Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота No 3
Варіант - 6

Виконали: студенти групи ФБ-13

Клименко Д. О. Стягайло Д. А.

Київ 2023

Мета: 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).

```
TOP bigrams:
ще : 46
хе : 44
чв : 42
ле : 40
цв : 38
ощ : 37
сд : 36
же : 36
де : 36
гд : 34
```

Оскільки серед перших п'яти біграм не було кандидатів на ключ при яких текст змістовно розшифровувався, було прийнято рішення про вивід перших 10 біграм.

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).

```
# 711 412
```

```
441 310
```

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

```
# 711 412
# вид н_рушения встреч_ется ниболее ч_сто последствия могут быть самые рзные если похищен текст книги сп
# для коллектив авторов это ктстроф и потери могут выржться в тысячах долларов однко если книга уже издн
```

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

```
dariaklymenko@darias-Air lab3 % /opt/homebrew/bin/python3 /Users/dariaklymenko/Documents/lab3/main.py
441 310 утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоиветербыллетнийтеплоедыханиемиранеспешноеиленивоестоитлишьвст
атьвысунутьсявокошкоитотчаспоймешьвотонаначинаетсянастоящаясвободаижизньвотонопервоеутролетадуглассполдингдвенадцатилетотродутоль
кочтооткрылглазаикаквтеплуюречкупогрузилсявпредрассветнуюбезмятежностьонлежалвсводчатойкомнаткеначетвертомэтажевовсемгороденебылоб
ашнивышеиоттогочтоонпарилтаквысоковвоздухевместесиюньскимветромвнемрождалась чудодейственнаясилапоночамкогдавязыдубыикленыслививались
воднобеспокойноеморедуглассокидывалеговзглядомпронзавшимтьмуточномаякисегоднявотздоровошепнулонвпередицелоелетонесчетноемножестводнв
ейчутьнеполкалендаряонужевиделсебямногорукимкакбожествошиваизкнижкипропутешествиятолькопоспевайрватьещезеленыеяблокиперсикичерныек
акночьсливыегоневытащитьизлесуизкустовизречкиакакприятнобудетпомерзнутьзабравшисьвзаиндевелыйледниккаквеселожаритьсявбабушкинойкух
незаодностысячьюцыплятапоказаделоразвнеделюемупозволялиночеватьневдомикепососедствугдеспалиегородителиимладшийбратишкатомаздесьвде
довскойбашнеонвзбегалпотемнойвинтовойлестниценасамыйверхиложилсяспатьвэтойобителикудесникасредигромовивиденийаспозаранкукогдадажем
олочникещеназвякалбутылкаминаулицахонпросыпалсяиприступалказаветномуволшебствустоявтемнотеуоткрытогоокнаоннабралполнуюгрудьвоздухаи
изовсехсилдунулуличныефонаримигомпогаслиточносвечкиначерномименнномпирогедугласдунулещеиещеивнебеначалигаснутьзвездыдугласулыбнул
сяткнулпальцемтамитамтеперьтутивоттутвпредутреннемтуманеодинзадругимпрорезалисьпрямоугольникивдомахзажигалисьогнидалекодалеконарас
светнойземлевдругозарилась целаявереницаоконвсемзевнутьвсемвставтьогромныйдомвнизуожилдедушкавынимайзубыизстаканадугласнемногоподо
ждалбабушкаипрабабушкажарьтеоладьисквознякпронесповсемкоридорамтеплыйдухжареноготестаивовсехкомнатахвстрепенулисьмногочисленныетет
кидядьядвоюродныебратьяисестрычтосехалисьсюдапогоститьулицастариковпросыпайсямиссэленлумисполковникфрилеймиссисбентлипокашляйтевст
аньтепроглотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайтелошадьвыводитеизсараяфургонпораехатьзастарьемпотусторонуовраготкр
ылисвоидраконьиглазаугрюмыеособнякискоровнизупоявятсянаэлектрическойзеленоймашинедвестарухиипокатятпоутреннимулицамприветственнома
хаякаждойвстречнойсобакемистертридденбегитевтрамвайноедепоивскорепоузкимрусламмощеныхулицпопливеттрамвайрассыпаявокругжаркиесиниеи
скрыджонхафчарливудменвыготовышепнулдугласулицедетейготовыспросилонубейсбольныхмячейчтомоклинаросистыхлужайкахупустыхверевочныхкач
елейчтоскучаясвисалисдеревьевмампаптомпроснитесьтихонькопрозвенелибудильникигулкопробиличасызданиисудаточносетьзаброшеннаяегорук
ойсдеревьеввзметнулисьптицыизапелидирижируясвоиморкестромдугласповелительнопротянулрукуквостокуивзошлосолнцедугласскрестилрукинагр
удииулыбнулсякакнастоящийволшебникводтотодумалонтолькояприказаливсеповскакаливсезабегалиотличноебудетлетоионнапоследокогляделгород
ищелкнулемупальцамираспахнулисьдверидомовлюдивышлинаулицулетотысячадевятьсотдвадцатьвосьмогогоданачалосьвтоутропроходяполужайкедуг
ласнаткнулсянапаутинуневидимаянитькоснуласьеголбаинеслышнолопнулаиотэтогопустячногослучаяоннастоорожилсяденьбудетнетакойкаквсенетак
ойешеипотомучтобываютднисотканныеизодныхзапаховсловноевесьмирможновтянутьносомкаквоздухвдохнутьивыдохнутьтакобяснялдугласуиегодесят
илетнемубратутомуотецкогдавезихвмашинезагородавдругиедниговорилещеотецможноуслышатькаждыйгромикаждыйшорохвселеннойиныеднихорошопро
боватьнавкусаиныенаощупьабываютитакиекогдаестьвсесразувотнапримерсегодняпахнеттакбудтоводнуночьтамзахолмаминевестьоткудавзялсяогро
мныйфруктовыйсадивседосамогогоризонтатакиблагоухаетввоздухепахнетдождемнонанебениоблачкатогоиглядиктотоневедомыйзахохочетвлесунопо
катамтишинадугласвовсеглазасмотрелнаплывущиемимополянетнисадомнепахнетнидождемдаиоткудабыразниябломьнетнитучиктотамможетхохотатьвл
есуавсетакидугласвздрогнулденьэтоткакойтоособенныймашинаостановиласьвсамомсердцетихоголесаануребятанебаловатьсяониподталкивалидруг
другалоктямихорошопапамальчикивылезлиизмашинызахватилисиниежестяныеведраисойдяспустынной проселочнойдорогипогрузилисьвзапахиземливл
ажнойотнедавнегодождящитепелсказалотецонивсегдавыютсявозлевиноградакакмальчишкивозлекухнидугласдугласвстрепенулсяопятьвитаешьвоб
```

Висновок: У ході виконання комп’ютерного практикуму були отримані навички розшифрування тексту, зашифрованого шифром афінної підстановки, розкриття ключа за допомогою апарату модулярної арифметики (пошук обернених елементів за модулем та розв’язування лінійних рівнянь) та створення розпізнавача певної мови.