КРИПТОГРАФІЯ 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.

Виконали Шанідзе Давид та Тивонюк Володимир

Варіант 19

Хід 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) , (b a 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.

Знаходимо найчастіші біграми зашифрованого тексту:

```
Most common bigrams: [('уф', 113), ('иж', 103), ('ьи', 93), ('хф', 86), ('щф', 84), ('кщ', 80), ('ек', 79), ('дз', 71), ('6а', 70), ('ен', 70)]
```

Тепер потрібно взяти 5 з них і зробити всі можливі комбінації з 5-ма найпопулярнішими в рос мові

```
popular_big = ["ст", "но", "то", "на", "ен"]
```

далі перебираємо всі можливі 2 пари пар переходів з нашого шифр тексту в рос мову в зашифрований текст => знаходимо пари a, б можливих ключів для розшифрування

```
[(130, 97), (825, 622), (775, 392), (488, 70), (290, 225), (124, 440), (310, 719), (160, 384), (52
Amount of keys: 431
```

Далі розшифровуємо даний текст цими ключами і перевіряємо на неможливі біграми

```
def check_keys_for_possibility(keys, get_crypt):
    impossible_bigrams = ['жь', 'кь', 'аы', 'оы', 'ьь', 'ыы', 'оь', 'эы',
                          'юь', 'яь', 'эь', 'ць', 'ыь', 'ыь', 'уь', 'еь', 'юы', 'яы']
```

На неправильні ключі видає помилку

```
Keys: 439, 322
Wrong key, impossible bigram!
```

з 431 варіантів ключів пройшли перевірку лише два

```
The real key potential is in: [(725, 100), (243, 183)]
```

цей ключ не підійде таки - навіть найпопулярніші біграми не ті

```
Keys: 243, 183
пдчжыюезпсыштршцрпзэбюэдзйотлгзрувлгйрщтьочббр
('но', 'сч', 'ыд', 'що', 'то')
```
\

Правильний ключ:

```
Keys: 725, 100
князьандрейприехалвглавнуюквартируармиивконцеиюнявойскаг
('то', 'ст', 'ен', 'но', 'го')
```

Ключ: (a, b) = (725, 100)

Розшифрований текст:

```
князьандрейприехалвглавнуюквартируармиивконцеиюнявойскапервойармиитойприкотор
ойнаходилсягосударьбылирасположенывукрепленномлагереудриссывойскавторойармиио
тступалистремясьсоединитьсяспервойармиейоткоторойкаговорилионибылиотрезаныбо
льшимисиламифранцузоввсебылинедовольныобщимходомвоенныхделврусскойармиинообоп
асностинашествияврусскиегубернииниктоинедумалниктоинепредполагалчтобывойнамог
лабытьперенесенадалеезападныхпольскихгубернийкнязьандрейнашелбарклаядетолликк
оторомуонбылназначеннаберегудриссытаккаknебылониодногобольшогоселаилиместечка
вокрестностяхлагерятовсеогромноеколичествогенераловипридворныхбывшихприармиир
асполагалосьвокружностидесятиверстполучшимдомамдеревеньпосюипотусторонурекиба
рклайдетоллистоялвчетырехверстахотгосударяонсухоихолоднопринялболконскогоиска
залсвоимнемецкимвыговоромчтоондоложитонемгосударюдляопределенияемуназначенияа
покаместпроситегосостоятьприегоштабеанатолякурагинакоторогокнязьандрейнадеялс
янайтивармиинебылоздесьонбылвпетербургеиэтоизвестиебылоприятноболконскомуинте
ресцентрапроизводящейсяогромнойвойнызанялкнязяандреяионрадбылнанекотороевремя
освободитьсяотраздражениякотороепроизводилавнеммыслькурагиневпродолжениеперв
ыхчетырехднейвовремякоторыхоннебылникудатребуемкнязьандрейобездилвесьукреплен
ныйлагерьиспомощьюсвоихзнанийиразговоровссведущимилюдьмистаралсясоставитьсебе
онемопределенноеепонятиеновопросотомвыгоденилиневыгоденэтотлагерьосталсянереше
ннымдлякнязяандреяонужеуспелвывестиизсвоеговоенногоопытатоубеждениечтоввоенно
мделеничегонезначатсамыеглубокомысленнообдуманныепланыкаконвиделэтоваустерлиц
компоходечтовсезависитоттогокакотвечаютнанеожиданныеинемогущиебытьпредвиденны
```

мидействиянеприятелячтовсезависитоттогокакикемведетсявседелодлятогочтобыуясни
тьсебеэтотпоследнийвопроскнязьандрейпользуясьсвоимположениемизнакомствамистар
алсявникнутьвхарактеруправленияармиейлициипартийучаствовавшихвономивывелдлясеб
яследующееепонятиеоположенииделкогдаещегосударьбылввильнеармиябыларазделенанат
роеяармиянаходилаьподначальствомбарклаядетоллияподначальствомбагратионаяподн
ачальствомтормасоваегосударьнаходилсяприпервойармиииноневкачествеглавнокомандую
щеговприказенебылосказаночтогосударьбудеткомандоватьсказанотолькочтогосударьб
удетприармиикрометогопригосудареличнонебылоштабаглавнокомандующегоабылштабимп
ераторскойглавнойквартирыпринембылначальникимператорскогоштабагенералквартирм
ейстеркнязьволконскийгенералыфлигельадютантыдипломатическиечиновникиибольшоек
оличествоиностранцевнонебылоштабаармиикрометогобездолжностипригосударенаходил
исьаракчеевбывшийвоенныйминистрграфбенигсенпочинустаршийизгенераловвеликийкня
зьцесаревичконстантинпавловичграфрумянцевканцлерштейнбывшийпрусскийминистрарм
фельдшведскийгенералпфульглавныйсоставительпланакампаниигенераладютантпаулучи
сардинскийвыходецвольцогенимногиедругиехотяэтилицаинаходилисьбезвоенныхдолжно
стейприармиинопосвоемуположениюимеливлияниеичастокорпусныйначальникидажеглавн
окомандующийнезналвкачествечегоспрашиваетилисоветуеттоилидругоебенигсениливел
икийкнязьилиаракчеевиликнязьволконскийинезналотеголилицаилиотгосударяистекает
такоетоприказаниевформесоветаинужноилиненужноисполнятьегоноэтобылавнешняяобст
ановкасущественныйжесмыслприсутствиягосударяивсехэтихлицспридворнойточкиавпри
сутствиигосударявседелаютсяпридворнымивсембылясенонбылследующийгосударьнеприн
ималнасебязванияглавнокомандующегонораспоряжалсявсемиармиямилюдиокружавшиеего
былиегопомощникиаракчеевбылверныйисполнительблюститель порядкаителохранительго
сударябенигсенбылпомещиквиленскойгубернииктоторыйкакбудтоделалкраяавсущностибы
лхорошийгенералполезныйдлясоветаидлятогочтобыиметьеговсегданаготовенасменубар
клаявеликийкнязьбылтутпотомучтоэтобылоемуугоднобывшийминистрштейнбылтутпотому
чтоонбылполезендлясоветаипотомучтоимператоралександрвысокоценилеголичныекачес
тваармфельдбылзлойненавистникнаполеонаигенералуверенныйвсебечтоимеловсегдавли
яниенаалександрапаулучибылтутпотомучтоонбылсмелирешителенвречахгенераладютант
ыбылитутпотомучтоонивездебылигдегосударьинаконецглавноепфульбылтутпотомучтоон
составивпланвойныпротивнаполеонаизаставивалександраповеритьвцелесообразностьэ
тогопланаруководилвсемделомвойныприпфулебылвольцогенпередававшиймыслипфулявбо
леедоступнойформечемсампфульрезкийсамоуверенныйдопрезренияковсемукабинетныйте
оретиккромеэтихпоименованныхлицрусскихииностранныхвособенностииностранцевкото
рыессмелостьюсвойственнойлюдямвдеятельностисредичужойсредыкаждыйденьпредлагал
иновыеневожиданныемыслибылоещемногоголицвторостепенныхнаходившихсяприармиипотому
чтотутбылиихпринципалывчислевсехмыслейиголосоввэтомогромномбеспокойномблестящ
емигордоммирекнязьандрейвиделследующиеболеерезкиеподразделениянаправленийипар
тийперваяпартиябылапфульиегопоследователитеоретикивойныверящиевточтоестьнаука
войныичтовэтойнаукеестьсвоинеизменныезаконызаконыоблическогодвиженияобходаитп
пфульипоследователиеготребовалиотступлениявглубьстраныотступленияпоточнымзако
нампредписаннымимнимойтеориейвойныивовсякомотступленииотэтойтеориивиделитолько
варварствонеобразованностьилизлонамеренностькэтойпартиипринадлежалинемецкиепр
инцывольцогенвинцингеродеидругиепреимущественнонемцывтораяпартиябылапротивупо
ложнаяпервойкакивсегдабываетприоднойкрайностибылипредставителидругойкрайности
людиэтойпартиибылитекоторыеещесвильнытребовалинаступлениявпольшуисвободыотвся
кихвпередсоставленныхплановкрометогочтопредставителиэтойпартиибылипредставите
лисмелыхдействийонивместестемибылипредставителяминациональностивследствиечего
становилисьещеодностороннеевспореэтибылирусскиебагратионначинавшийвозвышаться
ермоловидругиевэтовремябылараспространенаизвестнаяшуткаермоловабудтобыпросивш
егогосударяободноймилостипроизводстваеговнемцылюдиэтойпартииговориливспоминая
суворовачтонадонедуматьненакалыватьиголкамикартуадратьсябитьнеприятеляневпуск
атьеговроссиюинедаватьунывать войскуктретьейпартиикоторойболеевсегоимелдовери
ягосударьпринадлежалипридворныеделателисделокмеждуобоиминаправлениямилюдиэтой
партиибольшейчастьюневоенныеикоторойпринадлежаларакчеевдумалииговорилиличтогов
орятобыкновеннолюдинеимеющиеубеждений ножелающиеказатьсязатаковыхониговорилиличт
обезсомнениявойнаособенностакимгениемкакбонапартеегоопятьназывалибонапартетре
буетглубокомысленнейшихсоображенийглубокогознаниянаукиивэтомделепфульгениален
новместестемнельзянепризнатьтогочтотеоретикичастоодностороннниипотомуненадовпо
лнедоверятьимнадоприслушиватьсяиктомучтоговорятпротивникипфуляиктомучтоговоря
тлюдипрактическиеопытныеввоенномделеиизовсеговзятьсреднеелюдиэтойпартиинастоя
линатомчтобыудержавдрисскийлагерьпопланупфуляизменитьдвиженияругихармийхотяэ
тимобразомдействийнедостигалась нитанидругаяцельнолюдямэтойпартииказалосьтаклу
чшечетвертоенаправлениебылонаправлениекоторогосамымвиднымпредставителембылвел

икийкнязьнаследникцесаревичнемогшийзабытьсвоегоаустерлицкогоразочарованиягдео
нкакнасмотрвыехалпередгвардиеювкаскеиколетерассчитываямолодецкираздавитьфранц
узовипопавнеожиданновпервуюлинииюнасилуушелвобщемсмятениилюдиэтойпартииимеливс
воихсужденияхикачествоинедостаткискренностионибоялись наполеонавиделивнемсилу
всебеслабостьипрямовысказывалиэтоониговорилиничегокромегорясрамаипогибелиизвс
егоэтогоневыйдетвотмыоставиливильнуоставиливитебскоставимидриссуодночтонамост
аетсяумногосделатьэтозаключитьмирикакможноскореепоканевыгналинасизпетербургав
оззрениеэтосильнораспространенноевысшихсферахармииинаходилосебеподдержкуивпет
ербургеивканцлерерумянцевеподругимгосударственнымпричинамстоявшемтожезамирпят
ыебылиприверженцыбарклаядетоллинестолькокакчеловекасколькокаквоенногоминистра
иглавнокомандующегоониговорилиликакойонниесть всегдатакначиналиноончестныйдельны
йчеловекилучшеегонетдайтеемунастоящуювластьпотомучтовойнанеможетидтиуспешнобе
зединственачальствованияионпокажетточтоонможетсделатькаконпоказалсебявфинлянд
иижелиармиянашаустроенаисильнаиотступиладодриссынепонесшиникакихпораженийтом
ыобязаныэтимтолькобарклаюжелитеперьзаменятбарклаябенигсеномтовсепогибнетпото
мучтобенигсенужепоказалсвоюнеспособностьвгодуговорилилюдиэтойпартиишестыебени
гсенистыговорилинапротивчтовсетакинебылоникогодельнееиопытнеебенигсенаикакнив
ертисьвсетакипридешькнемуилюдиэтойпартиидоказываличтовсенашеотступлениедодрис
сыбылопостыднейшеепоражениеибеспрерывныйрядошибокчембольшенаделаютошибокговор
илионитемлучшепокрайнеймереескореепоймутчтотакнеможетидтиануженнекакойнибудьба
рклайачеловеккакбенигсенкоторыйпоказалужесебявмгодукоторомуотдалсправедливост
ьсамнаполеонитакойчеловекзакоторымбыохотнопризнаваливластьитаковойестьтолькоо
динбенигсенседьмыебылилицакоторыевсегдаестьвособенностипримолодыхгосударяхико
торыхособенномногобылоприимператореалександрелицагенераловифлигельадютантовст
растнопреданныегосударюнекакимператорунокакчеловекаобожающиеегоискренноибеско
рыстнокакегообожалростоввмгодуивидящиевнемнетольковседобродетелиноивсекачеств
ачеловеческиеэтилицахотяивосхищалисьскромностьюгосударяотказывавшегосяоткоман
дованиявойскаминоосуждалиэтуизлишнююскромностьижелалитолькоодногоинастаивалин
атомчтобыобожаемыйгосударьоставивизлишнеенедовериексебеобявилоткрыточтоонстан
овитсявоглавевойскасоставилбыприсебештабквартируглавнокомандующегоисоветуясьг
денужносопытнымитеоретикамиипрактикамисамбывелсвоивойскакоторыходноэтодовелоб
ыдовысшегососостоянияввоодушевленияввосьмаясамаябольшаягруппалюдейкотораяпосвоему
огромномуколичествуотносилась кдругимкаккмусостоялаизлюдейнежелавшихнимираниво
йныинаступательныхдвиженийниоборонительноголагерянипридриссенигдебытонибылон
ибарклаянигосударянипфулянибенигсенаножелающихтолькоодногоисамогосущественног
онаибольшихдлясебявыгодиудовольствийвтоймутнойводеперекрещивающихсяиперепутыв
ающихсяинтригкоторыекишелиприглавнойквартиреговударяввесьмамногомможнобылоусп
етьвтакомчтонемыслимобыбыловдругоевремяодиннежелаятолькопотерятьсвоеговыгодно
гоположенияныничесоглашалсяспфулемзавтраспротивникомегопослезавтраутверждалчто
неимеетникакогомненияобизвестномпредмететолькодлятогочтобыизбежатьответственн
остииугодитьгосударюдругойжелающийприобрестивыгодыобращалнасебявниманиегосуда
рягромкокричатосамоеначтонамекнулгосударьнаканунеспориликричалвсоветеударяясе
бявгрудьивызываянесоглашающихсянадуэльитемпоказываячтоонготовбытьжертвоюобщей
пользытретийпростовыпрашивалсебемеждудвухсоветовивотсутствиевраговединовремен
ноепособиезасвоювернуюслужбузнаячтотеперьнекогдабудетотказатьемучетвертыйнеча
янновсепопадалсянаглазагосударюотягченныйработойпятыйдлятогочтобыдостигнутьда
вноженнойцелиобедаугосударяожесточеннодоказывалправотуилинеправотувновьвыст
упившегомненияидляэтогоприводилболееилименеесильныеисправедливыедоказательств
авселюдиэтойпартииловилирубликрестычиныивэтомловленииследилитолькозанаправлен
иемфлюгерацарскоймилостиитолькочтозамечаличтофлюгеробратилсяводнусторонукаквс
еэтотрутневоенаселениеармииначиналодутьвтужесторонутакчтогосударютемтруднеебы
лоповернутьеговдругуюсрединеопределенностиположенияприугрожающейсерьезнойопас
ностипридававшейвсемуособеннотревожныйхарактерсредиэтоговихряинтригсамолюбийс
толкновенийразличныхвоззренийичувствприразноплеменностивсехэтихлицэтавосьмаяс
амаябольшаяпартиялюдейнанятыхличнымиинтересамипридавалабольшуюзапутанностьисм
утностьобщемуделукакойбыниподнималсявопросаужройэтихтрутнейнеоттрубивещенадпр
ежнейтемойперелеталнановуюисвоимжужжаниемзаглушализатемнялискренниеспорящиего
лосаизвсехэтихпартийвтосамоевремякаккнязьандрейприехалкармииисобраласьещеоднад
евятаяпартияначинавшаяподниматьсвойголосэтобылапартиялюдейстарыхразумныхгосуд
арственноопытныхиумевшихнеразделяяниодногоизпротиворечащихмнений отвлеченнопос
мотретьнавсечтоделалосьприштабеглавнойквартирыиобдуматьсредстваквыходуизэтойн
еопределенностинерешительностизапутанностиислабостилюдиэтойпартииговорилиидум
аличтовседурноепроисходитпреимущественноотприсутствиягосударясвоеннымдворомпр
иармииичтоармиюперенесенатанеопределеннаяусловнаяиколеблющаясяшаткостьотношен

ийкотораяудобнапридвореновреднавармиичтогосударюнужноцарствоватьанеуправлятьв
ойскомчтоединственныйвыходизэтогоположенияестьотездгосударясегодворомизармиич
тоодноприсутствиегосударяпарализуетпятьдесяттысячвойсканужныхдляобеспеченияег
оличнойбезопасностичтосамыйплохойнонезависимыйглавнокомандующийбудетлучшесамо
голучшегоносвязанногоприсутствиемивластьюгосударявтосамоевремякаккнязьандрейж
илбезделапридриссешишковгосударственныйсекретарьбывшийоднимизглавныхпредстави
телейэтойпартиинаписалгосударюписьмокотороесогласилисьподписатьбалашевиаракче
еввписьмеэтомпользуясьданнымемуотгосударяпозволениемрассуждатьобобщемходедело
нпочтительноиподпредлогомнеобходимостидлягосударявоодушевитьквойненародвстоли
цепредлагалгосударюоставитьвойскоодушевлениегосударемнародаивоззваниекнемудля
защитыотечествтосамоенасколькоонопроизведенобылоличнымприсутствиемгосударявм
оскveодушевлениенародакотороебылоглавнойпричинойторжествароссиибылопредставле
ногосударюипринятоимкакпредлогдляоставленияармиа

Висновок:

В даній лабораторній отримали досвід зламу біграмної підстановки афінного шифру. Виконали прийоми модулярної арифметики та провели частотний аналіз зашифрованого тексту. Використали додаткові функції для перевірки істинності розшифрованих текстів та визначили ключ розшифрування (725, 100).