Лабораторний практикум № 3 – Криптоаналіз афінної біграмної підстановки

Виконали: Гранік Микита ФБ-13 та Тарасов Микита ФБ-12

Варіант 7

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

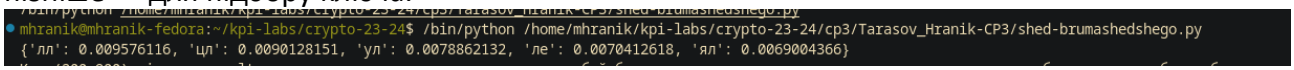
змістовним текстом російською мовою, відкинути цього кандидата.

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

Хід роботи

На початку роботи було написано форматувальник тексту, який прибирає непотрібні символи з тексту. Далі було реалізовано допоміжні функції, які потім допоможуть

дешифрувати шифротекст із нашого варіанту.
Спочатку вираховуються найчастіші біграми із нашого шифротексту, тим самим методом, що це робилось у першому комп'ютерному практикумі. Це нам знадобиться пізніше — для підбору ключа.



Маємо наступні значення. Це найчастіші біграми шифротексту.

Далі було реалізовано допоміжні функції, які будуть обраховувати індекс біграми у алфавіті, розбиваючи біграму на дві частини(дві літери). Це робилось за допомогою наступної формули з методички

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

Далі був реалізований метод Евкліда для розрахунків оберненого елементу. Це нам також знадобиться далі, коли ми будемо шукати ключі для дешифрування шифротексту.

Також був реалізований аналізатор тексту, який працює за простим принципом -- ми виписали окремі біграми, які у російському тексті не зустрічаються(якщо він написаний грамотно та без опечаток). Якщо ці біграми у дешифрованому тексті відсутні -- значить текст має бути правильно дешифрований. На практиці це було доведено.

І основна функція -- реалізує афінний дешифратор. Працює за принципом:
1) Пошук індексу біграми у алфавіті
2) Пошук оберненого елемента до елемента ключа
3) Якщо обернений елемент існує -- рахує індекс за наступною формулою:

$$X_i = a^{-1}(Y_i - b) \bmod m^2$$

І далі цей індекс перетворює у біграму(функція обернена до тої, що описувалась раніше).
4) Результат аналізується за допомогою аналізатора тексту і якщо аналізатор повернув True -- у термінал виводиться дешифрований текст та ключ-пара, якою він був дешифрований.

Далі у функції main() виконується вирішення системи рівнянь:

$$\begin{cases} Y^* \equiv aX^* + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

І отримані результаті передаються у кортеж keys у вигляді ключ-пари(кортежу). Далі, у функцію афінного дешифратора передається сам текст та ключ-пара. У результаті отримуємо змістовний текст та ключ-пару

Key (200,900) gives a result:
атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссего

спросилтомгубыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемьразаско
лькоразячистилзубызадесятьлетжизнишестьтысячразарукимылпятнадцатьтысячразспалчетыре
слишнимтысячиразиэтотольконочьюиселшестьсотперсиковивосемьсотяблокагрушвсегодвести
янеоченьтолюблюгрушичтохочешьспросиуменявсезаписаноесливспомнитьисосчитатьчтоядела
лзавседесятьлетпрямотысячимиллионовполучаютсявотвотдумалдугласопятьоноближепочему
потомучтотомболтаетноразведеловтомеонвсетрещititрещitсполнымртомотецсидитмолчана
сторожилсякакрысьатомвсеболтаетникакнеугомонитсяшипитипенитсякаксифонссодовойкнигя
прочелчетыресташтуккиносмотрелитогобольшесорокфильмовсучастиембакаджонсатридцатьс
джекомхоксисорокпятьстомоммиксомтридцатьдевятьсхутомгибсономстодевяностодвамульти
пликационныхпрокотафеликсадесятьсдугласомфербенксомвосемьразвиделпризраквопересло
номчаничетыреразасмотрелмилтонасиллсадажеодинпролюбовьсадольфомменжутолькоятогд
апросиделцелыхдевяносточасоввкиношнойуборнойвсеждалчтобэтаерундакончиласьипустили
кошкуиканарейкуилилетучуюмышьаужтутвсецеплялисьдругзадружкуивизжалидвачасабезпере
дышкииселзаэтовремячетыресталеденцовтристатянучексемьсотстаканчиковмороженоготомбо
лталещедолгоминутпятьпокаотецнепрервалегоаскольконягодтысегоднясобралтомровнодвести
пятьдесятшестьнеморгнувглазомответилтомотецрассмеялсяинаэтомокончилсязавтраконивнов
ьдвинулисьвлесныетенисобиратьдикийвиноградикрошечныеягодыземляникивсетроенаклоня
лиськсамойземлерукибыстроиловкоделалисвоеделоведравсетяжелелиадугласприслушивался
идумалвотвотоноопятьблизкопрямоуменязаспинойнеоглядывайсяработайсобирайягодыкидай
введрооглянешьсяспугнешьнетужнаэтотразнеупущунокакбыегозаманитьпоближечтобыпогляд
етьнанегоглянутьпрямовглазакакауменявспичечномкоробкеестьснежинкасказалтомиулыбнулс
яглядянасвоюрукуонабылавсякраснаяотягодкаквперчаткезамолчичутьнезавопилдугласнонетк
ричатьнельзявсполошитсяэхоивсеспугнетпостойкатомболтаетаоноподходитвсеближезначитон
онебоитсятоматомтолькопритягиваетеготомтоженемножкооноделобылоещевфевралевалилсн
егаяподставилкоробоктомхихикнулпоймалоднуснежинкупобольшеираззахлопнулскорейпобе
жалдомойисунулвхолодильникблизкосовсемблизкотомтрещалбезумолкуадугласнесводилснег
оглазможетотскочитьудратьведьиззалесанакатываетсякакаятогрознаяволнавотсейчасобрушит
сяираздавитдасэрзадумчивопродолжалтомобрываякустдикоговинограданавесьштатиллинойс
уменяуодноголетоместьснежинкатакойкладбольшенигденесыщешьхотьтреснизавтраяееоткро
юдугтытожеможешьпосмотретьвдругоевремядугласбытолькопрезрительнофыркнулнудамолс
нежинкакакбынетакносейчаснанегомчалосьтоогромноевотвотобрушитсясногонебаионлишь
зажмурилсяикивнултомдотогоизумилсячтодажепересталсобиратьягодыповернулсяиуставился
набратадугласзастылсидянакорточкахнукактутудержатьсятомиспустилвоинственныйкличкинул
сянанегоопрокинулназемлюонипокатилисьпотравебарахтаясьитузядругдруганетнетниочемдру
гомнедуматьивдругкажетсявсехорошодаэтастычкапотасовканеспугнуланабегавшуюволнувото
назахлестнулаихразлиласьшироковокругинесетобоихпогустойзеленитравывглубьлесакулактом
аугодилдугласупогубамвортусталогорячоисолонодугласобхватилбратакрепкостиснулегоиониз
амерлитолькосердцаколотилисьдадышалиобасосвистомнаконецдугласукрадкойприоткрылод
инглазвдругопятьничеговотоновсетутвсекакестьточноогромныйзрачокисполинскогоглазакотор
ыйтожетолькочтораскрылсяиглядитвизумлениинанеговупорсмотрелвесьмирионпонялвотчтон
ежданнопришлокнемуитеперьостанетсяснимиуженикогдаегонепокинетяживойподумалонпал
ьцыегодрожалирозовеянасветустремительнойкровьюточноклочкиневедомогофлагапреждене
виданногообретенноговпервыечейжеэтофлагкомутеперьприсягатьнаверностьоднойрукойонвс
еещестискивалтоманосовсемзабылонемиосторожнопотрогалсветящиесяалымпальцысловнохо
телснятьперчаткупотомподнялихповышеиогляделсовсехсторонвыпустилтомаоткинулсянаспин
увсеещевоздеврукукнебесамитеперьвесьонбылоднаголовоглазабудточасовыесквозьбойницы
неведомойкрепостиоглядывалимоствытянутуюрукуипальцыгденасветутрепеталкровавокрасн
ыйфлагтычтодугспросилтомголосегодоносилсяточносодназеленогозамшелогоколодцаоткудат
оизподводыдалекийитаинственныйподдугласомшепталисьтравыонопустилрукуиощутилихпуш
истыеножныигдетодалековтеннисныхтуфляхшевельнулпальцамивушахкакврakовинахвздыхал
ветермногоцветныймирпереливалсявзрачкахточнопестрыекартинкивхрустальномшарелесист

ыехолмыбылиусеяныцветамибудтоосколкамисолнцаиогненнымиклочкаминебапоогромномуо
прокинутомуозерунебосводамелькалиптицыточнокамушкиброшенныеловкойрукойдугласшум
нодышалсквозьзубыонсловновдыхалледивыдыхалпламятысячипчелистрекозпронизываливоз
духкакэлектрическиеразрядыдесятьтысячволосковнаголоведугласавырослинаоднумиллионну
юдюймавкаждомегоухестучалопосердцутретьеколотилосьвгорлеанастоящеегулкоухаловгруди
теложаднодышаломиллионамипоряиправдаживойдумалдугласпреждеяэтогонезналаможетиз
налданепомнюонвыкрикнулэтопросебяраздругойдесятыйнадожепрожилнасветецелыхдвенад
цатьлетиничегошенькинепонималивдругтакаянаходкадралсястомомивоттебетутподдеревомсв
еркающиезолотыечасыредкостныйхронометрсзаводомнасемьдесятлетдугдачтостобойдугласи
здалдикийвопльсгребтомавохапкуионивновьпокатилисьпоземледугтыспятилспятилоникатили
сьпосклонухолмасолнцегорелоунихвглазахивортуточноосколкилимонножелтогостеклаонизад
ыхалиськакрыбывыброшенныеизводыихохоталидослездугтынерехнулсянетнетнетнетдугласза
жмурилсявтемнотемягкоступалипятнистыелеопардытомитишетомкакпотвоемувселюдизнаютз
наютчтоониживыеяснознаютатыкакдумаллеопардынеслышнопрошлидальшевотьмуиглазауже
немоглизанимиуследитьхорошобытакпрошепталдугласхорошобывсезналионоткрылглазаотец
подбоченясьстоялвысоконаднимисмеялсяголоваегоупираласьвзеленолистыйнебосводглазаих
встретилисьдугласвстрепенулсяпапазнаетпонялонвсетакибылозадуманооннарочнопривезнасс
юдачтобыэтосомнойслучилосьонтожевзаговореонвсезнаетитеперьонзнаетчтоияужезнаюболь
шаярукаопустиласьсвысотыиподнялаегововвоздухпокачиваясьнанетвердыхногахмеждуотцомито
момисцарапанныйвстрепанныйвсеещеошарашенныйдугласосторожнопотрогалсвоилоктиониб
ыликакчужиеисудовлетворениемоблизнулразбитуюгубупотомвзглянулнаотцаинатомаяпонесу
всеведрасказалонсегодняяхочуодинвсетащитьонизагадочноусмехнулисьиотдалиемуведрадугл
асстоялчутьпокачиваясьиегоношавесьистекающийсокомлесоттягивалаемурукихочупочувствов
атьвсечтотолькоможнодумалонхочуустатьхочуоченьустатьнельзязабытьнисегоднянизавтранип
ослеоншелопьяненныйсосвоейтяжелойношейазанимплылипчелыизапахдикоговиноградаиосл
епительноелетонапальцахвспухалиблаженныемозолирукионемелиионспотыкалсятакчтоотецд
ажесхватилегозаплечоненадопробормоталдугласяничегояотличносправлюсьещедобрыхполча
саонощущалрукаминогамиспинойтравуикорникамниикоручтословноотпечаталисьнаеготелепо
цемногуотпечатокэтотстиралсятаялускользалдугласшелидумалобэтомабратимолчаливыйотец
шлипозадипредоставляяемуодномупролагатьпутьсквозьлескнеправдоподобнойцеликшоссеко
тороеприведетихобратновгородивотгородвтотжеденьиещеодноотровениедедушкастоялнаш
ирокомпарадномкрыльцеиточнокапитаноглядывалширокиенедвижныепросторыпереднимрас
кинулосьлетоонвопрошалветеринедостижимовысокоенебоилужайкугдестоялидугласитомиво
прошалитолькоегоодногодедушкаониужесозрелидедушкапоскребподбородокпятьсоттысячад
ажедветысячинавернякададахорошийурожайсобиратьлегкособеритевсеплачудесятьцентовзак
аждыймешоккоторыйвыпринесетекпрессуураа

Висновок: при виконанні даної роботи були отримані навички частотного аналізу на прикладі розкриття моноалфавітної підстановки, розглянуто метод знаходження ключа для розшифрування даного шифртексту з використанням знань з модульної арифметики.