МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

# КРИПТОГРАФІЯ

## КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Виконали:

Студенти групи ФБ-03

Митрофанова М.М. та Мец Є.В.

Київ – 2022

**Тема:** «Криптоаналіз афінної біграмної підстановки»

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

# ХІД РОБОТИ

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.

## *solve.py*

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

12 варіант

***bigrams.py***

```
['хк', 'ек', 'вю', 'пн', 'вх']
```

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.

***main.py***

Для перевірки змістовності тексту ми перевіряли наявність неможливих біграм у розшифрованому тексті.

```
wrong = ['аы', 'оы', 'иы', 'ыы', 'уы', 'еы', 'аь', 'оь', 'иь', 'ыь', 'уь', 'еь', 'юы', 'яы', 'эы', 'юь', 'яь', 'эь',
         'ць', 'хь', 'кь']
```

У випадку, коли неможливі буквосполучення були відсутні, виводимо ключ та розшифрований текст.

Знайдений ключ:

```
(555, 331)
```

Розшифрований текст:

когдапожарныеисоседиушлилеоауфманосталсясдедушкойсполдингомдугласомитомом
всеонизадумчивосмотрелинадогорающиеостаткигаражалеоткнулногойвмокруюзолуим
едленновысказалточтолежалонадушепервоечтоузнаешьвжизниэточтотыдуракпоследне
ечтоузнаешьэточтотывсетотжедуракмногоепередумалязаодинтолькочасисказалсебедав
едьтыслепойлеоауфманхотитеувидатьнастоящуюмашинусчастьяееизобрелитысячилетт
омуназадионавсеещеработаетневсегдаодинаковохорошонетновсетакиработаетионавсев
ремяздесьапожарначалбылодугласдаконечнопожаргаражнолинаправадолгораздумыват
ьнадэтимнезачемточтосгореловгараженеимеетникакогоотношениякссчастьюонподнялся
поступенямкрыльцаипоманилихзасобойвотшепнуллеоауфманпосмотритевокнотишесей
часвывсеувидитедедушкасполдингдугласитомнерешительнозаглянуливбольшоеокновы
ходившеенаулицуитамвтепломсветелампыониувиделиточтохотелимпоказатьлеоауфма
нвстоловойзамаленькимстоликомсаулимаршаллигралившахматыребекканакрываласто
лкужинуноэмивырезалаизбумагиплатьядлясвоихкуколрутрисовалаакварельюджозефпу
скалпорельсамзаводнойпаровоздверьвкухнюбылаоткрытатамвоблакепаралинаауфманв
ынималаиздуховкидымящуюсякастрюлюсжаркимвсерукивселицажилиидвигалисьиззас
теколчутьслышнодоносилисьголосактотозвонкораспевалпеснюпахлосвежимхлебомияс
нобылочтоэтосамыйнастоящийхлебкоторыйсейчаснамажутнастоящиммаслomтутбылов
сечтонадоивсеэтоживоенеподдельноедедушкадугласитомобернулисьипогляделиналеоа
уфманаатотнеотрывносмотрелвокноирозовыйотсветлампылежалнаеголиценуконечноб
ормоталонэтооносамоеиестьспервастихойгрустьюпотомсживымудовольствиеминаконе
цсоспокойнымодобрениемонследилкакдвижутсяцепляютсядругзадругаостанавливаютс
яивновьуверенноировновертятсявсевинтикиколесикиегодомашнегоочагамашинасчаст
ьясказалонмашинасчастьячерезминутуегоуженебылоподокномдедушкадугласитомвиде
ликаконзахлопоталвдометопоправитчтонибудьтопередвинеттоскладкуразгладиттопыл
инкусдуеттакойжеделовитыйвинтикбольшойудивительнойбесконечнотонкойвечнотаин
ственнойвечнодвижущейсямашиныапотомнепереставаяулыбатьсяониспустилисьскрыл
ьцавпрохладнуюлетнююночьдваразавгодводворвыносилибольшиехлопающиековрыир
асстилалиихналужайкегдеонибылисовсемнекместуиказалисьkакимитонеобитаемымипо
томиздомавыходилимамаибабушкаврукахонинесликакбудтоспинкикрасивыхплетеных
креселчтостоятвпаркеупавильонасгазированнойводойкаждомувручалитакойжезлсширо
койплетенойверхушкойивседугластомбабушкапрабабушкаимамастановилисьвкружокн
адпыльнымиузорамистаройарменииточносборищеведьмидомовыхзатемпознакупрабаб
ушкиедваонамигнетилиподожметгубывсевскидывалицепыипринималисьбезпередышки
молотитьковрывоттебевотприговаривалапрабабушкабейтеблохмальчикинежалейтеивш
ейнучтотытакоеговоришьукоризненнозамечалаейбабушкавсесмеялисьвокругбушевала
пыльнаябуряисмехпереходилвкашельвихрикорпииструипесказолотистыехлопьятрубоч
ноготабакавзвивалисьввоздухитрепеталиподбрасываемыевсеновымииновымиударамио
станавливаясьчтобыпередохнутьмальчикивиделиследысвоихбашмаковибашмаковвзрос
лыхтысячуразотпечатавшиесянаузорахковравосточныйрисуноктоисчезалтопоявлялсяв
новьвместесмернымприбоемударовчтоомывалегоберегаводтуттвоймужпролилкофеиба
бушкаударилапоковруаздесьтыпролиласметануипрабабушкавыбилаизковраогромныйс
толбпылисмотритетутвесьворсвытоптанахребятаребятаавотчернилапрабабушкаглупост
иуменячернилалиловыеаэтообыкновенныесиниехлоппосмотритекакуюдорожкупротопт
алиэтоизприхожейвкухнюохужэтаедаонадажельвовведетнаводопойдавайтекаповернем
егодругимбокомаможетпростозаперетьвседвериникогоневпускатьилипустьразуваютс
яещевприхожейхлопхлопнаконецковрыразвешанынаверевкахтомразглядываетузорхитр
оумныепетлиипереплетыцветыкакиетозагадочныефигурыразводыизмеящиесялиниито
мтычтостоишьвыбивайзанятновсетакивидетьвсякиевещиговориттомдугласподозритель
носмотритнанегочтотытамувиделдавесьгородлюдейдомавотинашдомхлопнашаулицахл
опавонточерноеоврагхлопвотшколахлопавотэтачуднаязакорючкатыдугхлопвотпрабабу

шкабабушкамамахлопсколькожелетпролежалунасэтотковерпятнадцатьицелыхпятнадца
тьлетпонемутопалидажевидныотпечаткибашмаковахнултомсилентыболтатьпареньсказ
алапрабабушкатутвидновсечтослучилосьунасвдомезапятнадцатьлетхлопконечноэтовсе
прошлоеноямогуибудущееувидатьвотсейчасзажмурюсьапотомрразпогляжунаэтиразвод
ыисразуувижугдемызавтрабудемходитьибегатьдугласпересталразмахиватьвыбивалкой
ачтоещетытамвидишьглавнымобразомниткивставилапрабабушкатуттолькоиосталасьод
наосновасразувиднокакеготкаливернозагадочносказалтомвэтусторонуниткиивтутожеяв
севижучертирогатыегрешникивадухорошаяпогодаиплохаяпрогулкипраздничныеобеды
земляничныепирыонсважнымвидомтыкалвыбивалкойтоводнотовдругоеместоковрадап
отвоемувыходитчтоядержутуткакойтопансионсказалабабушкавсякраснаяизапыхавшаяс
ятутвсевиднохотьинеоченьяснодугтынагниголовунабокизажмурьодинглазтольконесовс
емконечноночьювиднолучшекогдаковервкомнатеилампагоритивообщетогдатенибываю
тсамыеразныекривыеикосыесветлыеитемныеивиднокакниткиразбегаютсявовсестороны
пощупаешьворспогладишьаонкакшкуракакогонибудьзверяипахнеткакпустыняправдап
равдажаройпахнетипескомнавернотакпахнеткаменныйгробгдележитмумиясмотривиди
шькрасноепятноэтогоритмашинасчастьяпростокетчупскакоготосандвичасказаламамане
тмашинасчастьявозразилдугласиемусталогрустночтоитутонагоритонтакнадеялсяналеоа
уфманаужунеготовсепойдеткакнадоонвсехзаставитулыбатьсяикаждыйразкогдаземляпо
вернувшисьотсолнцанакренитсякчернымбезднамвселенноймаленькийгироскопкоторый
сидитудугласагдетовнутристанетповорачиватьксолнцуивотлеоауфманчтототампрошля
пилиосталасьтолькокучказолыдапеплахлопхлопдугласссилойударилвыбивалкойсмотри
тевотзеленыйэлектрическийавтомобильчикмиссфернмиссробертасказалтомбиипбиипх
лопвсерассмеялисьавоттвоилинииижизнидугонивсевузлахслишкоммногокислыхяблокис
оленыеогурцыпередсномкоторыегдезакричалдугласвсматриваясьвузорковравотэтачере
згодэтачерездвааэтачерезтричетыреипятьлетхлоппроволочнаявыбивалказашипелаточн
озмеяавотэтанавсюостальнуюжизньсказалтомонударилпоковрустакойсилойчтовсяпыль
пятитысячстолетийрвануласьизпотрясеннойтканинамгновеньезамерлаввоздухеипокаду
гласстоялзажмурясьистаралсяхотьчтонибудьразглядетьвпереплетающихсянитяхипестр
ыхразводахковралавинаармянскойпылибеззвучнообрушиласьнанегоинавекипогреблаег
онаглазахувсехродныхстараямиссисбентлиисаманемоглабысказатькарвсеэтоначалосьо
начастовиделадетейвбакалейнойлавкеточномошкиилиобезьянкимелькалионисредикоча
новкапустыисвязокбанановионаулыбаласьимиониулыбалисьвответмиссисбентливидел
акаконибегаютзимойпоснегуоставляянанемследыкаквдыхаютосеннийдымнаулицахако
гдацветутяблонистряхиваютсплечоблакадушистыхлепестковноонаникогдаихнебоялась
домунеевобразцовомпорядкекаждаямелочьнасвоемпривычномместеполывсегдачистов
ыметеныпровизияаккуратнозаготовленавпрокшляпныебулавкиводкнутывподушечкиая
щикикомодавспальнедоверхунабитывсякойвсячинойчтонакопиласьзадолгиегодымисси
сбентлибылаженщинабережливаяунеехранилисьстарыебилетытеатральныепрограммыо
брывкикружевшарфикижелезнодорожныепересадочныебилетысловомвсеприметыисви
детельствааедолгойжизниуменякучапластинокговорилаонавоткарузоэтобыловньюйорк
евдевятьсотшестнадцатоммнетогдабылошестьдесятиджонбылещеживавотджунмунэток
ажетсядевятьсотдвадцатьчетвертыйгодджонтолькочтоумертеперьзапахсухогосенаипле
скводынапоминалиемукакхорошобылоспатьнасвежемсеневпустомсараепозадиодиноко
йфермывсторонеотшумныхдорогподсеньюстариннойветряноймельницыкрыльякоторой
тихопоскрипывалинадголовойсловноотсчитываяпролетающиегодылежатьбыопятькакт
отдавсюночьнасеновалеприслушиваяськшорохузверьковинасекомыхкшелестулистьевк
тончайшимелеслышнымночнымзвукампоздновечеромдумалонемубытьможетпослышат
сяшагионприподниметсяисядетшагизатихнутонсноваляжетистанетглядетьвокошкосено
валаиувидиткакодинзадругимпогаснутогнивдомикефермераидевушкаюнаяипрекрасная
сядетутемногоокнаистанетрасчесыватькосуеетруднобудетразглядетьноеелицонапомни
темулицотойдевушкикоторуюонзналкогдатовдалекомитеперьужебезвозвратноушедше
мпрошломлицодевушкиумевшейрадоватьсядождюнеуязвимойдляогненныхсветляковзн

авшейочемговоритодуванчикеслиимпотеретьподподбородкомдевушкаотойдетотокнапо
томопятьпоявитсянаверхувсвоейзалитойлуннымсветомкомнаткеивнимаяголосусмерти
подревреактивныхсамолетовраздирающихнебенадвоедосамогогоризонтаонмонтэгбуде
тлежатьвсвоемнадежномубежищенасеновалеисмотретькакудивительныенезнакомыеем
узвездытихоуходятзакрайнебаотступаяпереднежнымсветомзариутромоннепочувствует
усталостихотявсюночьоннесомкнетглазивсюночьнагубахегобудетиграть улыбкатеплый
запахсенаивсеувиденноеиуслышанноевночнойтишипослужитдлянегосамымлучшимотд
ыхомавнизуулестницыегобудетожидатьещеоднасовсемуженевероятнаярадостьоностор
ожноспуститсяссеновалаосвещенныйрозовымсветомраннегоутраполныйдокраевощуще
ниемпрелестиземногосуществованияивдругзамретнаместеувидевэтомаленькоечудопот
омнаклонитсяикоснетсяегорукойуподножьялестницыонувидитстакансхолоднымсвежи
ммолокомнесколькояблокигрушэтовсечтоемутеперьнужнодоказательствотогочтоогром
ныймирготовпринятьегоидатьемувремяподуматьнадвсемнадчемондолженподуматьста
канмолокаяблокогрушаонвышелизводыберегринулсянанегокакогромнаяволнаприбояте
мнотаиэтанезнакомаяемуместностьимиллионыневедомыхзапаховнесомыхпрохладным
леденящиммокроетеловетромвсеэторазомнавалилосьнамонтэгаонотпрянулназадотэтой
темнотызапаховзвуковвушахшумелоголовакружиласьзвездылетелиемунавстречукаког
ненныеметеорыемузахотелосьсноваброситьсяврекуипустьволнынесутеговсеравнокудат
емнаягромадабереганапомнилаемутотслучайизегодетскихлеткогдакупаясьонбылсбитсн
огогромнойволнойсамойбольшойкакуюонкогдалибовиделонаоглушилаегоишвырнулав
зеленуютемнотунаполниларотносжелудоксоленожгучейводойслишкоммноговодыатутб
ылослишкоммногоземлиивнезапновотьместеноювставшейпереднимшорохчьятотеньдв
аглазасловносаманочьвдругглянулананегословнолесгляделнанегомеханическийпесстол
ькопробежатьтакизмучитьсячутьнеутонутьзабратьсятакдалекостолькоперенестиикогда
ужесчитаешьсебявбезопасностиисовздохомоблегченияявыходишьнаконецнаберегвдруг
передтобоймеханическийпесизгорламонтэгавырвалсякрикнетэтослишкомслишкоммно
годляодногочеловекатеньметнуласьвсторонуглазаисчезликаксухойдождьпосыпалисьос
енниелистьямонтэгбылодинвлесуоленьэтобыллоленьмонтэгощутилострыйзапахмускуса
смешанныйсзапахомкровиидыханиязверязапахкардамонамхаикрестовникавглухойночи
деревьястенойбежалинанегоисноваотступалиназадбежалииотступаливтактбиениюкров
истучащейввискахземлябылаустланаопавшимилистьямиихтутнавернобылимиллиарды
ногимонтэгапогружалисьвнихсловноонпереходилвбродсухуюшуршащуюрекупахнущу
югвоздикойитеплойпыльюсколькоразныхзапаховвоткакбудтозапахсырогокартофелятак
пахнеткогдаразрежешьбольшуюкартофелинубелуюхолоднуюпролежавшуювсюночьна
открытомвоздухевлунномсветеавотзапахпикулейвотзапахсельдереялежащегонакухонн
омстолеслабыйзапахжелтойгорчицыизприоткрытойбаночкизапахмахровыхгвоздикизсо
седнегосадамонтэгопустилрукуитравянойстебелеккоснулсяеголадоникакбудторебенокт
ихоньковзялегозарукумонтэгподнеспальцыклицуонипахлилакрицейоностановилсяглуб
оковдыхаязапахиземлиичемглубжеонвдыхалихтемосязаемеестановилсядлянегоокружа
ющиймирвовсемсвоемразнообразииумонтэгауженебылопрежнегоощущенияпустотыту
тбылочемнаполнитьсебяиотнынетакбудетвсегдаонбрелспотыкаясьпосухимлистьямивд
ругвэтомновоммиренеобычногонечтознакомоеегоногазаделачтотоотозвавшееся глухим
звономонпошарилрукойвтравеводнусторонувдругуюжелезнодорожныерельсырельсыве
дущиепрочьотгородасквозьрощиилесаржавыерельсызаброшенногожелезнодорожногоп
утипутьпокоторомуемунадоидтиэтобылотоединственнознакомоесрединовизнытотмаги
ческийталисманкоторыйещепонадобитсяемунапервыхпорахкоторогоонсможеткоснутьс
ярукойчувствоватьвсевремяподногамипокабудетидтичереззаросликуманикичерезморез
апаховиощущенийсквозьшорохишепотлесаондвинулсявпередпошпаламикудивлениюсв
оемуонвдругпочувствовалчтотвердознаетнечточегооднаконикакнесмогбыдоказатькогд
атодавнокларисса тожепроходилаздесьполчасаспустяпродрогшийосторожноступаяпош
паламостроощущаякактемнотавпитываетсявеготелозаползаетвглазавротавушахстоитгу
ллесныхзвуковиногиисколотыокустарникиобожженыкрапивойонвдругувиделвпередио

гоньогоньблеснулнасекундуисчезновапоявилсяонмигалвдалисловночейтоглазмонтэгз амернаместеказалосьстоитдохнутьнаэтотслабыйогонекионпогаснетноогонекгорелимон тэгначалподкрадыватьсякнемупрошлодобрыхпятнадцатьминутпреждечемемуудалосьп одойтипоближеоностановилсяиукрывшисьзадеревомсталглядетьнаогоньтихоколеблющ еесяпламябелоеиалоестраннымпоказалсямонтэгуэтотогоньибоонтеперьозначалдлянего совсемнеточтораньшеэтотогоньничегонесжигалонсогревалмонтэгвиделрукипротянуты екеготеплутолькорукителасидевшихвокругкострабылискрытытемнотойнадрукаминепо движныелицаоживленныеотблескамипламенионинезналчтоогоньможетбытьтакимонда женеподозревалчтоогоньможетнетолькоотниматьноидаватьдажезапахэтогоогнябылсов семдругойбогвестьсколькоонтакпростоялотдаваясьнелепойноприятнойфантазиибудтоо нлеснойзверькоторогосветкостравыманилизчащиунегобыливлажныевгустыхресницахг лазагладкаяшерстьшершавыймокрыйноскопытаунегобыливетвистыерогаиеслибыкровь егопролиласьназемлюзапахлобыосеньюондолгостоялприслушиваяськтепломупотрески ваниюкостравокругкострабылатишинаитишинабыланалицахлюдейибыловремяпосидет ьподдеревьямивблизизаброшеннойколеиипоглядетьнамирсостороныобнятьеговзглядо мсловномирвесьсосредоточилсяздесьуэтогокострасловномирэтолежащийнаугляхкусок сталикоторыйэтилюдидолжныбылиперековатьзановоинетолькоогоньказалсяинымтиши натожебылаиноймонтэгподвинулсяближекэтойособойтишинеоткоторойказалосьзависе лисудьбымираазатемонуслышалголосалюдиговорилиноонемогещеразобратьочемречь ихтекласпокойнотогромчетотишепередговорившимибылвесьмирионинеспешаразгляды валиегоонизнализемлюзналилесазналигородлежащийзарекойвконцезаброшеннойжелез нодорожнойколеионигоговорилиобовсеминебыловещиокоторойонинемоглибыговоритьм онтэгчувствовалэтопоживыминтонациямихголосовпозвучавшимвнихноткамизумления илюбопытстваапотомктотоизговорившихподнялглазаиувиделмонтэгаувиделвпервыйам ожетбытьивседьмойразичейтоголосокликнулеголадноможетенепрятатьсямонтэготступ илвтемнотудаужладнонебойтесьсновапрозвучалтотжеголосмилостипросимкнаммонтэг медленноподошелвокругкострасиделипятеростариководетыхвтемносиниеизгрубойхол щовойтканибрюкиикурткиитакиежетемносиниерубашкионнезналчтоимответитьсадите сьсказалчеловеккоторыйповсейвидимостибылунихглавнымхотитекофемонтэгмолчасмо трелкактемнаядымящаясяструйкальетсявскладнуюжестянуюкружкупотомктотопротян улемуэтукружкуоннеловкоотхлебнулчувствуянасебелюбопытныевзглядыгорячийкофео бжигалгубыноэтобылоприятнолицасидевшихвокругнегозаростигустымибородаминобо родыбылиопрятныиаккуратноподстриженыирукиуэтихлюдейтожебыличистыиопрятны когдаонподходилккоструонивсеподнялисьприветствуягостянотеперьсновауселисьмонт эгпилкофеаа

## Висновок

В ході лабораторної роботи ми здобули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.. За допомогою частотного аналізу ми знайшли 5 найчастіших біграм у зашифрованому тексті та знайшли кандидати на ключ за допомогою перебирання частих біграм мови та частих біграм шифртексту. За допомогою розпізнавача російської мови ми знайшли вірний ключ *(555, 331)* та змогли розшифрувати змістовний текст.