МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

КРИПТОГРАФІЯ

Комп’ютерний практикум №3

«Криптоаналіз афінної біграмної підстановки»

Перевірив:
Чорний О.М.
Савчук М.М.
Завадська Л.О.

Виконали:
Студентки групи ФБ-71
Гресь В.В.
Нацвін К.А.

Київ 2019

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
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.

Критерій відбору ключів:

Під час виконання роботи ми виявили, що можливих ключів може бути велика кількість і аби дарма не перенавантажувати програму, було вирішено скористатися методом відбору ключів, а саме критерієм заборонених біграм. Якщо розшифрований текст містив у собі біграми «аь», «юь», «уь», «еь», «йй», то ключі для його розшифрування відразу ж відкидались, що значно спрощувало пошуки істинного ключа.

Результати:

Розшифрування тексту за варіантом 22:
Використавши основи модулярної арифметики, критерій відбору ключів та частотний аналіз, було знайдено таку пару ключів:
a = 690, b = 91

Найчастіші біграми ШТ
ню
мт
бй
эю
шс

Шифрований текст:

Нюцюиюцээюзщыреибзцйбйщоткишязбйнййттшяроаужрцяшровзюобзуйзлжкяслаэвюяэкпакюясшратнйкхц
сзуывшсртлюзвнйчснюжажюрьбзгбэхэюдфцюеышсцэечыюгболхзцйткйэуйшжюшлкрзиэбйнйабьцэюсзмфф
юттгшярбйтыпйяшдснюгбэхмфахбшэщисмстюэюсянюоюеюхкнжеисзмфлшмчэяздбшчзткрзиэжюфрухжабкр
зиэфсзщкбпйнйуиуткббзфскожювйкбшамткбгвабцйлкрзиэесоюпэютутирыюгюисющьццжбшдснюэорнзсясч
ьыпечгфцсшсжюобьцэюцэцэмфцюыкаюмтхатюгболэщцйчзэкнжцйпсфюыюхадфьицсеьфкеокбнюцзрцжвабы
рырйтмтжзбйьабзчьеюэюжажюыюьибзовзлсябшэкфямпщоцчцзрптоатакыснюэсфсяаэюфыномтфстюэююотдо
зтдощзцхщкабйпшащэцэхаашейязрсжзодцйпсшсззютюдэтнюмтйккхтонйдонююйэтщзшйуимтжюстжзвядоэк

овкмяшьищкарщнжюесмтфяьабзцэясюйьищколовхпжаиалтывткдомазйэащтьцсящофымзэсюзэчщжутпсэсас
ийьцбйюяхпкксшюямпечжааюдзыжтшмчбзшйязщкрцдозщкбпйяшдснюэкцйжаабткуугсссльфхюнорчаэочтна
овдозяцйщэткфсзвюяпсхышсцэбйюяяштышсцэфскожюпамфссмфсяпйцзгфечшсэсгвабцйпйкьчешснющкрцг
юцэясцсюыцйощщзуыномтлацйнсябнйпояшйзйтьцгюютутэкэкшсейчзэонжсящаутевятэкпаашиовзавюяэккзч
йкрьцгюйпцйщоцчгватвтахмстфызпсмамфнюесцэясьиутжюойнжюшсяубатйышсбйнйишпыызфюцснюовхпц
зчьеюэюелйпдаэсжючяшлйпщовзюовзхршсшстфцсткмфнюэойтцйщешсэсеюясцэясбйгчнюэюзтоазщжюбатю
эювзыхютапгютфызюяяшбдцйфырцбйгжюшбйгжюшбйкрireижюесмттомазйдюмазйсщисссыаэюнюцюиюла
ыазсмттвяшйкцттшярбйкркбкйгжятзоихэсмтсажацсщьбзшзиюмфпсашбкгжнзчйфырцбйцййппсцэясбйцьгюо
хэюдфутщколесеюуйзлвттшярэкьваткбсзкзазджюштшрццсщйшббйяшйжбшщжпоатржтшбдыыабкяььуаюаэа
псцяирьцгюцээющйшбуцэюрьнючшгчгбэхэюдфбйьщжыпабзяэмчуюэюечесщьэафщяамчуюьдзлайшбжюгюц
ээюшстфцссяпсщьуфывкйишщчсжюшбйхпбзнсмтжвапбздазбткказмтабвзыфмчбзнсьвбматаккыабнжжюрюдб
кбзццжюяжмчвлдонюцюиюэкхкцчнюкзтфпсфьщкеодояшжельбзяйэкмфнжжюдзжатаасшсщьнюссыаэюмстф
ксаьесфстфмтлащорцчсймткеоцйчснюгюззбзцээюзшзцсятвнюабачхзэсбзяйэкмфжаютшлжвюдязрсмтжвбйщ
щмзжюбзфюыюясдфьижкбшчзющмзььфюыюясдфцюизмтткеоцйпсцэмфесьвхбрсщкабфышсбзцэясжафюцсн
чйксьуажзэсесьвутдапсцянйаткдгчцбыыяшйкщьдзжадабзясшрэкмфуфывроязовлкэтмтлатоэкнжцйпсмткрьцг
юбйсскздкцзэюмфашейязютбйыжьясщяачтпсдахацсцядсежзхдккышсцэютбйыжьязожюбцдожвцйцйроишбйа
ткдкйатдпишфзфсзщкбпйнйххбйгчцбыыяшжешсэщяацаьэтюэюзтйзэснждзиянжискзечйккзюытоэкпацсшсж
ютщйздщбйчтххгтирдоухззфюыкбзнятшяйщжюшщжятсарсщкабэщэкрзкзьйыыухшйдллшдоуткбютйззхацэ
бйцэдкфсмсцзпсшйиртшцйэлцэовэкбшязььнабшйжлафргчнйщэюоюавьльцюцсэсзатфпсэсфсийцйххашейязу
фывжацсцянйрцдожвбшжаузэсэкфсзлфьщкеоелайаткддаашейязцэясжыщоаяпсютуттякстюшсцяатирэтудтоба
язгжюшлкфюыющэфющцдожвчтахщкарчзюзхксэлшцйщэткястюашоькзызжатщэюфьдзэсщзюзурнйнсфтьцж
ышсуфывцэзпцйатриузясжзайчсфтьцжышснюцюиюфьщкеодоящцбхпчьрсмскашббоикызуккзсзжальзасьювр
омтжзшйдловрцжюесюкэтмтласрутжвеибйтыномтфстюэюявзцпйхбьижацсцяроэсясзьбзовзлсябшжышсцэечя
зутпсызжаукуфывкбзсчшрорипабзшстфцсчнмсифвздахакмабцйязвзэсмтжвбймйсямпдашсзвсябзяйеиовечню
рмьивзыхасзтфыткцсияььлжхбхпчьщьдыпйеиопцййапструтжвеибйгчнюэюбзфртшярощяашзисбоцсзудщйти
сщкцсэсасмтвюлвогцйьатюпсюйщжишдодсзвюябзфкфюбкэкзяфюисмтдодловчзпюэюзбэкгочщырясжамфахз
сфрдофршбдцсяжафюзснюовзяясмаэюнюцюыззэсжзмфпйаткдйкжюесмтунвлтюпаэюдфыюзтубиктфбзгбутчх
нюыюовкмцйчзесттжвродлсявтйвнйкьзвкбнюцюиюнюмтзхэюнюшсхышсцээсжзмфйцдойтдййтирфющцдои
шжсцэайдоцйпсоякбывэкшсяэнтйзмтьсюксьиюмфнюесщьзвлксьлжбюютнжжцдойтцтирфющцдоишвюлвогц
йьатюпсюйатйзмтзойнбзцзчнбзовощжкфюейжсойеижзузсйжсюзойэахаыюэтщзжалвогпйдщбйжюлаясдфзткь
взвячзнюцюбабйрочьыззэойзещэкрзюзрьзщудпсэсшзыарафкцсэсрзузжаейюяэхэюдфюткбтшвттюасзсззкзджт
шбдишсртвмтлассихрсмтжюссюафртэтюыстяыршсжюпсрсчшйкбшйкдймпишнйчзнюцюбаэщжвпыбшхзгжи
шдоеизцжюьзнютонйдонюртяааюоюпсшаовзлсябшщжьявтдйаткдчамстфызэыйкмфэйелсябшхзаьззбззщшмж
ннюцюиюмсцшйксщицсзщатзощзцхыюэтщзжаасзщудпсубпоухдфлкгбфвцйчззсцзтюбкзооюзсзяпвпсткфсдщэ
юмфдамттвцйярщнеюлтбшунрсувьцухдфутэохптканюцюиюяэссыаэюнютьмтмйщэаьхадэовцчжюлйчсэокм
цйщэаьзвцйбзнчтвьиасрсжзльзцжюьзщэтонйдощэнюцюиюэсжзэюбзщкфсабовзлсялюмуывготоцсшсисещэкя
стюрйщжаппсджишдоеицэдкдхдзшйкржздфеюмтисуаеаяэрсцсцпечжамуывготовзцящжюшкбяшбйтвсянйатк
дйкюзясфсукцюпслахадфнюовтосыпсабткшссзщзыацспсджапчзббатывтоцзэюшйеиучюярзфсэссшфвэкьапсф
сзяохнюцюбафьщкеоэкюащзжатщывзяжзханарйдщэкпамасэзсюоатпояшйзсрьцгюбйрозутубзовтосыщээыйкэ
тжючшхяейтыывщэйшкрмсмаьиеюкзяаэкжздзшйрилкжзаююаэсщзьдшбэщывзяжаюаэойткбэтжюююгюьдшб
ечырнюлшздяшгчзьналшйпцэыюцсшстэюабййкцюжюэюдфлшзявтсщбйшбухзлцсцядснюасжаеюэюзлязхалй
йзфьщкеоэкэооаюауткзурцбэщяарсзяпйцшэкярязззсхаеосрьцгюбйнйдщбйшбяшхзаздзлшюяэквйязцэясчьеюм
фютапишнйчзасжаеюмфщкязмтюцквесмтйышсасжаеюмфщкрцбйишщчкышснюесшстфцсжзяамфжстяроата
ксжьцерутжврицепаюавьгэбйтыномтфстюэючщжюпшцшязчькусснюевткпаэюдфсшнйцшйксацсцянйдщбйш
бяшатуттшяркьуюоюбксщывзяэойзжбывюсмтуновэкбшщжьцьщисмтвтмзмчровзыющкдаасюаястюмфзсхаео
зрутжвхббйщжтшбдщовзэсутгютюэюдфцэхазсхаеосвйкфюейххфскожюрюбкфякбеигвнйжаэыйкэтжюцсцяро
мтщзаюхадфшстфцсфюшзммкрмдзябацйтвщжутьяфссйкртохбйтробааьхамьтоесеюгздзщкткююханюцюиюл
ккэгэтюэюпсфсзяохбзыыномтфсфсрбаппсмтэазщжюпшцйххвзыхутэооаищжвырдотоцчзсяйэкпапсфсэылкшс
цпечжалкаюмтххвю

Розшифрований текст:

наташабыласпокойнееноневеселееонанетолькоизбегалавсехвнешнихусловийрадостибаловкатаньяконцертов
театраноонаниразунесмеяласьтакчтобыиззасмехаеенеслышныбылислезыонанемоглапетькактольконачинала
онасмеятьсяилипробовалаоднасамассобойпетьслезыдушилиееслезыраскаянияслезывоспоминанийотомневоз
вратномчистомвременислезыдосадычтотакзадаромпогубилаонасвоюмолодуюжизнькотораямоглабыбытьтак
счастливасмехипениеособенноказалисьейкощунствомнадеегоремококетствеонаинедумаланиразаейнеприход
илосьдажевоздерживатьсяонаговорилаичувствовалачтовэтовремявсемужчиныбылидлянеесовершеннотожеч
тошутнастасьяивановнавнутреннийстражтвердовоспрещалейвсякуюрадостьдаинебыловнейвсехпрежнихинт
ересовжизниизтогодевичьегобеззаботногополногонадеждскладажизничащеиболезненнеевсеговспоминалаон
аосенниемесяцыохотудядюшкуисвяткипроведенныесвотрадномчтобыонадалачтобывозвратитьхотьодиндень
изтоговременинуожэтонавсегдабылоконченопредчувствиенеобманывалоеетогдачтотососостояниесвободыиотк
рытостидлявсехрадостейникогдауженевозвратитсяболышеножитьнадобылоейотраднобылодуматьчтоонанелу
чшекаконапрежедедумалаахужеигораздохужевсехвсехктотолькоестьнасветеноэтогомалобылооназналаэтоисп
рашиваласебячтождальшеадальшеничегонебылонебылоникакойрадостивжизниажизньпроходиланаташавид

имостараласьтольконикомунебытьвтягостьиникомунемешатьнодлясебяейничегоненужнобылоонаудалялась отвсехдомашнихитолькосбратомпетейейбылолегкоснимоналюбилабыватьбольшечемсдругимиииногдакогда быласнимсглазунаглазсмеяласьонапочтиневыезжалаиздомуиизприезжавшихкнимрадабылатолькоодномупье рунельзябылонежнееосторожнееивместестемсерьезнееобращатьсячемобращалсяснеюграфбезуховнаташаосс сознательночувствовалаэтунежностьобращенияипотомунаходилабольшоеудовольствиевегообществеоонад аженебылаблагодарнаемузаегонежностьничтохорошеесостороныпьеранеказалосьейусилиемпьеруказалосьта кестественнобытьдобрымсовсемичтонебылоникакойзаслугивегодобротеиногданаташазамечаласмущениеине ловкостьпьеравееприсутствииивособенностикогдаонхотелсделатьдлянеечтонибудьприятноеиликогдаонбоялс ячтобычтонибудьвразговоренненавелонаташунатяжелыевоспоминанияоназамечалаэтоипринисывалаэтоегооб щейдобротеизастенчивостикотораяпоеепонятиямтаковаяжекакснеюдолжнабылабытьисовсемипослетехнечая нныхсловотомчтоежелибыонбылсвободеноннаколеняхбыпросилеерукиилюбвисказанныхвминутутакогосиль ноговолнениядлянеепьерникогданеговорилничегоосвоихчувствахкнаташеидлянеебылоочевидночтотесловат огдатакутешившиееебылисказаныкакговорятсявсякиебессмысленныесловадляутешенияплачущегоребенкане оттогочтопьербылженатыйчеловекнооттогочтонаташачувствоваламеждусобоюиимввысшейстепенитусилун равственныхпреградотсутствиекоторойоначувствоваласрагинымейникогдавголовунеприходилочтобыизееот ношенийспьероммоглавыйтинетольколюбовьсееилиещеменеесегосторонынодажеитотроднежнойпризнающе йсебяпоэтическойдружбымеждумужчинойиженщинойкоторойоназналанесколькопримероввконцепетровско гопостааграфенаивановнабеловаотрадненскаясоседкаростовыхприехалавмосквупоклонитьсямосковскимуго дникамонапредложиланаташеговетьинаташасрадостьюухватилась3аэтумысльнесмотряназапрещениедоктора выходитьраноутромнаташанастояланатомчтобыговетьиговетьнетаккакговелиобыкновенновдомеростовыхто естьотслушатьнадомутрислужбыачтобыговетьтаккакговелааграфенаивановнатоестьвсюнеделюнепропуская ниоднойвечерниобедниилизаутренаграфинепонравилосьэтоусердиенаташионавдушесвоейпослебезуспешно гомедицинскоголеченияиадеялась чтомолитвапоможетейбольшелекарствихотясострахомискрываяотдоктора носогласиласьнажеланиенаташиипоручилаеебеловойаграфенаивановнавтричасаночиприходилабудитьнаташ уибольшейчастьюнаходилаееуженеспящеюнаташабоялась проспатьвремязаутренипоспешноумываясьиссмир ениемодеваясьвсамоедурноесвоеплатьеистаренькуюмантильюсодрогаясьотсвежестинаташавыходиланапуст ынныеулицыпрозрачноосвещенныеутреннейзарейпосоветуаграфеныивановныНаташаговеланевсвоемприход еавцерквивкоторойпословамнабожнойбеловойбылсвященникивесьмастрогийивысокойжизнивцерквивсегдаб ыломалонародаНаташасбеловойстановилисьнапривычноеместопередиконойбожиейматеривделаннойвзадлев огоклиросаиновоедлянаташичувствосмиренияпередвеликимнепостижимымохватывалоеекогдаонавэтотнепр ивычныйчасутраглядяначерныйликбожиейматериосвещенныйисвечамигоревшимипереднимисветомутрапад авшимизокнаслушалазвукислужбызакоторымионастараласьследитьпонимаяихкогдаонапонималаихееличное чувствоссвоимиоттенкамиприсоединялоськеемолитвекогдаонанепонималаейещесладостнеебылодуматьчтож еланиепониматьвсеестьгордостьчтопониматьвсегонельзячтонадотольковеритьиотдаватьсябогукоторыйвэти минутыоначувствовалауправлялеедушоюонакрестиласькланяласьикогданепонималатотолькоужасаясьперед своеюмерзостьюпросилабогапроститьеезавсезавсеипомиловатьмолитвыкоторымонабольшевсегоотдавалась б ылимолитвыраскаяниявозвращаясьдомойвраннийчасутракогдавстречалисьтолькокаменщикишедшиенаработ удворникивыметавшиеулицуивдомахещевсеспалинаташаиспытывалановоедлянеечувствовозможностиисправ лениясебяотсвоихпороковивозможностиновойчистойжизниисчастияаа

Код програми:

```
import operator

most_common = ['ст', 'но', 'то', 'на', 'ен']
alphabets_2 = 'абвгдежзийклмнопрстуфхцчшщьыэюя'
impossibles = ["аь", "юь", "уь", "еь", "йй"]

def egcd(a, b):
    if a == 0:
        return b, 0, 1
    else:
        gcd, x, y = egcd(b % a, a)
        return gcd, y - (b//a) * x, x


def inverse(a, m):
    g, x, y = egcd(a, m)
    if g > 1:
        #try:
        #if (m*g + 1) % a == 0:
        return x % (m/g)
        #else:
            #print('does not exist')
            #return None
        #except ZeroDivisionError:
            # pass
    else:
        return x % m


def congruence(x1, y1, x2, y2, m):
```

```
    j = 0
    solved = 0
    x = x1 - x2
    y = y1 - y2
    j_list = []
    for i in range(0, m):
        if ((x*i - y) % m) == 0:
            solved = i
            j list.append(i)
            if inverse(i, m) is not None:
                v = y1 - i * x1
                while v < 0:
                    v += m
                j = v % m
    return solved, j


with open('22.txt', 'r', encoding='utf-8') as file:
    data = file.read().replace('\n', '')
    n = 2
    bigrams = [data[i:i + n] for i in range(0, len(data), n)]
    file.close()


def lettc(data):
    all_freq = {}
    for i in data:
        if i in all_freq:
            all freq[i] += 1
        else:
            all_freq[i] = 1
    return all_freq


counted bigrams = sorted(lettc(bigrams).items(), key=operator.itemgetter(1))
counted bigrams.reverse()
print(counted_bigrams[0:5])


def decr(bigr_1, bigr_2, bigr_3, bigr_4):  # bigr_1, bigr_2 - most common   bigr_3, bigr_4 - encoded
    x1 = alphabets 2.find(bigr 1[0]) * 31 + alphabets 2.find(bigr 1[1])
    x2 = alphabets 2.find(bigr 2[0]) * 31 + alphabets 2.find(bigr 2[1])
    y1 = alphabets_2.find(bigr_3[0]) * 31 + alphabets_2.find(bigr_3[1])
    y2 = alphabets_2.find(bigr_4[0]) * 31 + alphabets_2.find(bigr_4[1])
    #print(x1, y1, x2, y2)
    res = congruence(x1, x2, y1, y2, 961)

    return res


bigrams_from_dict = [counted_bigrams[i][0] for i in range(0, len(counted_bigrams))]
ciph_bigrams = bigrams_from_dict[0:5]
temp = [(x, y) for x in most_common for y in ciph_bigrams if x != y]
possible_bigrams = [(x, y) for x in temp for y in temp if x[0] != y[0] and x[1] != y[1] and x[0] != y[1]
                    and y[0] != x[1]]


file1 = open('data.txt', 'w')


def main():
    for j in range(0, len(possible_bigrams)):
        message = ''
        f = decr(possible_bigrams[j][0][0], possible_bigrams[j][0][1], possible_bigrams[j][1][0],
                 possible_bigrams[j][1][1])
        print(f)
        print(j)
        if f[1] != 0:
            for k in bigrams:
                igrek = alphabets_2.find(k[0]) * 31 + alphabets_2.find(k[1])
                x = inverse(f[0], 961)*(igrek - f[1]) % 961
                x1 = int(x // 31)
                x2 = int(x % 31)
                if alphabets_2[x1] + alphabets_2[x2] in impossibles:
                    continue
                message += alphabets_2[x1] + alphabets_2[x2]
            if f == (690, 91):
                print(message)
                file1.write(message)
                break


main()
with open('data.txt', 'r') as txt_file:
    plain_text = txt_file.read()
    n = 2
    new_bigrams = [data[i:i + n] for i in range(0, len(plain_text), n)]
    txt_file.close()


counted_new_bigrams = sorted(lettc(new_bigrams).items(), key=operator.itemgetter(1))
```

```
counted_new_bigrams.reverse()
print(counted_new_bigrams[0:5])
```

Висновок:

Під час данного комп’ютерного практикуму, ми опанували прийомами роботи в модулярній арифметиці та набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки.