропиталатамвесьурожайодуванчиковструямиречекигорныхручьевдажеба
бушкавкакойнибудьфевральскийденькогдабеснуетсязаокномвьюгаислепитвесьмириулюде
йзахватываетдыханьедажебабушкатихонькоспуститсявпогребнаверхувбольшомдомебудет
кашельчиханьехриплыеголосаистоныпростуженнымдетямоченьбольнобудетглотатьаносы
унихпокраснеютточновишнивынутыеизналивкивсюдувдомепритаитсяковарныймикробито
гдаизпогребавозникнетточнобогинялетабабушкапрячатотоподвязанойшальюонапринесет

эточтотовкомнатукаждогоболящегоиразольетдушистоепрозрачноевпрозрачныестаканыист
аканыэтиосушатоднимглоткомлекарствоиныхвременбальзамизсолнечныхлучейипраздног
оавгустовскогополудняедваслышныйстукколестележкисмороженымчтокатитсяпомощены
мулицамшорохсеребристогофейерверкачторассыпаетсявысоковнебеишелестсрезаннойтра
выфонтаномбьющейизподкосилкичтодвижетсяполугампомуравьиномуцарствувсеэтовсево
дномстаканедадажебабушкакогдаспуститсявзимнийпогребзаиюнемнавернобудетстоятьта
мтихонькосовсемоднавтайномединениисосвоимсокровеннымсосвоейдушойкакидедушкаи
папаидядябертидругиетожесловнобеседуястеньюдавноушедшихднейспикникамистеплым
дождемсзапахомпшеничныхполейижареныхкукурузныхзеренисвежескошенногосенадаже
бабушкабудетповторятьсноваисноватежечудесныезолотящиесясловачтозвучатсейчаскогда
цветыкладутподпресскакбудутихповторятькаждуюзимувсебелыезимывовсевременасноваи
сноваонибудутслетатьсгубкакулыбкакакнежданныйсолнечныйзайчиквотьмевиноизодуван
чиковвиноизодуванчиковвиноизодуванчиковониприходилинеслышноуходилипочтибесшу
мнотравапригибаласьираспрямляласьвновьонискользиливнизпохолмамточнотениоблаковэ
тобежалилетниемальчишкидугласотстализаблудилсязадыхаясьотбыстрогобегаоностанови
лсянакраюовраганасамойкромкенадпропастьюиоттудананегодохнулохолодомнавостриву
шиточнооленьонвдругучуялстаруюкакмиропасностьгородраспалсяздесьнадвеполовинызд
еськончиласьцивилизацияздесьживетлишьвспухшаяземляежечасносовершаетсямиллионс
мертейирожденийиздесьпроторенныеилиещенепроторенныетропытвердятчтобыстатьмуж
чинамимальчишкидолжныстранствоватьвсегдавсюжизньстранствоватьдугласобернулсяэт
атропаогромнойпыльнойзмеейскользиткледяномудомугдевзолотыелетниеднипрячетсязим
аатабежиткраскаленнымпесчанымберегамиюльскогоозераавонтакдеревьямгдемальчишкип
рячутсямежлистьевточнотерпкиеещенезрелыеплодыдикойяблониитамрастутизреютавотэт
акперсиковомусадуквиноградникукогороднымгрядамгдедремлютнасолнцеарбузыполосат
ыесловнокошкитигровоймастиэтатропазаросшаякапризнаяизвилистаятянетсякшколеатапр
ямаякакстрелаксубботнимутренникамгдепоказываютковбойскиефильмывотэтавдольручья
кдикойлеснойчащедугласзажмурилсяктоскажетгдеокончаетсягородиначинаетсялеснаяглуш
ьктоскажетгородврастаетвнееилионапереходитвгородиздавнаинавекисуществуетнекаянеу
ловимаяграньгдеборютсядвесилыиоднанавремяпобеждаетизавладеваетпросекойлощинойл
ужайкойдеревомкустомбескрайнееморетравицветовплещетсядалековполяхвокругодиноки
хфермалетомзеленыйприбойяростноподступаетксамомугородуночьзаночьючащилугадаль
ниепросторыстекаютпооврагувсеближезахлестываютгородзапахомводыитравигородсловн
опустеетмертвеетивновьуходитвземлюикаждоеутрооврагещеглубжевгрызаетсявгородигро
зитпоглотитьгаражиточнодырявыелодчонкиипожратьдопотопныеавтомобилиоставленные
намилостьдождяиразедаемыержавчинойэйаусквозьтайныоврагаигородаивременимчалисьд
жонхафичарливудменэйдугласмедленнодвинулсяпотропинкеконечноеслихочешьпосмотре
тьнадвесамыеглавныевещикакживетчеловекикакживетприроданадоприйтисюдаковрагувед
ьгородвконцеконцоввсеголишьбольшойпотрепанныйбурямикорабльнанемполнонародуивс
ехлопочутбезусталивычерпываютводуобкалываютржавчинупоройкакаянибудьшлюпкахиб
аркадетищекораблясмытоенеслышнойбурейвременитонетвмолчаливыхволнахтермитовим
уравьеввраспахнутойовражьейпастичтобыощутитькакмелькаюткузнечикиишуршатвжарки
хтравахточносухаябумагачтобыоглохнутьподпеленойтончайшейпылиинаконецрухнутьгра
домкамнейипотокомсмолыкакрушатсятлеющиеугликостразажженногогромомисинеймолн
иейнамигозарившейторжестволесныхдебрейтаквотзначитчтотянулосюдадугласатайнаявой
начеловекасприродойизгодавгодчеловекпохищаетчтотоуприродыаприродавновьберетсвое
иникогдагородпонастоящемудоконцанепобеждаетвечноемугрозитбезмолвнаяопасностьон

вооружилсякосилкойитяпкойогромныминожницамионподрезаеткустыиопрыскиваетядомв редныхбукашекигусеницонупрямоплыветвпередпокаемувелитцивилизациянокаждыйдомт огоиглядизахлестнутзеленыеволныисхоронятнавекиакогданибудьслицаземлиисчезнетпосл еднийчеловекиегокосилкиисадовыелопатыизеденныержавчинойрассыплютсявпрахгородч ащадомаоврагдугласозадаченномигаетнокакаяжесвязьмежчеловекомиприродойкакпонять чтозначатонидругдлядругакогдаонопустилглазапервыйлетнийобрядпозадиодуванчикисоб раныизаготовленывпрокпорараприступатьковторомунодугласзастылинедвижетсясместадугп ошлидугголосазатихливдалекеяживойсказалдугласночтотолкуониещебольшеживыечемяка кжеэтокакжетаконстоялводиночествеглядянасвоиногиневсилахдвинутьсясместаинаконецп онялвтотвечердугласвозвращалсядомойизкиновместесродителямиибратомтомомиувидели хвяркоосвещеннойвитринемагазинатеннисныетуфлидугласпоспешноотвелглазаноегоноги ужеощутилиприкосновениепарусиныизаскользилиповоздухубыстрейбыстрейземлязаверте ласьзахлопалиполотняныенавесынадвитринамитакойонподнялветертаконмчалсяродители итомшагалинеторопясьамеждунимипятясьзадомшелдугласинесводилглазстеннисныхтуфе льтампозадивполуночнойвитринехорошаябылакартинасказаламамаагабуркнулдугласстоял июньдавноминовалотовремякогданалетопокупаюттакиетуфлилегкиеитихиеточнотеплыйд ождьчтошуршитпотротуарамужеиюньиземляполнапервозданнойсилыивсевокругдвижется ирастеттраваипосейденьпереливаетсясюдаизлуговомываеттротуарыподступаеткдомамкаж етсягородвотвотчерпнетбортомипокорнопойдетнадноивзеленомморетравнеостанетсянивс плесканирябидугласвдругзастылточновросвмертвыйасфальтикрасныйкирпичулицыневсил ахтронутьсясместапапвыпалилонвонтамвокнетеннисныетуфлиотецдаженеобернулсяазаче мтебеновыетуфлискажипожалуйстаможешьтымнеобяснитьнуудазатемчтовнихчувствуешь себятакбудтовпервыевэтолетоскинулбашмакиипобежалбосикомпотраветочновзимнююноч ьвысунулногиизподтеплогоодеялаиподставилветручтодышитхолодомвоткрытоеокноиони стынутстынутапотомвтягиваешьихобратнопододеялоионисовсемкаксосулькивтеннисныхт уфляхчувствуешьсебятакбудтовпервыевэтолетобредешьбосикомполенивомуручьюивпроз рачнойводевидишькактвоиногиступаютподнубудтооніпереломилисьидвижутсячутьвпере дитебяпотомучтоведьвводевсевидитсянетакпапсказалдугласэтооченьтруднообяснить

Висновок

В ході комп’ютерного практикуму були отримані навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опановані прийоми роботи в модулярній арифметиці. Були реалізовані підпрограми з необхідними математичними операціями, знайдені найчастіші 5 біграм у наданому шифртексті та у російській мові, після чого отримані пари та ключі. За допомогою автоматичного розпізнавача змістовності тексту був отриманий ключ (17, 94) та розшифрований текст.