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

Лабораторна робота №3
З Криптографія

Виконали студенти группи ФБ-81
Дубравська О.
Зозуля А.

Перевірив
Чорний О.

Київ – 2020
08.11

Мета

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Завдання

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 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

Для знаходженя ключа була використана функція bruteforce() що в свою чергу використовує такі функції:

Bigram_counter_no_intersections() – підрахунок найчастіших біграмм ВТ

Crack_key() – за переданими двома біграммами ВТ та двома ШТ шукає ключ на основі розв'язку системи лінійних порівнянь

Gcd() – НСД

Inverse() – Пошук оберненого за модулем

Chr(), Ord() – перегружені функції для нового алфавіту

Check_rus() – перевірка тексту на змістовність (Було використано одразу два критерії по 3 перевірки в кожному: Частоти букв О, А, Е не менше 6% та частоти Щ, Я, Э не більше 1%. Незважаючи на «м'які» тести, через значну їх кількість, функція спрацьовує корректно, а «м'які перевірки» дозволяють гарантувати що навіть якщо через незначну довжину тексту було помітно порушено частоти відповідних букв- текст не буде відкинутий)

Программа по черзі виконує співставлення 625 випадків (по 5 біграмм ВТ та 5 біграмм ШТ), однак фактично їх виходить значно менше адже значна кількість співставлень відсікається за відсутності оберненого, або якщо біграмми ВТ та ШТ повторились

Найчастіші біграмми ШТ: ЩЕ, ХЕ, ЧВ, ЛЕ, ЦВ

За результатами роботи функції bruteforce() знаходиться ключ, за допомогою якого здійснюється розшифровка у функції decrypt()

Далі наведено ШТ та відповідний ВТ

ШТ

ывлеюгзебщпещхщуйэвиывиюфгувхцубхщыюнюжлепэшфмиьхдощбуднзегдщебоцвшуюгьпцвэщувкмзеиэбчиюндхщюасдбмон
хегщгдэщжезьщемвощфысьмайыегыйяййыэшжеаекидщщеюжгьдеьцонгочвнюиюыжвюудеьбюгьщесфвшвоюзйэящкщьюгочвню
лмшужеейцурпцвдэяхщаюьдеуэвющэвдиайятвепцвчвлеюйщецыаешвэеяикгехщаэациэибвкмрйжуажййдекущтепэшфмздсу
гьвоцвяйкзфтшшхдуюиьйынюгдхацовойэращеюияциаяимюыжцввджвяцэввлломоодмхщуйэмюэзопюзкнэщегбдсефвьхбжще
нюцатщввэиегтеаехохтюйлдицзьхдщщщюяьзщюоцвлеюосдлузлзащавызйферддьйомюиаыьепжмнюбжщцаещээойтзэвзвщуп
мюжьощшаощвыжееююззьдеаейюшдоездюйбпгьвиюэколпщхмоихсшфеэмлеотзомщйвхцывбжхебахиэьщхйэашжеттфележебд
фюфпнюфмшуиэжяппшдгдщесдцжцвхеюцхеяднвжееютбзййысддемилпмюзахшнюлллоюэпподйшяюьхщужиуцтабззлзьйопнбо
ящпиэщииамленйхдбднвнщлврпшилмиьадшахушайыэффтппмюцдсззезщадцьцихжшуфгбиэихеныжпбоцднесдегмаущйыктгд
ыйктййнвмоктздгидатаомтщлвхеийрдимяцшуьюывмтшзюашнэьгоэавюрдвджгмпиээщеиэивдодзехатщйыэшззшзунзщхеюи
зчсдэайэхенвжьфжпсхгчплвжмвиртдэппщуртцюиэппедчйдещорпдпвюбжлотвдюлофехщыддетеодаьйояхрдбмлпнднелеыщ
хдощуцщазнибыутвднтащебацэзьгордфесьаещзкнсднюятьдаахмчвюцхеиовющежемпзькюжямюгьщцсбвдсчепзлепэшбмтв
гоэвубюзмвппцинэзьэщтапуиэпхлеоенщнщрдэщлабмхтфуиюййаещэдэвлюцрпбжэщыдидсдщохилпийшгмищцвюбйощйапедм
лесгцатьчщбуэьгйцамиэавдкюяцрорпбдкьйомьщеаохдяючвейчвзухвьхэерючежюшзюахмрпяйзхфйдыжецэзчящктмоодьь
епюйяйрйощоюцдиеиатщхщнеэмьхгьощщеоюиьвдгивюыжшухехщкдэщжюяцлщлейдюйбпгьюйяйгдиднидбосдьдиараощаагю
ывмтвдцэззяхщаыйжгпюфпэшяияйхмлпияюцмахщмайвкмшуовывбочвгййобуиэывзджююцгйбасдйэвюэасуяхуцбущуфтлпэь
вмхшоеяхрпдюцибофебаитвлпхлпэьуеюююэлпбийэлпбинюфугьвоцвхестюцгдтэфйнеэатщщавытдщааошумюжячеaееоодзт
лояййысьюцсьмашайыьхлеяюсбфеюоэщуйзлепрдюйкизолюуцобуйюгктнвэиииюдэяхщагююцхенедефепэлпсаийкиящбушзшз
унтахаьыхдрпдэьщчижеьюхибунюзьдесьюцаетщфеюайвкмжгеэзчхаздхенехднвящжесьвчаеяютвючсьцукммюфпэьхцхене
ещжпмюфгцвцвзщяшдыээжежуйэфгэзюайыччюднвкгшвиьвчлпэьяьхэжмьхиьбщйыфпжягьматщаефмлесгцадьтцэьакгдйпгц
эьдемимоэщчртщгдьцэьщщузмюнпамвикнсшувлонвиюовкмлебпчвмвзьжемвшзгдяиампнлоппбообхдвыхщнвшуялнюгьэабу
охобхдзечадыегжеыщхдктеаюаирюунедмщуудвайыэанвфупдэмчвмьщелеяймоюааачвэуопэьжеюэюааееыпхщаэаяхзснгые
тепюхиэьаелецюктпмзшршеьбюекгдьвтщщдчиубждгдхеьцкнвюиэвднвфузчшщдетадшимжйцумюэщчйощйаэмтщвдеьйомюхе
бавахивлфеионвздоюубтесаыдхщнвшуцуюэрдцзщхмвлоцущцшайюшдрддебочищукмжйпиуцфйжпщцоеидфгшйощемлмжгвдфв
юаюообюаюьймвшжеэуяххариндщщэшгщчикгялнювамжфуощпйццмюегнещеегбдфюфпюйбпгьфпжяиэцвтбнещеегбмлещщзеяй
ьддьяецыфгсцфжтбшвяцвиощиалещщнвбчрйхаюиючпммьшгяошулобжфгфиыжпптбшвиьййраыьнщеаощяэшулопдицщццаявяц
буиьэщхдвыбщпееыаебухтвдсдощийыщцыэщзщцймилмлежщощрасгиацэиюшщыйзащеоюиьцвмтшзлебджювшщхщужиубяэшуло
пдхомццвяйощвыявжявщэаадощыщтщкщфйыьжеуцщуыднвлеьэяхщабммоппмвппдюлмледшяйдужижиженввиищятпнзетечютд
юйбпгьчизднвепфйзщиакунэшщфпызяйтьхиэиианвзшущиорпбдпюцижефвчвйэгцлпнющецыаеямтщтаэаощськммочиэилпбо
одэаьдааощчвощоюшдийрднпцвдщнюиадежпиэвиьхсшрдехщуйэтфппрюфпюцпмлпиящцоугьцааюфпэьаэвдтщфеоещпхэбонн
ощиафпжяфпцвчвжьфждэлолвяьчвдодэйайыжевыоененезаиаразевыбвжйцулмлепеяшдерйхаюиияэяхщагютврюфпэшиацаыв
вюсюлоюэуцвшэщйыаегюфпгьпднеизящсджпннхезефюфпящчвэвьхлммьдшоюьхиьрйрарежюгьщелекщтьээмюфзнэцвсдмаае
юиэисьмюцвзиубэфгщдещечйшвюзкоусжээщтеяииюфггщкееюччэацапесьзецюмозьхцоуоеуюмодшяййыхетеуиэижецээчтэ
гчяййыбозэгчяййымааейшгюдпюйбпгьищщхйэзьлвепцвсдчйыутвывяцбехдыиьхзавдсщяобамщсдэанелезатэфйфщиээщне
жетщгдидчвряоеуюжйжпннтвшивлугцхлехщтапэсбеелеяоодгджюубвюцдеюччщупнлмлеяешайыиалимьящфгмючехйуышзко
усбщмазщбиьхзазьйысьзьюауйжекюжмтщкдцьщхйэашцаающвмабзнэщежееюсюбжовщцэапейцщцвюлозьйычвййзаятдпэшьх
леяюсбеужищеегдьдэбоодфееаоененетщкервтвэитзщанезчудйожецэзчкмючсджэзлрдяюнюиюэзмюсетпыжтащенепхсшыщ
ьвчвнюлоиэяцсбэапепещдйогдыйхедетамайвднвюдэяхщавомоодбпртгьоецуппиачпковфндхщоедесшсдкюэьдэяцсдцааю
цвэщфепэюцзасеяинэшзчуртэщсззееысдкюмвежцищемарцзлцвпепемайыщпзьуасьцвэиюэяхщавоцэлеююфпрдеыэвчвтаае
увзетеьджюсббамщиаиьмахенщщавысьщцяцодчэтдбщпенегдеаиююуэзлвиюэзлпмотвяьреэщдепвлпзщшаощсуяхсуяхлпви
дшхщпелееецацабацыещзщеггдюпшщмцкнвюутючшабщощщщэщжлзьдшфглоиэюаэьубяшбммьшгжюуббуиьппбжхееэщуьхамьх
фйсщощвыятжмючктюцощщпвлхешекюиэзоднефепэчщущхдижппчиртлпчврянюбоодщэзопсеьаохтгднщхекудээиэибацыещ
кибохтгдййаююэяхщаяэяхщавонвздадяйтьреошйынщмаонгоюзщатаььтаэазехдвьнйнвэьдюртюцгсдееэюцгющцччщупнлм
жмящнюпхмьшияцдеыуппамрпзьроадздыщчврялежпсбамгдещнвсбэаэщьэяхщаеадежпиээщщьюцмюепаелешгкитвяцдееюдп
эьдюиюложьвиибпейцамиьоецуппбозацыжервщцжиртлпцацытдоехдсвщцюзмвусщекуяцфгкмрпцвсдчйбщцщлоцвкгвюфттщ
нгкмжгпййождгдфгнхрйжщиаквбжхебуктюаоюцдзщшгюйбпгьбпбюфпбвмьщелеяйэщщднесдроюэппамбжронвжешатьэзребц
июывэцчврятазщрдюйкизоажхенежетщттхздэтахщшщсьцвэиюэяхщалттвящуэбчиюндамтщжпунлпэшшвчвйэрпуюиьрйещйы
эшдеюйбазеашлльюусзочвцаделекюцииайгшацвэшвдсдтщеорпиьчврясдщелечпбопнххлпфмшуиэщщсдлоиэледещохиболп
жйсднегужиоаэвбжронвпйцвгщнюаеегыюфпждвпщюиьаепзкнбатахщьпсефггдяилмепэшэвчвадздююубиьмюмтчеодеычмдэ
лпепэьйыямвиртюцсшсднвлптвэиубшштиубзчшгыьгйцаоиэивюрдрячиртлпщещьмоодяюзьжгхюйэяхщабмчвлеааатюцгсхе
эщщднесдюфывепнюсьлоздшшианвщузлмюхебуэьрймщшатьтцьеэуллмюзэгцлпнюшвчвиьрйещеьбюбжщенюиьмахенщтьаобч
йэылщхрдшгматжщешгмааеюцжьгджювитщразервяцсехдйнощзацыбддебщпезмйэтвощжестюцгдиавоцвмюцвэуллотвнюжн
мющхлеуииьтаэазехдющдетаэадужиубхошунхрдощнвшардздхылофмгдмащавыцюэздщощоеядьзхвдюэзмочпцвлпиьгоощнв
пйсьшузохефпызяйтьрехджоодэввифйядшаждгдфггщнерйюглофцчвтщхдвыпелебдеыаеьйнщыщхдгдбмгдхдбщььзецюьхнэ
сфибнвиювичврянвзшрйвдзджюлмгчхтзбчишщюаюьтайгшаощюоэшййшоэшещяйгдтидщвоюзйэхесдегжщюаыьзекжгьщенюэь
щцфцжштьыьжеуцюаюьтаэахщчвэвьхэеэщхдупндидвоюзйэсдвчщупнлмтщжпежуддежпунтвовднвюяхмощуепнюдещечйшвчв
ьхзанэудеьщйжпннтвшиэихещщеьаожецэзчкмопияжмрплобчжоцвмозохтюйквэипхнэмвижппщцюэдэтвэипхнэмвзочвжпнн
мвцвщцэардздхытцбойэлмдэяццыцвэшявхжпдидьдмаеылочводэжгьюйбауэяхщавочвнюжйядтпктаевшэфмюлоылмьмоодпз
ощпищуээяцыщзщиовюьхюааьтаэазехдзющцдевдюпиьоецумбииюмюдэпааюфпбуиьээзяхщагючвяцсехдзюэизеэщощвыам
ьхфйсщощфйзщшнюучаущюимьюжфучугьоддпэьовлмяхусидгшкухтхеажщедещиюаугшазевытпктепиьсхчвмоюзопщувюывяь
чщдецуыьбщщхйэунищцжфтзелммьщебджюсбюанвшубюфгеэяхщаыйцачюэирпмюамлпияцднеунощбпвзвимождгдяйдвмюьщег
фгыюфпсесакумюфгоажгщьвияцжпмохенюятздэаьпзьхегехщыйяйдужибочвэухвэсюаяйбацыещзщэабвюатайывдсуыжывдю
иэмошушйиадечюмюзэциуцнщхекудэяцепзьхестюцсшэщаеиовифйлхнэлвижппикщежесьмюкмщджгмяппсбхщжвччнюшияцюу
жгщдеьжечмзьмюййнежетщщехдйанюэьюэлвиаэабнппяцнвжегдпмзобднердздшамйдвеавэнщещамхвусеьыьрйчайыгдчиэи
жпунудщехехдьжывмиькдбовшвыэьаееадебпээкоудкюдэяхщаеапехдизопбжщещечирттвдюлмлеоелжлпчвййщщгдидййте
льиюдохжящэаюйбатьцчгдкьвдюжвюубщпзьсюцвбжщефебалимьтесьюцсуяхубвдыюэенвздажщеощшшщешежэудеьоезелалл
жмадбщяиэиюайгкукоудеьээяхщабмшузьмасллотвьщдецуьхлпйтаияцгпэзбоцвещяйсдкюцвюзаихевджюсбеавэнщшвяцзщ
цюфпбуйэрпхаьллотвюшдеэщбачмжмвддыллкмбжбщжпежепиьаэгцуджэяхщагюфтианжщеэвнюэехеяецыойидкмхшоекуяцдэ
хеажщещещхиьнйююфпьхрдяднючвкмшууеошйыунзебчвййнвсдчхрдщеэаяюубсдкюцвцэзьовывхшфеьэяхщащщбмйэбщкижм
юфпмлпвоубкщжещехеэфлошусдеьбюдэчврпшинююцхеиилмйэзлзайыяецыхесдийрддшллььоуссдэахдоехеаеяюкмтщрдкюхт
ыжюцядэащдба

ВТ

утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоиветербыллетнийтеплоедыханиемиранеспешноеиленивоестоитлишьвстатьвысунутьсявокошкоитотчаспоймешьвотоначинаетсянастоящаясвободаижизньвотонопервоеутролетадуглассполдингдвенадцатилетотродутолькочтооткрылглазаикаквтеплуюречкупогрузилсявпредрассветнуюбезмятежностьонлежалвсводчатойкомнаткеначетвертомэтажевовсемгороденебылобашнивышеиоттогочтоонпарилтаквысоковоздухевместесиюньскимветромвнемрождаласьчудодейственнаясилапоночамкогдавязыдубыикленысливалисьводнобеспокойноеморедугласокидывалеговзглядомпронзавшимтьмуточномаякисегодняводоровошепнулонвпередицелоелетонесчетноемножестводнейчутьнеполкалендаряонужевиделсебямногорукимкакбожествошиваизкнижкипропутешествиятолькопоспевайрватьещезеленыеяблокиперсикичерныекакночьсливыегоневытащитьизлесуизкустовизречкиакакприятнобудетпомерзнутьзабравшисьвзаиндевелыйледниккаквеселожаритьсявбабушкинойкухнезаодностысячьюцыплятапоказаделоразвнедельюемупозволялиночеватьневдомикепососедствугдеспалиегородителиимладшийбратишкатомаздесьвдедовскойбашнеонвзбегалпотемнойвинтовойлестниценасамыйверхиложилсяспатьвэтойобителикудесникасредигромовивиденийаспозаранкукогдадажемолочникещенезвякалбутылкаминаулицахонпросыпалсяиприступалкзаветномуволшебствустоявтемнотеуоткрытогоокнаоннабралполнуюгрудьвоздухаиизовсехсилдунулуличныефонаримигомпогаслиточносвечкиначерномименинномпирогедугласдунулещеиещеивнебеначалигаснутьзвездыдугласулыбнулсяткнулпальцемтамитамтеперьтутиводтутвпредутреннемтуманеодинзадругимпрорезалисьпрямоугольникивдомахзажигалисьогнидалекодалеконарассветнойземлевдругозариласьцелаявереницаоконвсемзевнутьвсемвставатьогромныйдомвнизуожилдедушкавынимайзубыизстаканадугласнемногоподождалбабушкаипрабабушкажарьтеоладьисквознякпронесповсемкоридорамтеплыйдухжареноготестаивовсехкомнатахвстрепенулисьмногочисленныететкидядьядвоюродныебратьяисестрычтосехалисьсюдапогоститьулицастариковпросыпайсямиссэленлумисполковникфрилеймиссисбентлипокашляйтевстаньтепроглотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайтелошадьвыводитеизсараяфургонпораехатьзастарьемпотусторонуоврагаоткрылисвоидраконьиглазаугрюмыеособнякискоровнизупоявятсянаэлектрическойзеленоймашинедвестарухиипокатятпоутреннимулицамприветственномахаякаждойвстречнойсобакемистертридденбегитевтрамвайноедепоивскорепоузкимрусламмощеныхулицпоплыветтрамвайрассыпаявокругжаркиесиниеискрыджонхафчарливудменвыготовышепнулдугласулицедетейготовыспросилонубейсбольныхмячейчтомоклинаросистыхлужайкахупустыхверевочныхкачелейчтоскучаясвисалисдеревьевмампаптомпроснитесьтихонькопрозвенелибудильникигулкопробиличасыназданиисудаточносетьзаброшеннаяегорукойсдеревьеввзметнулисьптицыизапелидирижируясвоиморкестромдугласповелительнопротянулрукуквостокуивзошлосолнцедугласскрестилрукинагрудииулыбнулсякакнастоящийволшебникоттотодумалонтолькояприказаливсеповскакаливсезабегалиотличноебудетлетоионнапоследокогляделгородищелкнулемупальцамираспахнулисьдверидомовлюдивышлинаулицулетотысячадевятьсотдвадцатьвосьмогогоданачалосьвтоутропроходяполужайкедугласнаткнулсянапаутинуневидимаянитькоснуласьеголбаинеслышнолопнулаиотэтогопустячногослучаяоннасторожилсяденьбудетнетакойкаквсенетакойещеипотомучтобываютднисотканныеизоднихзапаховсловновесьмирможновтянутьносомкаквоздухвдохнутьивыдохнутьтакобяснялдугласуиегодесятилетнемубратутомуотецкогдавезихвмашинезагородавдругиедниговорилещеотецможноуслышатькаждыйгромикаждыйшорохвселеннойиныеднихорошопробоватьнавкусаиныенающупьабываютитакиекогдаестьвсесразувотнапримерсегодняпахнеттакбудтоводнуночьтамзахолмаминевестьоткудавзялсяогромныйфруктовыйсадивседосамогогоризонтатакиблагоухаетввоздухепахнетдождемнонанебениоблачкатогоиглядиктотоневедомыйзахохочетвлесунопокатамтишинадугласвовсеглазасмотрелнаплывущиемимополянетнисадомнепахнетнидождемдаиоткудабыразнияблоньнетнитучиктотамможетхохотатьвлесуавсетакидугласвздрогнулденьэтоткакойтоособенныймашинаостановиласьвсамомсердцетихоголесаануребятанебаловатьсяониподталкивалидругдругалоктямихорошопапамальчикивылезлиизмашинызахватилисиниежестяныеведраисойдяспустынноймроселочнойдорогипогрузилисьвзапахиземливлажнойотнедавнегодождяищитепчелсказалотецонивсегдавьютсявозлевиноградакакмальчишкивозлекухнидугласдугласвстрепенулсяопятьвитаешьвоблакахсказалотецспустисьназеплюпойдемснамихорошопапаионигуськомпобрелиполесувпередиотецрослыйиплечистыйзанимдугласапоследнимсеменилкоротышкатомподнялисьнаневысокийхолмипосмотреливдальвонтамуказалпальцемотецтамобитаютогромныеполетнемутихиеветрыинезримыеплывутвзеленыхглубинахточнопризрачныекитыдугласглянулвтусторонуничегонеувиделипочувствовалсебяобманутымотецкакидедушкавечноговоритзагадкамииивсетакидугласзатаилдыханиеиприслушалсячтотодолжнослучитьсяподумалоняужзнаюавотпапоротникназываетсявенеринволосотецнетороплivошагалвпередсинееведропозвякивалоунеговрукеаэточувствуетеионковырнулземлюноскомбашмакамиллионылеткопилсяэтотперегнойосеньзаосеньюпадалилистьяпоказеМлянесталатакоймягкойухтыяступаюкакиндеецсказалтомсовсемнеслышнодугласпотрогалземлюноничегонеощутилонвсевремянастороженноприслушивалсямыокруженыдумалончтотослучитсяночтооностановилсявыходижегдетытамчтотытакоемысленнокричалонтомиотецшлидальшепотихойподатливойземленасветенеткружеватоньшенегромкосказалотеципоказалрукойвверхгделиствадеревьеввплеталасьвнебоилиможетбытьнебовплеталосьвлиствуверавноулыбнулсяотецвсеэтокружевазеленыеиголубыевсмотритесьхорошенькоиувидителесплететихсловногудящийстанокотецстоялуверенопохозяйскиирассказывалимвсякуювсячинулегкоисвободноневыбираясловчастоонисамсмеялсясвоимрассказамиотэтогоонитеклиещесвободнеехорошоприслучаепослушатьтишинуговорилонпотомучтотогдаудаетсяуслышатькакноситсяввоздухепыльцаполевыхцветовавоздухтакигудитпчеламидадатакигудитавотслышитетамзадеревьямиводопадомльетсяптичьещебетаньевотсейчасдумалдугласвотоноужеблизкоаященевижусовсемблизкорядомдикийвиноградсказалотецнамповезлосмотритеканенадоахнулпросебядугласнотомиотецнаклонилисьипогрузилирукившуршащийкустчарырассеялисьтопугающееигрозноечтоподкрадывалосьблизилосьготовобылоринутьсяиипотрястиегодушуисчезлоопустошенныйрастерянныйдугласупалнаколенипальцыегоушлиглубоковзеленуютеньивынырнулиобагренныеалымсокомсловноонвзрезаллесножомисунулрукивоткрытуюранумальчикизавтракатьведрачутьнедоверхунаполненыдикимвиноградомилеснойземляникойвокруггудятпчелыэтововсенепчелыацелыймиртихонькомурлычетсвоюпесенкуговоритотецаонисидятназамшеломстволеупавшегодереважуютсандвичииипытаютсяслушатьлескакслушаетонотецчутьпосмеиваясьискосапоглядываетнадугласахотелбылочтотосказатьнопромолчалоткусилещекусоксандвичаизадумалсяхлебсветчинойвлесунеточтодомавкуссовсемдругойверноостреечтолимятойотдаетсмолойаужаппетиткакразыгрываетсядугласпересталжеватьипотрогалязыкомхлебиветчинунетнетобыкновенныйсандвичтомкивнулпродолжаяжеватьяпонимаюпапведьужепочтислучилосьдумаетдугласнезнаючтоэтоноонобольшущеепрямогромадноечтотоегоспугнулогдежеонотеперьопятьушловтоткустнетгдетозамнойнетнетздесьтутрядомдугласисподтишкапощупалсвойживотоноещевернетсянадотольконемножкоподождатьбольнонебудетяужзнаюнезатемонокомнепридетнозачемжезачема

Висновки

- В результаті роботи отримано навички по роботі з афінним шифром, в першу чергу- з його криптоаналізом.
- Афінний шифр можна вважати за виконання певних умов достатньо надійним до ручного криптоналізу, що однак базується не на надійності шифру, а на тому що людина не здатна до швидкого виконання малих монотонних повторюваних дій. Для процессора розшифрування афінного шифру не є проблемою.
- Python не дуже підходить для криптоаналізу, C++ би српрацював в рази швидше.