Бочок О.С., Павелко В.С. *ФБ-03*

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

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

Варіант 15

1. Реалізували функції обчислення оберненого елементу за розширеним алгоритмом Евкліда, та функцію розв'язку лінійних порівнянь(3 випадки), функції:

- gsd()
- evclid()
- lin_porivnyanya()

2.

5 найчастіших біграм мови:

```
['ст', 'но', 'то', 'на', 'ен']
```

Дані з lab_1:

Алфавіт	Імовірність
ст	0,01411
но	0,012361
то	0,011454
на	0,011095
ен	0,011086

5 найчастіших біграм шифр-тексту:

```
['ыу', 'як', 'юк', 'ып', 'оу']
```

3. Реалізували функції комбінацій пар біграм та їх перетворення у цифровий еквівалент:

- combination_of_bi()
- ind_bi()

та функцію знаходження ключів [пар (a,b)]:

- find_ab()

4. Реалізували функцію дешифрування тексту:

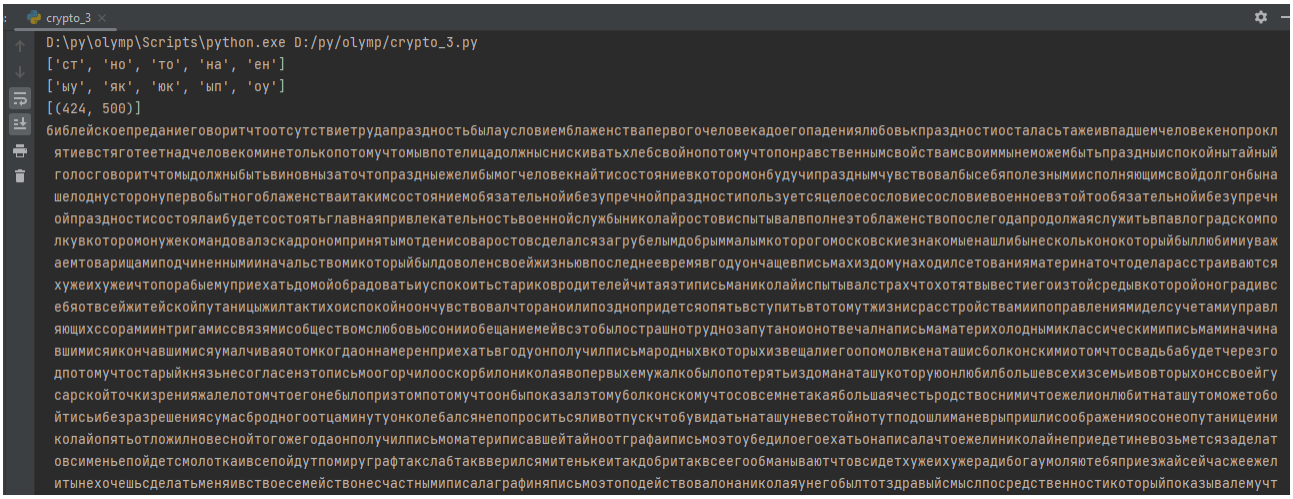
- decrypt()

Та методом пошуку у тексті неможливих біграм відкинули непідходящі тексти, та знайшли ключ.

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

- неможливі збіги літер у мові: жодне слово не починається на літеру «ы» чи «ь»

5. Підставили ключ та отримали змістовний текст:



библейскоепреданиеговоритчтоотсутствиетрудапраздностьбылаусловиемблаженствапервогочеловекадоегопадениялюбовькпраздностиосталасьтажеивпадшемчеловекенопроклятиевстяготеетнадчеловекоминетолькопотомучтомывпотелицадолжныснискиватьхлебсвойнопотомучтопонравственнымсвойствамсвоиммыненоженбытьпраздныиспокойныйголосговоритчтомыдолжныбытьвиновнызаточтопраздныежелибымогчеловекнайтисостояниевкоторомонбудучипраздныймчувствовалбысебяполезнымиисполняющимсвойдолгонбынашелоднусторонупервобытноблаженствоитакимсостояниемобязательнойибезупречнойпраздностипользуетсяцелоесословиесословиевоенноевэтойтообязательнойибезупречнойпраздностисостоялаибудетсостоятьглавнаяпривлекательностьвоеннойслужбыниколайростовиспытывалвполнеэтоблаженствопослегодапродолжаяслужитьвпавлоградскомполкувкоторомонужекомандовалэскадрономпринятымотденисоваростовсделалсязагрубелымдобрымималымкоторогомосковскиезнакомыенашлибынесколькономоторыйбыллюбимиуважаемтоварищамиподчиненнымииначальствомикоторыйбылдоволенсвоейжизньювпоследнеевремявгодуончащевписьмахиздомунаходилсетованияматеринаточтоделарасстраиваютсяхужеихужеичтопорабыемуприехатьдомойобрадоватьиуспокоитьстариковродителейчитаяэтописьманиколайиспытывалстрахчтохотятвывестиегоизтойсредывкоторойоноградивсебяотвсейжитейскойпутаницыжилтактихоиспокойноончувствовалчтораноилипозднопридетсяопятьвступитьвтотомутжизнисрасстройствамиипоправлениямиделсучетамиуправляющихссорамиинтригамиссвязямисобществомслюбовьюсониобещаниемейвсэтобылострашнотруднозапутаноионотвечалнаписьмаматерихолоднымиклассическимиписьманачинавшимисяикончавшимисяумалчиваяотомкогдаоннаменренприехатьвгодуонполучилписьмародныхвкоторыхизвещалиегоопомолвкенаташисболконскимиотомчтосвадьбабудетчерезгодпотомучтостарыйкнязьнесогласенэтописьмоогорчилооскорбилониколаявопервыхемужалкобылопотерятьиздоманаташукоторуюонлюбилбольшевсехизсемьивоторыхонссвоейгусарскойточкизренияжалелотомчтоегонебылоприэтомпотомучтоонбыпоказалэтомуболконскомучтосовсемнетакаябольшаячестьродствоснимичтоежелионлюбитнаташутоможетобойтисьибезразрешениясумасбродногоотцаминутуонколебалсянепопроситьсяливотпускчтобувидатьнаташуневестойнотутподошлиманевырыпришлисоображенияосонеопутаницеиниколайопятьотложилновеснойтогожегодаонполучилписьмоматериписавшейтайноотграфаписьмоэтоубедилоегоехатьонаписалачтоежелиниколайнеприедетиневозьметсязаделатовсименьепойдетсмолоткаивсепойдутпомируграфтакслабтаквверилсямитенькеитакдобритаквсеегообманываютчтовси

детхужеихужерадибогаумоляютебяприезжайсейчасжеежелитынехочешьсделатьменяивствоесемействонесчастн
ымиписалаграфиняписьмоэтоподействовалонаниколаяунегобылтотздравыйсмыслпосредственностикоторыйпок
азывалемучтобылодолжнотеперьдолжнобылоехатьеслиневотставкутовотпускпочемунадобылоехатьоннезнално
выспавшисьпослеобедаонвелелоседлатьсерогомарсадавнонеезженногоистрашнозлогожеребцаивернувшисьнавз
мыленномжеребцедомойобявиллаврушкелакейденисоваосталсяуростоваипришедшимвечеромтоварищамчтопод
аетвотпускиедетдомойкакнитрудноистраннобылоемудуматьчтоонуедетинеузнаетизштабачтоемуособенноинтер
еснобылопроизведенлионбудетвротмистрыилиполучитаннузапоследниеманеврыкакнистраннобылодуматьчтоон
такиуедетнепродавграфуголуховскомутройкусаврасыхкоторыхпольскийграфторговалунегоикоторыхростовнапа
рибилчтопродастзатысячикакнинепонятноказалосьчтобезнегобудеттотбалкоторыйгусарыдолжныбылидатьпанн
епшаздецкойвпикууланамдававшимбалсвоейпаннеборжозовскойонзналчтонадоехатьизэтогоясногохорошегоми
ракудатотудагдевсбыловздорипутаницачерезнеделювышелотпускгусарытоварищинетолькопополкуноипобрига
дедалиобедростовустоившийсяголовыпорубподпискиигралидвемузыкипелидвахорапесенниковростовплясалтреп
акасмайоромбасовымпьяныеофицерыкачалиобнималиируронилиростоваселдатытретьегоэскадронаещеразкачали
егоикричалиурапотомростоваположилиевсаниипроводилидопервойстанциидополовиныдорогикакэтовсегдабыва
етоткременчугадокиевавсемыслиростовабылиещеназадивэскадроненоперевалившисьзаполовинуонуженачалзаб
ыватьтройкусаврасыхсвоеговахмистрадожойвейкуибеспокойноначалспрашиватьсебяотомчтоикаконнайдетвотр
адномчемближеонподезжалтемсильнеегораздосильнеекакбудтонравственноечувствобылоподчиненотомужезако
нускоростипаденияТелвквадратахрасстоянийондумалосвоемдоменапоследнейпередотраднымстанциидалямщик
утрирублянаводкуикакмальчикзадыхаясьвбежалнакрыльцодомапослевосторговвстречиипослетогостранногочув
ствaнеудовлетворениявсравнениистемчегоожидаешьвстожекчемужеятакторопилсяниколайсталвживатьсявсвой
старыймирдомаотециматьбылитежеонитольконемногопостарелиновоевнихбилокакоетобеспокойствоиниогдане
согласиекоторогонебывалопреждеикотороекакскороузналниколайпроисходилоотдурногоположенияделсонебыл
ужедвадцатыйгодонаужеостановиласьхорошетьничегонеобещалабольшетогочтовнейбылоноиэтогобылодостато
чноонавсядышаласчастьемилюбовьюстехпоркакприехалниколайивернаянепоколебимаялюбовьэтойдевушкирад
остнодействовалананегопетяинаташабольшевсехудивилиниколаяпетябылужебольшойтринадцатилетнийкрасив
ыйвеселоиумношаловливыймальчикукоторогоужеломалсяголоснаташуниколайдолгоудивлялсяисмеялсяглядя
нанеесовсемнетаговорилончтожподурнеланапротивноважностькакаятокнягинясказалонейшопотомдададарадост
ноговориланаташанаташарассказалаемусвойроманскняземандреемегоприездвотрадноеипоказалаегопоследнееп
исьмочтожтырадспрашиваланаташаятактеперьспокойнасчастливаоченьрадотвечалниколайонотличныйчеловекч
тожтыоченьвлюбленакактебесказатьотвечаланаташаябылавлюбленавборисавучителявденисованоэтосовсемнето
мнепокойнотвердоязнаючтолучшеегонебываетлюдейимнетакспокойнохорошотеперьсовсемнетаккакпрежденик
олайвыразилнаташесвоенеудовольствиеотомчтосвадьбабылаотложенанагоднонаташасожесточениемнапустилас
ьнабратадоказываяемучтоэтонемоглобытьиначечтодурнобыбыловступитьвсемьюпротивволиотцачтоонасамаэто
гохотелатысовсемсовсемнепонимаешьговорилаонаниколайзамолчалисогласилсяснеюбратчастоудивлялсяглядян
анеесовсемнебылопохожечтобыонабылавлюбленнаяневеставразлукессвоимженихомонабыларовнаспокойнавесе
ласовершеннопопрежнемуниколаяэтоудивлялоидажезаставлялонедоверчивосмотретьнасватовствоболконскогоо
нневерилвточтоеесудьбаужерешенатемболеечтоонневидалснеюкнязяандреяемувсказалосьчточтонибудьнетовэт
омпредполагаемомбракезачемотсрочказачемнеобручилисьдумалонразговорившисьразсматерьюосестреонкудив
лениюсвоемуиотчастикудовольствиюнашелчтоматьточнотакжевглубинедушииногданедоверчивосмотреланаэто
тбраквотпишетговорилаонапоказываясынуписьмокнязяандреястемзатаеннымчувствомнедоброжелательствакот
ороевсегдаестьуматерипротивбудущегосупружескогосчастиядочерипишетчтонеприедетраньшедекабрякакоеже
этоделоможетзадержатьеговерноболезньздоровьеслабоеоченьтынеговоринаташетынесмотричтоонавеселаэтоуж
последнеедевичьевремядоживаетаязнаючтоснейделаетсявсякийразкакписьмаегополучаемавпрочембогдаствсих
орошобудетзаключалаонавсякийразонотличныйчеловекпервоевремясвоегоприезданиколайбылсерьезенидажеск
ученегомучилапредстоящаянеобходимостьвмешатьсявэтиглупыеделахозяйствадлякоторыхматьвызвалаегочтоб
ыскореесвалитьсплечэтуобузунатретийденьсвоегоприездаонсердитонеотвечаянавопроскудаонидетпошелснахму
реннымибровямивофлигелькмитенькеипотребовалунегосчетывсегочтотакоебылиэтисчетывсегониколайзналеще
менеечемпришедшийвстрахинедоумениемитенькаразговориучетмитенькипродолжалсянедолгостароставыборн
ыйиземскийдожидавшиесявпереднейфлигелясострахомиудовольствиемслышалисначалакакзагуделизатрещалка
кбудтовсвозвышавшийсяголосмолодогографаслышалиругательныеистрашныесловасыпавшиесяоднозадругимра
збойникнеблагодарнаятварьизрублюсобакунеспапенькойобворовалитдпотомэтилюдиснеменьшимудовольствие
мистрахомвиделикакмолодойграфвеськрасныйсналитойкровьювглазахзашиворотвытащилмитенькуногойиколе
нкойсбольшойловкостьювудобноевремямеждусвоихсловтолкнулегоподзадизакричалвончтобыдухутвоегомерза
вецздесьнебыломитенькастремглавслетелсшестиступенейиубежалвклумбуклумбаэтабылаизвестнаяместностьсп
асенияпреступниковвотрадномсаммитенькаприезжаяпьяныйизгородапрятalсявэтуклумбуимногиежителиотрад
ногопрятавшиесяотмитенькизналиспасительнуюсилуэтойклумбыженамитенькиисвояченицысиспуганнымилица
мивысунулисьвсенииздверейкомнатыгдекипелчистыйсамоваривозвышаласьприказчицкаявысокаяпостельподст
еганнымодеяломсшитымизкороткихкусочковмолодойграфзадыхаясьнеобращаянанихвниманиярешительнымиш
агамипрошелмимонихипошелвдомграфиняузнавшаятотчасчерездевушекотомчтопроизошловофлигелесоднойст
ороныуспокоиласьвтомотношениичтотеперьсостояниеихдолжнопоправитьсясдругойстороныонабеспокоилась о
томкакперенесетэтоеесынонаподходиланесколькоразнацыпочкахкегодверислушаякаконкурилтрубкузатрубкойа
а

Висновок

Під час виконання комп’ютерного практикуму №3 здобули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки. Окрім цього, опанували основні прийоми роботи в модулярній арифметиці.

(код програми та результати експериментів прикріплюються 😈)