МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Варіант 5

Виконали:

студенти гр. ФБ-11

Цема В.В.

Ципун Р.Г.

Перевірила

Селюх П. В.

Київ 2023

Мета роботи

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

Порядок виконання роботи

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

Текст

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнс
дуэммндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкяс
ввццтнавпьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзцюс
фспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсгцыз
зфрщихзтчщрихнэпозтгфккчщкдмклыоьеынуййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсх
эццьедктництндуццоэивупхюфйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбин
курдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшдекхн
дуаошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьби
шиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжц
рнмющькккюиеуяэзтьяяреурндуьцоэгкмбобмщкскехюксдцтсывзтмсунйьксщиссшнчщзй
ьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйнмсуншснхтуйнцц
мсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбу
тнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьйнвнцх
ркпрыожврщьянкиюджкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяышвнунх
щлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщмб
риввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяю
суйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбьеелфеипвидийдкяязщ
пупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсис
цйвнихчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзих
ывуллвовявшньсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвац
лотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийд
ьяшншвосюсчязиьсунуллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгйрщтнгбфд
зйьцэибусчжвавмнззфдыоиюшсосюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщх
ичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшнищюиьсщожсюдгнуцрнчзшр
ынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшвнюдцфвдыоияосунй
пщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуццщ

щцспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвынуняуумпьшвшр
ццисcцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожяш
сввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсстгнхщщщфд
дбтьпнзкьеэдхнщьжвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрс
нсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьсцклжшвнунакуба
кюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвпьызмбйнвнцхпн
уцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцт
сывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьавтулцибсчннисозфдыожллрдцбщшдск
рщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфсчсщьавпьскггыоющлхвииспьвиулбут
нзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщ
йеуйнзщшьявхщеуеидебупьесузющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищь
ккффдкфьнхчщмщявисчтжьамаофисрябсчшижслбубщэнщфдэмсщябубчзйсанэирщхщм
сэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюиищщшдекщсхдскхсовпннчубакакхуямдк
яяхсвнхбжсмкщнщьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцсп
рыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьвнбкубьебчсвйнжндуеисхавупмююсшодкл
ьулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщ
убссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнх
щыглозфьцэидктнунэибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщву
цфьцжьщнмкпмдкяярнэирщввпноулцфрынщхыщмснфжврйвньркзскыщссвнхбрифкясо
зййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьичдрщдкикгбмщб
ущстссвйьшвоейулцгйщшфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфи
шдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзищссыршьудццрреулфщщаефд
хссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнмспбмщбущськмюннисдкдкц
фжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщькккгнввшни
вжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньбиулбунхнчйдпнввкцйнуншвэьт
нщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщбущсфрмщчяовупмюосш
нкуаохщмсэкццзтбыыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихщавиэ
жьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкм
бкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамозмщбвс
каьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкиющькккбыоскчицпьявиц
чзивяьочлцсвпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяякду
нкчзжсюсбчкнбквьфзтнуноьюддкнхживналбуыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтс
ывзтьятнакфкпрябйожсюсунюиикцфтсввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсс
тхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгьерынньэьынавэк
иютыннькиютноьакеишдщщшвпвмндтихжцшнйнюирсыэьяокпмаобщцсэщбушсхщмсэк
ссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунтсчтгвмьввьелвмкрюеэз
тдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпв
юскиосырынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихв
нстйнянцуфкщщцсунхдицяедьакхуумжсвнчрлвньзтьяйкчзезьцюсжрыщумьцэиясезьцвн
внунищьеяцпьерынхщщцыцвиьянсибясшнлсиьпвтснфюирыюсцьаккнивжошижсмкарс
сжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяспнчкх
уцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщ
шдбофдгвмсжкддьяжьяущнввввшнмьвврщозенйсуньейпфкаьтныоеущькхзцнулцзтднче
лвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхмьакггмщшд
жсунлххэхьзтлрэчбудкввзнввшнжьжврщунынжвжрццисчцэиаьмчврщищссркжэжвмнд
тфрлцяьклхнгцязвэкьзцэиьшсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмсл
дзьлсрщйносыклрлврнввлэусхщрнавпьгбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщ
шдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкрижэпншн
хщынгспнунрнгошддкяяфсшьыоарфдрижлццэччсавпьзншвйнрнкизфтсиспынкгбмщбущ
ссцшнмьввьщянмсхмдктнянккбщшдекццжлывйквэпншнхщынгспныэрнгошддкйыявзтц

нюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвюдцфюирыусунлрлцдкяя
ыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбрыяьц
щжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшныйнмьунжкиюхщлвхщпэжвчсп
ьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчсжвюсстибдцньтсюсстхщээрщьечщк
змщрнтслкеурьйомюхщньюсстгнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуиюш
ннуяетнхщюиакфккчлспьыопьрцмнрншбынлсюдризьяуфкшдвчсксчавзтрщхсщв

Розшифрований текст

убиватьбольшененадопослетогокаконужеубилнаследуетемубытьблагодарныминачепри
шлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснова
нииодинаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещ
енныйнарциссизмэтическаяценностьэтойдоброты этимнеоспариваетсяможетбытьэтовоо
бщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособеннояснопрос
тупающийвчрезвычайномслучаеобремененногосознаниясвоейвиныписателянетсомнен
иячтоэтасимпатияпопричинеотождествлениярешительноопределилавыборматериаладо
стоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступник
аполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступни
кукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертн
огонаследияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоев
скийвгерманиибылобуреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпа
тологическойстрастикоторыйнеподдаетсяинойоценкенискакойсторонынебылонедостат
кавоправданияхэтогостранногоинедостойногоповедениячувствовиныкакэтонередкобыв
аетуневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевскийморотг
овариватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсяврассиюизбежавз
аключениявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточнопро
ницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавным
былаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассуд
ногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпокане
терялвсегоиграбыладлянеготакжесредствомсамонаказаниянесчетноеколичествораздава
лонмолодойженесловоиличестноесловобольшенеиграть илинеиграть вэтотденьионнару
шалэтословокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяие
едокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудовлет
ворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсявто
мчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестинаследую
щийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзаметилачтото
отчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепр
одвигалосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвяз
ивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниям
иккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозволялс
ебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодогописателян
етрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорнойст
растиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтрим
астеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотм
аленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляется
женщинаинакакиеудивительныедлянеесамойзаконо нарушенияеетолкаетнеожиданноеж
изненноевпечатлениенововеллаэтаеслиподвергнутьеепсихоаналитическомутолкованию
говоритоднакобезтакойоправдывающейтенденциигораздобольшепоказываетсовсеминое
общечеловеческоеилискореообщемужскоеитакоетолкованиестольявноподсказаночтонет
возможностиегонедопуститьдлясущностихудожественноготворчествахарактерночтопис
ательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчт

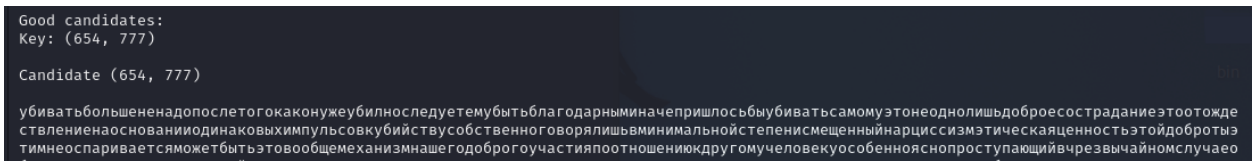
оупомянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврас
сказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэ
тойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережит
ьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуж
далисьотказавшаясяоткакихбытонибылонадежднасороквторомгодужизнионапопадаетв
овремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредив
сехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственность
юисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивого
юношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдаю
щейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывп
аркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинусл
едоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочислен
ныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужд
енавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитье
гопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоивше
мусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетиграться снабжает
егоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуход
омпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожер
твоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпуте
шествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздыва
етнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущением
обнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушите
льдолгавернулсякигреонанапоминаетемуобегообещаниинооджимыйстрастьюонбран
итсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыку
питьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсам
оубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправ
онасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпечатленияод
накопсихоанализучитчтоонавозникланаосновеумопостроямогововожденияпериодапол
овогосозреванияокаковомвожденииинекоторыевспоминаютсовершенносознательносог
ласноумопостроямомувожденииоматьдолжнасамавестиюношувполовуюжизньдлясп
асенияегоотзаслуживающегоопасенияврединанизмастольчастыесублимирующиехудож
ественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпо
рокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательски
свидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляетсяэквив
алентомстаройпотребностивонанизмениоднимсловомкромесловаигранельзяназватьетее
аа

Найчастіші біграми шифрованого тексту:

1. вн
2. тн
3. дк
4. хщ
5. ун

Спочатку програма шукає топ 5 найчастіших біграм зашифрованого тексту, далі співставляє їх з відповідними п’ятьма найчастішими біграмами в російській мові. Таким чином формуються різні комбінації, які надалі використовуються для пошуку ключів.

Ключ: (654, 777)



Розпізнавач російської мови

Для визначення того, чи являється текст інформативним використовувався підхід на основі частоти знаходження літери у тексті. Для кожного набору ключів аналізувався розшифрований текст, у випадку коли частота зустрічання літер “о” та “е” входить у норму, то текст вважається коректним.

Висновок:

У ході виконання даного практикуму було набуто знань з використання афінного шифру та методів його криптоаналізу. Навчилися аналізувати текст на його інформативність за допомогою статистичних даних, розглянули декілька моделей на основі яких проводився аналіз. допомогою статистичних даних, розглянули декілька моделей на основі яких проводився аналіз.