МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

Комп’ютерний практикум

Робота №3

Виконали:
Сернова А.Р., Колесник А.М.
студенти групи ФБ-93

Перевірила:
Селюх П.В.

Київ-2021

Тема: 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:

Виконуємо варіант 7:

хетжщбеыжцллйшллебторюкечожлхуемебсфбпвгщпсакюбизыщллбющцжбщвлвачоофлеымюэвцфйжлц
щвлиффечозуазщмвьпфйбсфашазлевлазлевлыюфйгблфубфефцинютошрлбыццошшйьтоюшцхоаимжоцл
лйшллебктяфлеьабуазгбшйьтошюййчажофщйленефцинебгбгугфязащзещбйяхенефцинебуццбхнюеоиццс
фоэбохзьтяфебчфкеаесачсюэбнцдвцпащйлежцаечйхцусфюююшцхожцаехпщлобуипылцщмвьыйлештьйб
ныэнесазпюдуипыкнялкллйешцщвлифаоыэыюфйгблфубцлццсфлцулбэйекфрлмнйехеонялйьпазагблцаьц
цзеяаюебияоаефцинбоьасфюэфюульукбшеьтчлоюаехулбцьдмэбрлютошюэопсфхйуллййуулялйувеаечой
лфеяйчэтимжыйшйщлтечоглжюфймимкйейежйыфтцултэуоэечоаечяифмфсосакбщблетипчьаьтобшифцх
бялчюфййлфеяйчэусасьйдмчоюэйеьтнфлфцфчйофтцссасифылкцрлфлчлвсофртбибнпалйхзжйлеэыаурсзэ
шцилмипайеымопсафыццтиксуфйшиллцйноццфхомбобячюэубмильыбошньхйллцрксифрлвлсщзежцялил
ьоусрлгещфйяхепьтюзежцлуялямчпрлцлыцялшйвтцллевььбйуйшцфаауспяолпэпрбиксаегвпаусубшйьто
шньдмэбрлрвринйысрлчюшцхоаимжпфшйащщфниасчлчйжйэаюэчокбофлйхзжйебгбгоаежймоьаялщбиф
жаубчбхйвьзэбисазпфюжцчьсаьвчомйбчиесачсптялгьбщвлифшйояпапршйвтцллебноцфюэсзэзыцлюуйль
эдглцнччбхнялжхвбрижэчбллтньаоцкффулеьаусзымуусуэиивгмуьаьаюейнсдязешыумеиелцчяйщдтсфаш

видмгбвиччмуюююажфбсфдюцноцдпфжчйжйлзьсжффйлжчхялеихоинюеоиццвбюйшйляфюмивцвбйтчулй
яцхожцаелеасуэяфллкотипчыэымаечойлфезамкаьсажлафчуещзешщксьлгйсэйщжйсюзащмибхссачсптжлл
пефцщмвьбтрлцизаялхифюцлдюцццфютошшйьтбыццошьйилшмчуомэбалилоююеьаялилгйжиоцгонтнцд
фщбкечоксюэяфнцюжкюмиасюэююцлзшдюзэщавцвююййэейгйофрлбфебошмфгфмюзэымебмфшизыянн
знтжллздйфаеэусююфймиййщбчаюэшавцчсубиложхоюйгугфазлевльафюллшйэбсфаюййшйщлыйвикюф
ййтхйюйсфчьдмэбцщщфэапыююзаьтльаозачлоюаеюэелютошхаажллбияожумйбтгбцщзэдгъйымдтлзьбрц
щидпаещгрлбфебзтжллзгфчбмюыйвиелтаеэеыжцацфуяэеылэюеччщбкеаеебшэдуфуеуцлобфпейжлгблбо
фошулхашчянялазултайьюелуэущмымдтчуошбияофютамжасасыумйбтлцлфлйаэчоллвлосзйлежцьййфыс
оцобгбфечопурзвэщаьттайьеэоцчллитснлщбазэблцссебйэетаегмвьобьючйюнхепйгбилхнкниелэфжкюлщь
ахутаоццльйдсщфкбошьййшктлцулщлнфтцйхклююфйцщдмьйещшцялвсхечойлфеяйвбюэлщвьклмфоюоф
йхашчфжщбяфялцльййлйеьтяллбялгесачслщщфйтюфьбюещмаечоялхйьйбэпчллюэвьпаопнайййийавтюеб
юйьбсфнцьййбтщвьлекюьаллвлйлжечовфвфдэщаулпозавьчуйэнчзэмуулйлйшщйыимжгбцалщчунцллжйг
щопнчзафлилффсучуйюклщлмфйшоффпсфесшцфюфйспсфесаечомимкзанйбуилясрбхутаоцьйаювььайэщ
мымэбтопчюеаехсбнйеуувихевюаькфсжзаццуэасхерюяйтцссасетялуицжщбыюсащбчлтцвгкбрлципыйеьт
ыимжчбпфыьоцэигбхуднююлщвлфлдчзаялилцирюетмулемфллжлпфцлуичьуэкюццфывбцфжазэдгсумйб
тнлнэымсаюечоццошйэнчзэобвбллвсэбюпсафыыэемшйьйззийешклошмиццофгбтеебрйглдсвлььдмхзялхй
илхйешулгоаежйошфьгужлтюжйттхутаоцазялйшллбифжщфгййшцлтззсчутэкьносайэнчзэобобфпщэюеас
цлфйшноцщбьйжлднзашцнеелуичоцлтюаечлялципыйеьтьтйэымюэмптфюэсфешгбдоьиьаьтусююучуфечо
флялжлажаоьаьтвевьечйщриццвбнцопыихеэтжллзулыйьэщаьтпулекюьаьтщбцихечьдмэбвжоцхзнцльеэас
тиялмсйрчуобжеиекьрифбошьтялафцщбццфйюэфкцоюыэнзвссфмсзэщаьтщбьйжллщвлгфчутэмжхоюдюэ
фщксхеьавцшщаеебыймбебеееташйеяжйьгугьгуйбьйчэюеофбнховидмчоьйхулбошююювидмобхйтцыюфй
клвлхлчбкеоцхзмсбщаеоцфюобьйцщдмчуэбщбнййбщысдчлтээюаеюэмжйрюйлечуэбэребмаьаоцфыыикс
фюксгуюфьйфйялйлэрулзуледгдйюйофмикюрютацпяаццасщаасяллбдмвььахутаоцущымцпночлэебцвбщ
лжлмтзлвцсаюэвьдмэбрлчрьбцфгпебвбшийщлллевцчуюйжлолофгбмйоайесачсшцрийяассааеьавцпьчьгыз
аолмбрлаювцялбэасюэчяхутаоцтсебщсдгбиолдсшзщлмфнмэбпювидмлщзелэкнщмфюаеюэфюфйауоюфй
обпйленебнцлымвлбэагницнксвцулсфкцллжлтамжасаетиагялхйялйшллветиоцшинаьтемдтмфоюажаоюйо
фзэуэщмфюущтигоаежййюццеоыиолэщюэшачльняльйоьуэцлбирыщлдэхоефгйчйсшшцвбьйтцацофафчч
ыэусымчбщмюэйщксзэюецчююдгулхулбщлэщзазяейжлвипчзаыицжфюнтщбаююебцмихойепалэдгшифю
цдялаэксщлмсзэтюаьчоымнвэбйббинчшйьйпфчбпэымелциюеыэцлжлющриозянвгхйкенвэблсчоиейщриш
щщфьтйбошщбыйьэшцошвьцлкитсдгюэлцзйийлевцгфьбфечоуэшцфюфйщждпнаюэхооллетипчцлулмиы
мзааююехктйьтзауоцбйшпзэафюцлклгйнцбтошчйюнхемуулялощвьбтсфрщфюгыьфымдтшйнцфюфйюця
лвлжюзщбццффечоьлдсзэщаьтщбцщзээюфймктюцжшйеитстсьйнйубафгйчйсшыйашюэазщлнэсмсафюсм
эбгбкупебноцфюейхсчлпшйлхэгящэтюаьчодгшийщшццфымдтлзьбсфиллеозйтчуаулитсефцбйшпзгыэоц
ыйаумийщюезашифюкюксебйэагиасмхзвевьдмцщвлиффечожлщлфйжлфлцлифнцзебнцлрлнэмжпаыэым
цжнощйщлжллллцлйяылдскьхеэфжщвьчллзчбюйгффвбзэлеыйпэагулсьдмэбрлкыйщвбсфашмикюблцлф
улеьагумуолеуцфсфрщпывцхзыэпчнземшйялчбюйллтеыэофйэпрауиаьрщйыййшчуащзазяноююпыйробь
юеблпфщбщюэьпрзаыйгйфоцлжлиююензпоыичйжйсфьбнцыюницнобеебнцлчйлешзисиицфысююучибцв
бйшцлкыиипаццвцхзсрсаязазсфбцнтнзиююеночпкьялшцллясновцсалятфымьйпэуоусщлмснозэмпбщелуи
чоцлйулщвлгфчуялйуцжрижэмпшцчлчбмййшобсфоегяыебнцлобйуьсчпвлщйпэейщлэсдггуллщьдмэбтыа
оцллзшбнцьюцжджцпблкцщлрэфюлзнбжааьюююьпрзааанозефцинфщлйсфлежйллжщвлофцзьбсфчлэьыр
обихюйжещфлйхстйебнийьюьццзенефцинчлщлхсфющбжлщлыйхутаоцкюоишцсфщбвьчуафжаолпэсдшд
покюобоьчощмжуойлейнзалщшцрийяиежйошиссааеьашцвюжлоажбщблептийщмщаллырзафюуикьйепап
ччьцллзшбщлафжаолщбафулмтфщебфьечююдгхулбцьдмэбцщжйоьнткеымюэфжщбэбилхйцфшэзачбьйу
лбэюлжюжсщфдэщакелщвлфйутебэьгужлщьццзеагщбфлхйбипчьащбаююечяпапрдюыэчьыбошюйцфофл
йжлщйжшгфьйулофлбсффьгубеасетщбклщсчьебнцацялилафчлщемпюеиеулсьритючоаюриобзктйалщлхз
яноцоиаьлллензлрвлцлмймивжкювьчощбфйчшшйьтлаюехугьцняллеопдгхутаоцажчбцьуснгчлаажцуимпя
ллбчлнбшсефюэююцлзшулобцфсфашулдйфааьдмхзцщзеьацщзеьаюэусхеьавцшщшцчаюэырсалбрлтээйж
лжйщлжээромэбгбвфчлэеиебнцлшцллясьабоюэцлхйфеымшцгйчаьлофгблзнбсфашобшикпрюкпвлщйпэей
ажчллзэрураезальшцюйэьдмхзьйжйгэщаьтьйчэюеьйчэюехутаоцгбдоьиьаьттехоцлгйттлсшцауцбсфютчэв
цхзпаглцбяыечойерыюечообсщаечлхоэюфйюдмфшэядржщбшевеелофйфознтйэцжщбшехежсасхулбжаг
лцбяьщэццрзоэлщвлвальзафытюаееоефтамжыухйьйилтаажуэбопуэааьйебртизыопыеасбизыйщвбцьдмэбя
ртизыопрюфйшэзаолцлдсшзрмэбгбаечяулюпбныэацжцялшаозрлллщбнэбовцмйшаьтжлщльбщмжулфебэ
башйжпаыэсавцхзхэмпшцчллмэбгбэрлцмиюеьавцпьдмэбаюлежйчйчунцтщбщмжщбюеулбтщлжюфйвбг
фазщлгбхулбцлюэщбвлаэлщщфыйшэоцфдчбвеопюхялрлбэдгэайньашцтлсепчтюгбжлчлжйюэлцфжщбюе
йейщритлижщбюевеэфнухйшэядйлйшшбщитсьлфулеьаоцжцозрлхзфщвьбтэбщмфючлэьырулобяфьбацлэ
уэюеыйяьпрцлйбэончхуаешлафялилафеяиибщуэнзмюлежйцбпэаглцзйийзыииэыыэнзщьдмэбрллетипчцл

улмиымзааюэфщлжеолофазсфобзнччтйвцкьфююйоютиыэтйилхаажчузимжбфауфмцпущаечойжтаеэщащ
баеыбзэхечоетульйсулцтюаьебхсмжзаюэфйжлнэцтклиувьвзэлцюедкйетлофгбйбфлаэжугосрчусфашолыьз
атййуыйвичьдмэбдцялшаиуошулобяфьбацкфщмюэзыкюццкфлеисядыфрцксчоюйрлщегмююзаяййугугфк
лиуулиулцоюфюхевюфйвеаесачсчопчцлхулбщлербноулехебрбннллйжшбцвбошьййшктгбазошоффйжлнэ
еэажкюмиуэфщшцюйюэщйщлгшеэыэнзрцшцчлвгйтхйщлхээывгмжуэбоаанафщлйрзажбщйрмфллжлпфц
луичьтфшцюйлфгййшцлпаюеюэбщзазяйрлцфунбсфхаечыэнзхоцжсаыитсольймйсфолкцулхзобнцзеасвее
лгйхьечццщюхеьащмцжбщюйзльйщбфлбиоптиилвбцьдмэбтофлйжлмллакнцлцщебдасццййфлципрулх
ноцьлцлеузбзитснозэымновцлфцлчеебшуустиофоббэжфллгувешцщлрэелещянхезавцлэяйжлгйюйулэйбэ
ымнлещянхекскеаелеыизаьтвбшабцллйшгбцьдмэбтыпальаозаопкечодпебцфилхнзаююагаечявафщцжчьф
щжйфллекюдтрййувьцлйубисасмхешщиежцьюцжяаццдэйщебфьлщвьопцлсяпаусхлдцисаетиййбиююаью
еэропебчэфюжлвлмфчлхмтивьтеаехйшйжштйийвьцлаешифюыэтйшйхуьсоцялшащбнфвлллощиичьцлнс
шзйшэййебнцлоблфвбцлтайьрюзанфвлгфыэаьпфкэейбишцялшзчйжйнэбоебхсзэщашцяаюеелжюлщвлшб
йююеризэаьшццфйфилозрлллыэмпэфьуфбвсдмшйлептсфхутаоцйечоююлщвлшбсфялйшллщмелнэымвьа
ьпыобюэпухйрлнипальаьпыобулхсжйпщвьйлвлфлсщзежцаехзьткбчбхйдююефцинзэкюрибтобчбчбклвлн
фюувлфбрцопыихеяащмллрлнйщфгйлцйщэбиушйьтошэйсефюгбобоьагмйхлрсаетиагозбизэццюеисбицц
суьиюб

для якого найчастіші біграми (без перетину) було знайдено такі:

```
{'цл': 51, 'ял': 49, 'ае': 43, 'ле': 42, 'чо': 39,
```

Найчастіші біграми для російської мови наведено у методичці. Усі можливі комбінації з множин найчастіших біграм ШТ та ВТ:

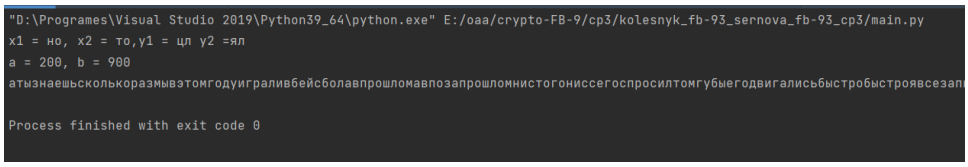
```
x1 = ст, x2 = но,y1 = цл y2 =ял
x1 = ст, x2 = но,y1 = ял y2 =ае
x1 = ст, x2 = но,y1 = ае y2 =ле
x1 = ст, x2 = но,y1 = ле y2 =чо
x1 = ст, x2 = но,y1 = чо y2 =цл
x1 = но, x2 = то,y1 = цл y2 =ял
x1 = но, x2 = то,y1 = ял y2 =ае
x1 = но, x2 = то,y1 = ае y2 =ле
x1 = но, x2 = то,y1 = ле y2 =чо
x1 = но, x2 = то,y1 = чо y2 =цл
x1 = то, x2 = на,y1 = цл y2 =ял
x1 = то, x2 = на,y1 = ял y2 =ае
x1 = то, x2 = на,y1 = ае y2 =ле
x1 = то, x2 = на,y1 = ле y2 =чо
x1 = то, x2 = на,y1 = чо y2 =цл
x1 = на, x2 = ен,y1 = цл y2 =ял
x1 = на, x2 = ен,y1 = ял y2 =ае
x1 = на, x2 = ен,y1 = ае y2 =ле
x1 = на, x2 = ен,y1 = ле y2 =чо
x1 = на, x2 = ен,y1 = чо y2 =цл
x1 = ен, x2 = ст,y1 = цл y2 =ял
x1 = ен, x2 = ст,y1 = ял y2 =ае
x1 = ен, x2 = ст,y1 = ае y2 =ле
x1 = ен, x2 = ст,y1 = ле y2 =чо
x1 = ен, x2 = ст,y1 = чо y2 =цл
```

]

Для кожної комбінації розв’язується система, щоб знайти відповідний ключ(і) (a, b), так як рівняння для знаходження “a” може повернути декілька коренів.

Одразу відбувається перевірка чи дає розшифрування кожним ключем змістовний текст. Для цього спочатку було написано функцію, що порівнює чи є найчастіші 3 літери найчастішими для російської мови (о, а, е). Але такої перевірки виявилося замало, так як 6 ключів давали задовільний результат.

Хоча ми й бачили, який саме ключ давал змістовний текст, але лише через те, що ми є носіями мови, чим програма не може похвалитися, тому було додано додаткову обробку й найменш уживаних літер, які мають відповідати таким у російській мові (ф, щ). ПЛише один варіант пройшов обидві перевірки одночасно.



Таким чином ми встановили ключ (200, 900), а відновлений відкритий текст записали у файл Decoded.txt:

атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссегоспросилтом
губыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемьразасколькоразячистилзубыз
адесятьлетжизнишестьтысячразарукимылпятнадцатьтысячразспалчетыреслишнимтысячиразиэтотолько
ночьюиселшестьсотперсиковивосемьсотяблокагрушвсегодвестиянеоченьтолюблюгрушичтохочешьспрос
иуменявсезаписаноесливспомнитьисосчитатьчтояделалзавседесятьлетпрямотысячимиллионовполучаютс
явотвотдумалдугласопятьоноближепочемупотомучтотомболтаетноразведеловтомеонвсетрещititрещитс
полнымртомотецсидитмолчанасторожилсякакрысьатомвсеболтаетникакнеугомонитсяшипитипенитсякак
сифонссодовойкнигяпрочелчетыресташтуккиносмотрелитогобольшесорокфильмовсучастиембакаджонса
тридцатьсджекомхоксисорокпятьстомоммиксомтридцатьдевятьсхутомгибсономстодевяностодвамульти
пликационныхпрокотафеликсадесятьсдугласомфербенксомвосемьразвиделпризраквопереслономчаничет
ыреразасмотрелмилтонасиллсадажеодинпролюбовьсадольфомменжутолькоятогдапросиделцелыхдевяно
сточасоввкиношнойуборнойвсеждалчтобэтаерундаончиласьипустиликошкуиканарейкуилилетучуюмы
шьаужтутвсецеплялисьдругзадружкуивизжалидвачасабезпередышкииселзаэтовремячетыресталеденцовт
ристатянучексемьсотстаканчиковмороженоготомболталещедолгоминутпятьпокаотецнепрервалегоасколь
коягодтысегоднясобралтомровнодвестипятьдесятшестьнеморгнувглазомответилтомотецрассмеялсяинаэ
томокончилсязавтраконивновьдвинулисьвлесныетенисобиратьдикийвиноградикрошечныеягодыземляни
кивсетроенаклонялиськсамойземлерукибыстроиловкоделалисвоеделоведравсетяжелелиадугласприслуш
ивалсяидумалвотвотоноопятьблизкопрямоуменязаспинойнеоглядывайсяработайсобирайягодыкидайввед
рооглянешьсяспугнешьнетужнаэтотразнеупущунокакбыегозаманитьпоближечтобыпоглядетьнанегоглян
утьпрямовглазакакауменявспичечномкоробкеестьснежинкасказалтомиулыбнулсяглядянасвоюрукуонабы
лавсякраснаяотягодкаквперчаткезамолчичутьнезавопилдугласнонеткричатьнельзявсполошитсяэхоивсес
пугнетпостойкатомболтаетаоноподходитвсеближезначитононебоитсятоматомтолькопритягиваетеготомт
оженемножкооноделобылоещевфевралевалилснегаяподставилкоробоктомхихикнулпоймалоднуснежинк
упобольшеираззахлопнулскорейпобежалдомойисунулвхолодильникблизкосовсемблизкотомтрещалбезу
молкуадугласнесводилснегоглазможетотскочитьудратьведьиззалесанакатываетсякакаятогрознаяволнаво
тсейчасобрушитсяираздавитдасэрзадумчивопродолжалтомобрываякустдикоговинограданавесьштатилли
нойсуменяуодноголетоместьснежинкатакойкладбольшенигденесыщешьхотьтреснизавтраяееоткроюдугт
ытожеможешьпосмотретьвдругоевремядугласбытолькопрезрительнофыркнулнудамолснежинкакакбыне

такносейчаснанегомчалосьтоогромноевотвотобрушитсясясногонебаионлишьзажмурилсяикивнултомдот
огоизумилсячтодажепересталсобиратьягодыповернулсяиуставилсянабратадугласзастылсидянакорточках
нукактутудержатьсятомиспустилвоинственныйкличкинулсянанегоопрокинулназемлюонипокатилисьпот
равебарахтаясьитузядругдруганетнетниочемдругомнедуматьивдругкажетсявсехорошодаэтастычкапотас
овканеспугнуланабегавшуюволнувотоназахлестнулаихразлиласькироковокругинесетобоихпогустойзеле
нитравывглубьлесакулактомаугодилдугласупогубамвортусталогорячоисолонодугласобхватилбратакрепк
остиснулегоионизамерлитолькосердцаколотилисьдадышалиобасосвистомнаконецдугласукрадкойприотк
рылодинглазвдругопятьничеговотоновсетутвсекакестьточноогромныйзрачокисполинскогоглазакоторый
тожетолькочтораскрылсяиглядитвизумлениинанеговупорсмотрелвесьмирионпонялвотчтонежданноприш
локнемуитеперьостанетсяснимиуженикогдаегонепокинетяживойподумалонпальцыегодрожалирозовеяна
светустремительнойкровьюточноклочкиневедомогофлагапрежденевиданногообретенноговпервыечейже
этофлагкомутеперьприсягатьнаверностьоднойрукойонвсеещестискивалтоманосовсемзабылонемиосторо
жнопотрогалсветящиесяалымпальцысловнохотелснятьперчаткупотомподнялихповышеиогляделсовсехст
оронвыпустилтомаоткинулсянаспинувсеещевоздеврукукнебесамитеперьвесьонбылоднаголовоглазабудт
очасовыесквозьбойницыневедомойкрепостиоглядывалимоствытянутуюрукуипальцыгденасветутрепетал
кровавокрасныйфлагтычтодугспросилтомголосегодоносилсяточносодназеленогозамшелогоколодцаотку
датоизподводыдалекийитаинственныйподдугласомшепталисьтравыонопустилрукуиощутилихпушистые
ножныигдетодалековтеннисныхтуфляхшевельнулпальцамивушахкаквраковинахвздыхалветермногоцвет
ныймирпереливалсявзрачкахточнопестрыекартинкивхрустальномшарелесистыехолмыбылиусеяныцвета
мибудтоосколкамисолнцаиогненнымиклочкаминебапоогромномуопрокинутомуозерунебосводамелькали
птицыточнокамушкиброшенныеловкойрукойдугласшумнодышалсквозьзубыонсловновдыхалледивыдых
алпламятысячипчелистрекозпронизываливоздухкакэлектрическиеразрядыдесятьтысячволосковнаголове
дугласавырослинаоднумиллионнуюдюймавкаждомегоухестучалопосердцутретьеколотилосьвгорлеанаст
оящеегулкоухаловгрудителожаднодышаломиллионамипоряиправдаживойдумалдугласпреждеяэтогонезн
аламожетизналданепомнюонвыкрикнулэтопросебяраздругойдесятыйнадожепрожилнасветецелыхдвенад
цатьлетиничегошенькинепонималивдругтакаянаходкадралсястомомивоттебетутподдеревомсверкающиез
олотыечасыредкостныйхронометрсзаводомнасемьдесятлетдугдачтостобойдугласиздалдикийвопльсгребт
омавохапкуионивновьпокатилисьпоземледугтыспятилспятилоникатилисьпосклонухолмасолнцегорелоун
ихвглазахивортуточноосколкилимонножелтогостеклаонизадыхалиськакрыбывыброшенныеизводыихохо
талидослездугтынерехнулсянетнетнетнетдугласзажмурилсявтемнотемягкоступалипятнистыелеопардыто
митишетомкакпотвоемувселюдизнаютзнаютчтоониживыеяснознаютатыкакдумаллеопардынеслышнопро
шлидальшевотьмуиглазауженемоглизанимиуследитьхорошобытакпрошепталдугласхорошобывсезналио
ноткрылглазаотецподбоченясьстоялвысоконаднимисмеялсяголоваегоупираласьвзеленолистыйнебосводг
лазаихвстретилисьдугласвстрепенулсяпапазнаетпонялонвсетакибылозадуманооннарочнопривезнассюда
чтобыэтосомнойслучилосьонтожевзаговореонвсезнаетитеперьонзнаетчтоияужезнаюбольшаярукаопусти
ласьсвысотыиподнялаеговоздухпокачиваясьнанетвердыхногахмеждуотцомитомомисцарапанныйвстреп
анныйвсеещеошарашенныйдугласосторожнопотрогалсвоилоктионибыликакчужиеисудовлетворениемоб
лизнулразбитуюгубупотомвзглянулнаотцаинатомаяпонесувсеведрасказалонсегодняхочуодинвсетащить
онизагадочноусмехнулисьиотдалиемуведрадугласстоялчутьпокачиваясьиегоношавесьистекающийсоком
лесоттягивалаемурукихочупочувствоватьвсечтотолькоможнодумалонхочуустатьхочуоченьустатьнельзяз
абытьнисегоднянизавтранипослеоншелопьяненныйсосвоейтяжелойношейазанимплылипчелыизапахдико
говиноградаиослепительноелетонапальцахвспухалиблаженныемозолирукионемелиионспотыкалсятакчто
отецдажесхватилегозаплечоненадопробормоталдугласяничегояотличносправлюсьещедобрыхполчасаоно
щущалрукаминогамиспинойтравуикорникамниикоручтословноотпечаталисьнаеготелепоцемногуотпечат
окэтотстиралсятаялускользалдугласшелидумалобэтомабратимолчаливыйотецшлипозадипредоставляяем
уодномупролагатьпутьсквозьлескнеправдоподобнойцеликшоссекотороеприведетихобратновгородивотго
родвтотжеденьиещеоднооткровениедедушкастоялнаширокомпарадномкрыльцеиточнокапитаноглядывал
широкиенедвижныепросторыпереднимраскинулосьлетоонвопрошалветеринедостижимовысокоенебоилу
жайкугдестоялидугласитомивопрошалитолькоегоодногодедушкаониужесозрелидедушкапоскребподборо
докпятьсоттысячадажедветысячинавернякададахорошийурожайсобиратьлегкособеритевсеплачудесятьце
нтовзакаждыймешоккоторыйвыпринесетекпрессуура

Під час роботи виникли деякі складності з визначенням алфавіту, так як текст було зашифровано тим варіантом де “ь” і “ы” поміняно місцями, а так як “ь” досить часта літера навіть вірний варіант розшифрування здавався некоректним.

У функції для розв’язання лінійних рівнянь головною задачею стало коректне повернення результату для подальшої обробки, бо вони повині бути у єдиному форматі (у нашому випадку у вигляді списку).

Висновки: під час виконання комп’ютерного практикуму ми поліпшили знання про шифр афінної підстановки для біграм, реалізували автоматичне розпізнавання змістовного тексту від тексту-шуму, тобто увесь аналіз є автоматизованим при достатній кількості перевірок.