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

Криптологія
Комп’ютерний практикум

Робота №3

Виконали:
студенти групи ФБ-14
Мартиненко Даніїл
Цуканов Данило

Київ-2023

Мета роботи:

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

Шифртекст варіанту 4:

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощкяоэою
этцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыеныбдьмиыыяшцрб
гянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмяояйывщеыйсбжощлзшя
рфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглр
зщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдхпезхлсопжипеызохлншплбй
щждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезжурфешщпнзшятоужертцлвяхщжпофожущпкк
шяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозноюуйэвзхягжжзщрф
яоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмогйжш
фшайрмлзннтзхаокшйбчаощяанбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфмовоцяанфшл
яйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочскввжаббжнзбляьхзскктцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшя
полфзятзбжьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщо
цыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггднотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэ
бтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхлдырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйк
рзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозые
ыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйз
хйшмшжшалтыбжхябжюакцопиыщчыдншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпонойкыпюш
щчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюши
мйшлыпутцурряешбзкцколппотзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзхлцюпзхщж
щккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксааножутоао
нзскккрздвюптжждшсэыпзыцяделоцлыбжанхмлзннсюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряешйкешзо
ешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлце
ызоножяяоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзцжжущпрф
уяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеызоешыедвайнинзшязпкцрфеш
мяеыцпяовкрфекуяжубждоджглкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшо
щжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэжйуппбзлж
фяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмз
юдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбыцжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямзюдечрэйкиордиыцпя
мфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкцкпоноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыо
цюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшясжеьзоешрйэжпзжжбяаоешывбзлжцшшйфшрэщ
жсокыйшлцлыксфохямвмуйчжуезаяалжшбчшшфссешмяпзюнзоешедвдвлгфезшйдбряилгфеыхзскчквкщыезтлыниоовмушссожзбибзв
фвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюнешибряшяякжшбчфуэжмзчшвд
щкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцыыиеыыявлаомяркгяшптцпмдущесзноншшкм
окцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбзбяшжддыцшдзщжэзччамекуяанюзскжуэыоцлзшящжбж
дояоратлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоуже
ртцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячовунщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуф
аляятфсчподояоносшншмоешдбждтззпсчжшбчншщзнэйсеньовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзеюко
щеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчбюпповбнзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяп
ндощкпорфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтз
вжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеы
йсжулямрчфюшпфмяяявлвжипюпэышбмунрчфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовккшяабйчуцжелжрбрякывд
юшлвоходошзяобпбжжуэырйбзщтелмяилщкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщк
гфсймовккцивыйгшьльфжшншмолдопсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжюп
муяззощуиврймзвожзпофотывдохлцюпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулва
йншопэзцжбкюнзоносочзсыяхщжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказхяанаоешезв
жбякбмурфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупа
йтзншщзнэйсшкопншфузхпмдьюшшящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхззоскфопбоцщкчфылидмышкбмщпбкуяяоек
зожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчхябфбждоцпюдлвямэжглцяекжшскч
йфибяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфлцабгя
ыювояфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыыядвзбряжзлжипюпоцчбптдохлибвоанаопоьшй
кешзокюыврухкнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгяыкаяшябялб
гцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаоешезвжпонопмйкйвюпууэжжйю
шряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйскпонзшясшмышйсщжшз
псчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяег
дяуяряоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшярллзджипюшлцлырэчмзуиыяхскмыуф
оцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюдншуусйшфкзныб
жхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпеяпыэжйэзпэыгднншуущешфалноыжглл
кеыщжуясащуивхзак

Завдання:

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.

```
def extended_gcd(a, b):
    if a == 0:
        return b, 0, 1
    else:
        g, x, y = extended_gcd(b % a, a)
        return g, y - (b // a) * x, x

def mod_inverse(a, m):
    g, x, y = extended_gcd(a, m)
    if g != 1:
        return None
    else:
        return x % m
```

(розв’язування лінійних рівнянь вбудовано в функцію пошуку потенційних ключів, далі буде)

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 count_bi(text):
    c2_nocross = dict()
    i = 0
    while True:
        if (i >= len(text) - 1):
            break
        b = text[i] + text[i + 1]

        if b not in c2_nocross.keys():
            c2_nocross[b] = 0
        c2_nocross[b] += 1
        i += 2
    return c2_nocross
```

```
['еш', 'еы', 'шя', 'ск', 'до']
```

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).

```
def count_a_b(bi, most_bi):
    for bi1 in bi:
        Y1 = alphabet.find(bi1[0]) * m + alphabet.find(bi1[1])
        for bi2 in bi:
            if bi2 != bi1:

                Y2 = alphabet.find(bi2[0]) * m + alphabet.find(bi2[1])

                result = dict()
                for mos1 in most_bi:
                    X1 = alphabet.find(mos1[0]) * m + alphabet.find(mos1[1])
                    for mos2 in most_bi:
                        if mos2 != mos1:
                            X2 = alphabet.find(mos2[0]) * m +
alphabet.find(mos2[1])
                            d = extended_gcd(X1 - X2, m ** 2)[0]
                            if d == None:
                                continue
                            if d == 1:
                                a = ((Y1 - Y2) * mod_inverse(X1-X2, m**2)) %
(m ** 2)
                                b = (Y1 - a * X1) % (m**2)
                                result[a] = b

                            elif d > 1:
                                if (Y1 - Y2) % d == 0:
                                    X0 = (Y1 - Y2) // d * mod_inverse((X1 -
X2) // d, (m ** 2) // d)
                                    for i in range(d):
                                        a = (X0 + i * ((m ** 2) // d)) % (m
** 2)
                                        b = (Y1 - a * X1) % (m ** 2)
                                        result[a] = b

    return result
```

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

```
def calculate_index_of_coincidence(text):
    frequencies = {}
    for char in text:
        if char in frequencies:
            frequencies[char] += 1
        else:
            frequencies[char] = 1
    ic_value = sum([(count * (count - 1)) for count in
frequencies.values()]) / (len(text) * (len(text) - 1))
    return ic_value
```

```
def decrypt(text, a, b):
    result = ''
    a = mod_inverse(a, m ** 2)
    if a == None:
        return -1
    i = 0
    while True:
        if (i >= len(text) - 1):
            break
        Y = alphabet.find(text[i]) * m + alphabet.find(text[i + 1])
        X = a * (Y - b) % (m ** 2)
        result += alphabet[X // m] + alphabet[X % m]
        i += 2
    return result


def decrypt_keys(text, keys):
    textes = dict()
    for i in keys:
        d_text = decrypt(text, i, keys[i])
        index = calculate_index_of_coincidence(d_text)

        if abs(index - 0.0553) < 0.01:
            textes[i, keys[i]] = d_text
    return textes
```

Відсіювання текстів відбувається, як і в другій ЛР, за допомогою індексів відповідності (якщо текст змістовний, то його ІВ близький до ІВ мови)

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

Висновки:

продовжуємо вивчати атаки на шифри за допомогою частотного аналізу. В цій ЛР на прикладі афінного шифру, в якому біграми заміняються на інші за формулою y =ax+b. При розшифруванні робиться припущення, що 2 з найпопулярніших біграм мови переходять в 2 з найпопулярніших біграм шифртексту, створюється система рівнянь, з якої можна знайти потенційні значення ключа. Оскільки таких значень багато і вручну перевіряти тексти було б нераціонально, був обраний спосіб відсіювання текстового шуму за допомогою індексів відповідності (якщо текст змістовний, то його ІВ близький до ІВ мови).