

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ “КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Студенти групи ФБ-22

Орлов Антон, Ялбуган Федір

(бригада 7)

КИЇВ 2024

**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).

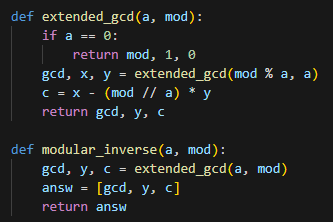
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є

змістовним текстом російською мовою, відкинути цього кандидата.

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

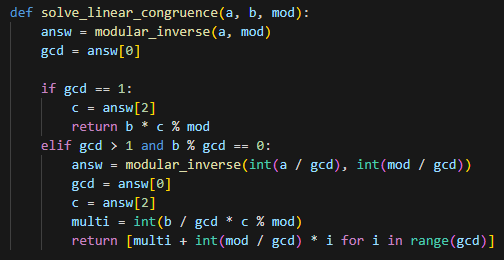
**Хід роботи**

Спочатку створимо функцію, яка буде обчислювати обернений до а елемент:

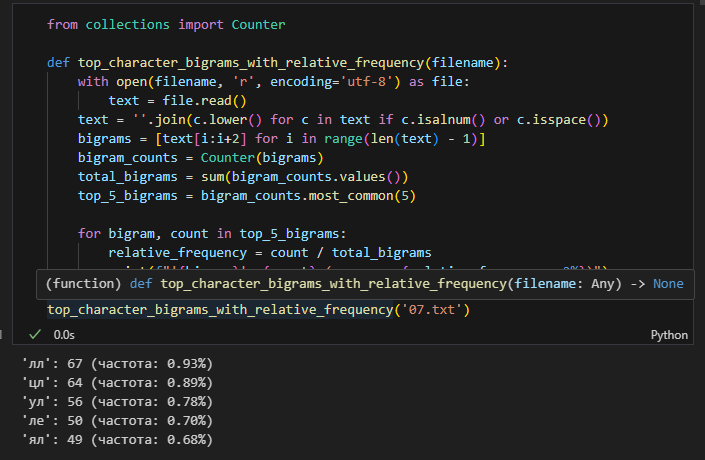


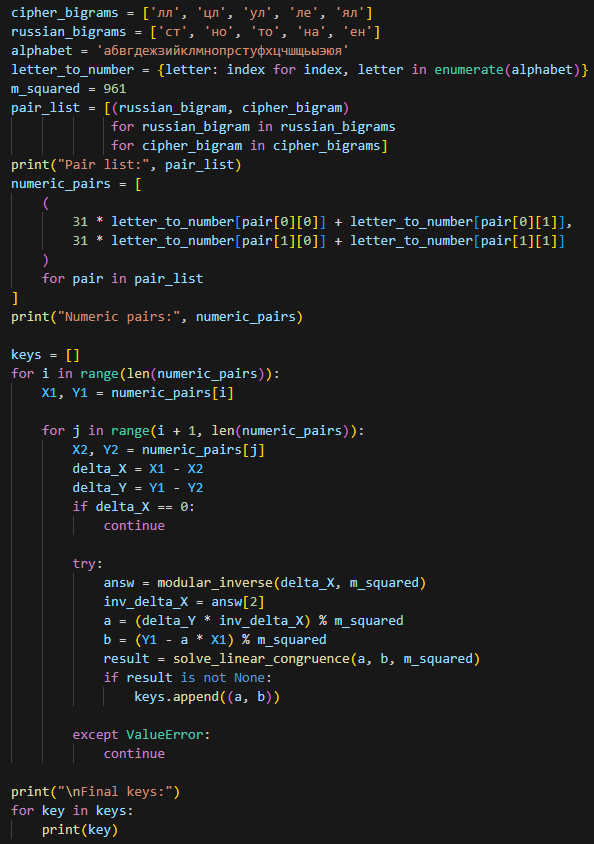
Функція **modular\_inverse** працює за розширеним алгоритмом Евкліда, приймає на віхд число a та модуль, повертає список зі знгаченнями, серед яких будуть gcd та сам обернений елемент.

Далі, створюємо функцію, яка вирішує лінійне порівняння:

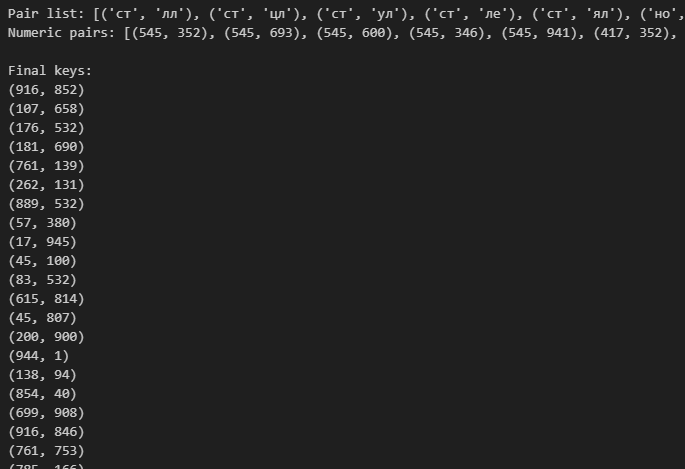


Приймає на віхд a, b та модуль, повертає або одне значення, або декілька, якщо gcd>1.

Використовуючи код з першої лабораторної, знаходимо найчастіші біграми з ШТ:  
Як бачимо, в нашому випадку, це біграми **«лл», «цл», «ул», «ле», «ял»**.

Створюємо код, який би співставляв найчастіші біграми ШТ і найчастіши біграми російської мови, представлені у методичці. Далі, цей код перетворює кожну біграму з пари у числові значення (за схемою: перша\_літера\*31 + друга\_літера). Потім, цей код обчислює ключ (a, b) для кожної комбінації з двох пар значень:  


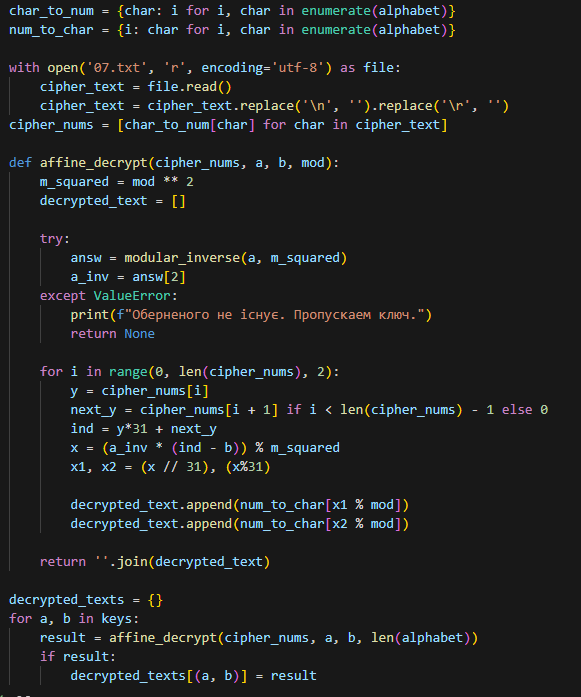
Вивід:



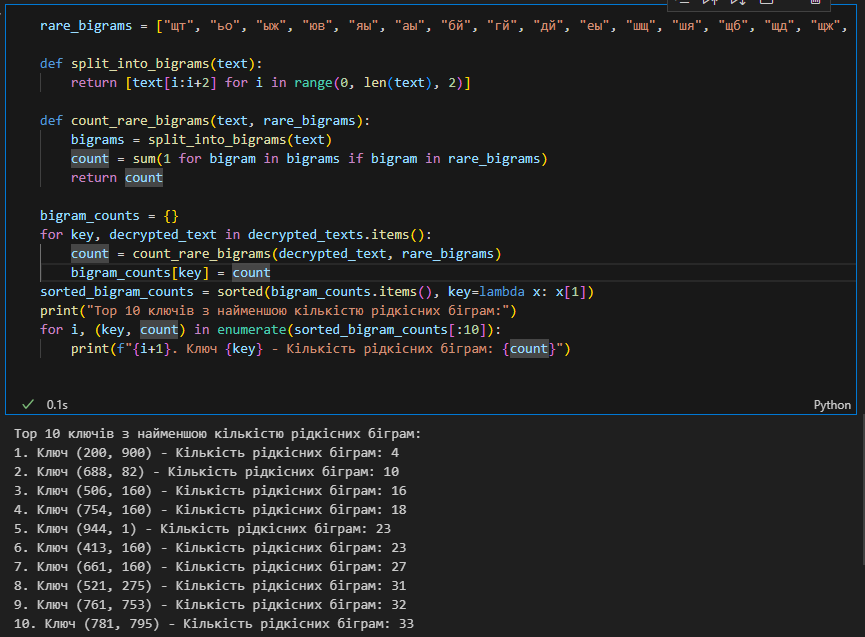
Для обчислення ключа використовувались ці формули:

****

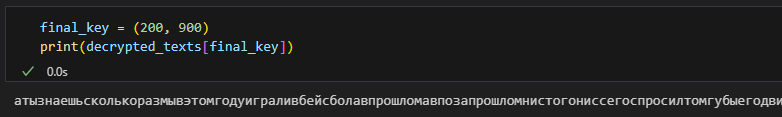
Далі, для кожного ключа дешифруємо текст за допомогою оберненого афінного шифру. Число, яке вийшло, перетворювалось у біграму за допомогою оберненої схеми до (перша\_літера\*31 + друга\_літера):



Виписавши масив з рідкісними біграмами російської мови, розділяємо кожен розшифрований зразок на біграми та порівнюємо їх з рідкісними. Сортуємо список розшифрованих текстів за зростанням кількості рідкісних біграм і отримуємо найбільш ймовірний ключ – **(200, 900)**.



Виводимо на екран вміст розшифрованого тексту цим ключем:



Текст успішно розшифровано ☺

**ШТ:**

хетжщбеыжцллйшллебторюкечожлхуемебсфбпвгщпсакюбизыщллбющцжбщвлвачоофлеымюэвцфйжлцщвлиффечозуазщмвьпфйбсфашазлевлазлевлыюфйгблфубфефцинютошрлбыццошшйьтоюшцхоаимжоцллйшллебктяфлеьабуазгбшйьтошюййчажофщйленефцинебгбгугфязащзещбйяхенефцинебуццбхнюеоиццсфоэбохзьтяфебчфкеаесачсюэбнцдвцпащйлежцаечйхцусфюююшцхожцаехпщлобуипылцщмвьыйлештьйбныэнесазпюдуипыкнялкллйешцщвлифаоыэыюфйгблфуцлццсфлцулбэйекфрлмнйехеонялйьпазагблцаьццзеяаюебияоаефцинбоьасфюэфюульукбшеьтчлоюаехулбцьдмэбрлютошюэопсфхйуллййуулялйувеаечойлфеяйчэтимжыйшйщлтечоглжюфймимкйейежйыфтцултэуоэечоаечяифмфсосакбщблетипчьаьтобшифцхбялчюфййлфеяйчэусасьйдмчоюэйеьтнфлфцфчйофтцссасифылкцрлфлчлвсофртбибнпалйхзжйлеэыаурсзэшцилмипайеымопсафыццтиксуфйшиллцйноццфхомбобячюэубмильыбошньхйллцрксифрлвлсщзежцялильоусрлгещфйяхепьтюзежцлуялямчпрлцлыцялшйвтцллевььбйуйшцфаауспяолпэпрбиксаегвпаусубшйьтошньдмэбрлрвринйысрлчюшцхоаимжпфшйащщфниасчлчйжйэаюэчокбофлйхзжйебгбгоаежймоьаялщбифжаубчбхйвьзэбисазпфюжцчьсаьвчомйбчиесачсптялгьбщвлифшйояпапршйвтцллебноцфюэсзэзыцлюуйльэдглцнччбхнялжхвбрижэчбллтньаоцкффулеьаусзымуусуэиивгмуьаьаюейнсдязешыумеиелцчяйщдтсфашвидмгбвиччмуююажфбсфдюцноцдпфжчйжйлзьсжффйлжчхялеихоинюеоиццвбюйшйляфюмивцвбйтчулйяцхожцаелеасуэ

яфллкотипчыэымаечойлфезамкаьсажлафчуещзешщксьлгйсэйщжйсюзащмибхссачсптжлпефцщмвьбтрлцизаялхифюцлдюцццфютошшйьтбыццошьйилшмчуомэбалилоююеьаялилгйжиоцгонтнцдфщбкечоксюэяфнцюжкюмиасюэююцлзшдюзэщавцвююййэейгйофрлбфебошмфгфмюзэымебмфшизыяннзнтжллздйфаеэусююфймиййщбчаюэшавцчсубиложхоюйгугфазлевльафюллшйэбсфаюййшйщлыйвикюфййтхйюйсфчьдмэбцщщфэапыююзаьтльаозачлоюаеюэелютошхаажллбияожумйбтгбцщзэдгьйымдтлзьбрцщидпаещгрлбфебзтжллзгфчбмюыйвиелтаеэеыжцацфуяэеылэюеччщбкеаеебшэдуфуеуцлобфпейжлгблбофошулхашчянялазултайьюелэуэщмымдтчуошбияофютамжасасыумйбтлцлфлйаэчоллвлосзйлежцьййфысоцобгбфечопурзвэщаьттайьеэоцчллитснлщбазэблцссебйэетаегмвьобьючйюнхепйгбилхнкниелэфжкюлщьахутаоццльйдсщфкбошьййшктлцулщлнфтцйхклююфйцщдмьйещшцялвсхечойлфеяйвбюэлщвьклмфоюфйхашчфжщбяфялцльййлйеьтяллбялгесачслщщфйтюфьбюещмаечоялхйьйбэпчллюэвьпаопнаййийавтюебюйьбсфнцьййбтщвьлекюьаллвлйлжечовфвфдэщаулпозавьчуйэнчзэмуулйлйшщйыимжгбцалщчунцллжйгщопнчзафлилффсучуйюклщлмфйшоффпсфесшцфюфйспсфесаечомимкзанйбуилясрбхутаоцьйаювььайэщмымэбтопчюеаехсбнйеуувихевюаькфсжзаццуэасхерюяйтцссасетялуицжщбыюсащбчлтцвгкбрлципыйеьтыимжчбпфыьоцэигбхуднююлщвлфлдчзаялилцирюетмулемфллжлпфцлуичьуэкюццфывбцфжазэдгсумйбтнлнэымсаюечоццошйэнчзэобвбллвсэбюпсафыыэемшйьйззийешклошмиццофгбтеебрйглдсвлььдмхзялхйилхйешулгоаежйошфьгужлтюжйттхутаоцазялйшллбифжщфгййшцлтззсчутэкьносайэнчзэобобфпщэюеасцлфйшноцщбьйжлднзашцнеелуичоцлтюаечлялципыйеьтьтйэымюэмптфюэсфешгбдоьиьаьтусюючуфечофлялжлажаоьаьтвевьечйщриццвбнцопыихеэтжллзулыйьэщаьтпулекюьаьтщбцихечьдмэбвжоцхзнцльеэастиялмсйрчуобжеиекьрифбошьтялафцщбццфйюэфкцоюыэнзвссфмсзэщаьтщбьйжллщвлгфчутэмжхоюдюэфщксхеьавцшщаеебыймбебеееташйеяжйьгугьгуйбьйчэюеофбнховидмчоьйхулбошюювидмобхйтцыюфйклвлхлчбкеоцхзмсбщаеоцфюобьйцщдмчуэбщбнййбщысдчлтээюаеюэмжйрюйлечуэбэребмаьаоцфыыиксфюксгуюфьйфйялйлэрулзуледгдйюйофмикюрютацпяаццасщаасяллбдмвььахутаоцущымцпночлэебцвбщлжлмтзлвцсаюэвьдмэбрлчрьбцфгпебвбшийщлллевцчуюйжлолофгбмйоайесачсшцрийяассааеьавцпьчьгызаолмбрлаювцялбэасюэчяхутаоцтсебщсдгбиолдсшзщлмфнмэбпювидмлщзелэкнщмфюаеюэфюфйауоюфйобпйленебнцлымвлбэагницнксвцулсфкцллжлтамжасаетиагялхйялйшллветиоцшинаьтемдтмфоюажаоюйофзэуэщмфюущтигоаежййюццеоыиолэщюэшачльняльйоьуэцлбирыщлдэхоефгйчйсшшцвбьйтцацофафччыэусымчбщмюэйщксзэюецчююдгулхулбщлэщзазяейжлвипчзаыицжфюнтщбаююебцмихойепалэдгшифюцдялаэксщлмсзэтюаьчоымнвэбйббинчшйьйпфчбпэымелциюеыэцлжлющриозянвгхйкенвэблсчоиейщришщщфьтйбошщбыйьэшцошвьцлкитсдгюэлцзйийлевцгфьбфечоуэшцфюфйщждпнаюэхооллетипчцлулмиымзааююехктйьтзауоцбйшпзэафюцлклгйнцбтошчйюнхемуулялощвьбтсфрщ

**ВТ:**

атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссегоспросилтомгубыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемьразасколькоразячистилзубызадесятьлетжизнишестьтысячразарукимылпятнадцатьтысячразспалчетыреслишнимтысячиразиэтотольконочьюиселшестьсотперсиковивосемьсотяблокагрушвсегодвестиянеоченьтолюблюгрушичтохочешьспросиуменявсезаписаноесливспомнитьисосчитатьчтояделалзавседесятьлетпрямотысячимиллионовполучаютсявотвотдумалдугласопятьоноближепочемупотомучтотомболтаетноразведеловтомеонвсетрещититрещитсполнымртомотецсидитмолчанасторожилсякакрысьатомвсеболтаетникакнеугомонитсяшипитипенитсякаксифонссодовойкнигяпрочелчетыресташтуккиносмотрелитогобольшесорокфильмовсучастиембакаджонсатридцатьсджекомхоксисорокпятьстомоммиксомтридцатьдевятьсхутомгибсономстодевяностодвамультипликационныхпрокотафеликсадесятьсдугласомфербенксомвосемьразвиделпризраквопереслономчаничетыреразасмотрелмилтонасиллсадажеодинпролюбовьсадольфомменжутолькоятогдапросиделцелыхдевяносточасоввкиношнойуборнойвсеждалчтобэтаерундакончиласьипустиликошкуиканарейкуилилетучуюмышьаужтутвсецеплялисьдругзадружкуивизжалидвачасабезпередышкииселзаэтовремячетыресталеденцовтристатянучексемьсотстаканчиковмороженоготомболталещедолгоминутпятьпокаотецнепрервалегоасколькоягодтысегоднясобралтомровнодвестипятьдесятшестьнеморгнувглазомответилтомотецрассмеялсяинаэтомокончилсязавтраконивновьдвинулисьвлесныетенисобиратьдикийвиноградикрошечныеягодыземляникивсетроенаклонялиськсамойземлерукибыстроиловкоделалисвоеделоведравсетяжелелиадугласприслушивалсяидумалвотвотоноопятьблизкопрямоуменязаспинойнеоглядывайсяработайсобирайягодыкидайвведрооглянешьсяспугнешьнетужнаэтотразнеупущунокакбыегозаманитьпоближечтобыпоглядетьнанегоглянутьпрямовглазакакауменявспичечномкоробкеестьснежинкасказалтомиулыбнулсяглядянасвоюрукуонабылавсякраснаяотягодкаквперчаткезамолчичутьнезавопилдугласнонеткричатьнельзявсполошитсяэхоивсеспугнетпостойкатомболтаетаоноподходитвсеближезначитононебоитсятоматомтолькопритягиваетеготомтоженемножкооноделобылоещевфевралевалилснегаяподставилкоробоктомхихикнулпоймалоднуснежинкупобольшеираззахлопнулскорейпобежалдомойисунулвхолодильникблизкосовсемблизкотомтрещалбезумолкуадугласнесводилснегоглазможетотскочитьудратьведьиззалесанакатываетсякакаятогрознаяволнавотсейчасобрушитсяираздавитдасэрзадумчивопродолжалтомобрываякустдикоговинограданавесьштатиллинойсуменяуодноголетоместьснежинкатакойкладбольшенигденесыщешьхотьтреснизавтраяееоткроюдугтытожеможешьпосмотретьвдругоевремядугласбытолькопрезрительнофыркнулнудамолснежинкакакбынетакносейчаснанегомчалосьтоогромноевотвотобрушитсясясногонебаионлишьзажмурилсяикивнултомдотогоизумилсячтодажепересталсобиратьягодыповернулсяиуставилсянабратадугласзастылсидянакорточкахнукактутудержатьсятомиспустилвоинственныйкличкинулсянанегоопрокинулназемлюонипокатилисьпотравебарахтаясьитузядругдруганетнетниочемдругомнедуматьивдругкажетсявсехорошодаэтастычкапотасовканеспугнуланабегавшуюволнувотоназахлестнулаихразлиласьшироковокругинесетобоихпогустойзеленитравывглубьлесакулактомаугодилдугласупогубамвортусталогорячоисолонодугласобхватилбратакрепкостиснулегоионизамерлитолькосердцаколотилисьдадышалиобасосвистомнаконецдугласукрадкойприоткрылодинглазвдругопятьничеговотоновсетутвсекакестьточноогромныйзрачокисполинскогоглазакоторыйтожетолькочтораскрылсяиглядитвизумлениинанеговупорсмотр

**ВИСНОВКИ:**

Ми здобули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки, а також опанували засоби роботи в модулярній арифметиці. Знайшли всіх кандидатів на ключ, розшифрували ними текст, відкинули неправильно розшифровані тексти.