МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп’ютерний практикум №3

з дисципліни Криптографія:

«Криптоаналіз афінної біграмної підстановки»

Виконали:

Студенти групи ФБ-96

Сендецький Костянтин

Твердохлібов Денис

Київ 2019

Мета роботи

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 (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

У ході роботи реалізували підпрограмми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь.
Визначили 5 найчастіших біграм тексту варіанта 1 (‘рн’, ‘ыч’, ‘нк’, ‘цз’, ‘иа’).
Перебрали можливі варіанти співставлення частих біграм мови(«ст», «но», «то», «на», «ен») та частих біграм шифртексту. Для кожного кандидата на ключ було розшифровано текст.
За допомогою перевірки частот літер ‘а’,’о’,’е’,’ф’,’щ’,’ь’ для всіх розшифрованих текстів, знайшли оригінальний змістований текст.
Ключ (13,151)

Зашифрований текст (13, 151)

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйв
фяжтинфвйвйвсжнпчнмпгущзкыфвйвутсюцзкыкынмотзщбйыыбшхолуычгкицепзкианьуыфлл
фтыраючькиащзтыфэнкйяпезтнкжкккысечамнмпжэпаычйдбцвсшчмтшслаиятасзбчжйыыбшывл
тйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвгзжзычэявс
шчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщ
яцзреотйсфтбйщялчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвяз
аозеарчэяицкятчрогцфэкыпэзтйпчаэеэявахыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлч
окбцккузбнинепжвininачрнсджяцццаиятчщтецрнбяшквдиабцотияьаццйвычфткюмпьяэяддаь
ччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоья
ючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычц
яучпяэязяшкинвдэякзюнзтмакырцсоушрнецчнкяуялжочознкьызацчнкяжсгмпчнвдепйдрчкеэя
рклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнйцнбшзикзчшклзпеепаопниашчеквдзеязэгце
ккьызацчнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытн

щрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбц
яыыцлтбцдйрцецкзвзвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззя
бчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштх
лтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрн
вязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзг
зщырнэяччяыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэ
ззвьдчекеэгызнзтчнпнивучппжкнкэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхч
тыыззэивьяньзяфякщтыээчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойзьялчуцднеэнпейвя
зярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнмпмэья
ючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуыч
мебцкяюцотноыкиащзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесорк
ееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтй
срнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутсюцзкыфпцеэярнкецз
кышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвецыог
збшучяпхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддь
ыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфя
пьзеебччцщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчтыгшшчкгнккршчтчиншчияцзывь
яючбятьюьюаьыкьзаучйзтысюиебчщзечучючькваднеэльачрнвязарчтчйдбйеплюрбучэтийшчр
нвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэ
ипкйчнезучлчмыбшхыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдз
еотечамнклзйяебччекфвйкинвдщыечикфвжяццзебчочьвеслеяздчюзюабйчыикфтщрчащяцзшс
иаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяшкжкмафпзкфвч
ьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачя
юцйдбцььэтнкфякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлч
цяцйцнйамврьйпзквдзтмаьпнкэофяйтмпдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяа
щявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычицнввдевинзтсолчспейцаыяч
ыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшд
эпаычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчыз
якиащзфяеыюччажсчащзьянвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццн
кпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнй
вдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзкеэзщйхча
щзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрн
вязарчтчсжлжыяызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшч
учлжияшкрбнитятнрцшчрнгятчлаэтмэщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсят
чтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпацытыызкьццзтьянввящыбчя
ыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнк
ыкряеыичвзрнпйкщтыызэээкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинр
цбйзтрнзьфлшхфэычаэгмнкуффтчавяюзаояалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзай
яхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчучючцяцзицтллфвычялкшяю
аэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкбцкя
цяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтч
юеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецн
мяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебччцеопнхофяжтгщачрнвязаозгкзщ
пцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцотцяьнщ
ммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырн

бчнксяжцпажэецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвы
рчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкыозрнотмусзщяхаэбычпабшкытнщммпрбчачяя
зсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжцзеотлжееинеэнрычщывжкк
йэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнввджкйсиахыычяктзфятыыяько
ыечзнзтчхучычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаы
чэкуфиахыпнхофяяаяжеы

Розшифрований текст

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневр
отикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейнассложн
остинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазовывелича
йшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайшихдос
тиженийиировойлитературыпереоценитькотороеневозможноксожалениюпередпроблемойпис
ательскоготворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакм
оралистпредставляяегочеловекомвысоконравственнымнатомосновании чтотолькототдостигае
твысшегонравственногосовершенствактопрошелчерезглубочайшиебездныгреховностимыигн
орируемодносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеис
пытываемоеискушениеприэтомемунеподдаваяськтожепопеременноготогрешиттораскаиваясьст
авитсебевысокиенравственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястр
оитсвоюжизньоннеисполняетосновногопринципанравственностинеобходимостиотречениявто
времякакнравственныйобразжизнивпрактическихинтересахвсегочеловечестваэтимоннапомин
аетварваровэпохипереселениянародовварваровубивавшихизатемкаявшихсявэтомтакчтопокая
ниестановилосьтехническимпримеромрасчищавшимпутькновымубийствамтакжепоступалива
нгрозныйэтасделкассовестьюхарактернаярусскаячертадостаточнобесславениконечныйитогнр
авственнойборьбыдостоевскогопослеисступленнойборьбывоимяпримиренияпритязанийперви
чныхпозывовиндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткпо
дчинениюмирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскому
мелкодушномунационализмукчемуменеезначительныеумыпришлисгораздоменьшимиусилия
мичемонвэтомслабоеместобольшойличностидостоевскийупустилвозможностьстатьучителем
иосвободителемчеловечестваиприсоединилсяктюремщикамкультурабудущегонемногимбудет
емуобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатакую
неудачупомощипостиженияисилелюбвиклюдямемубылоткрытдругойапостольскийпутьслуже
ниянампредставляетсяотталкивающимрассматриваниедостоевскоговкачествегрешникаилипр
еступниканоэтоотталкиваниенедолжноосновыватьсянаобывательскойоценкепреступникавыяв
итьподлиннуюмотивациюпреступлениянедолгодляпреступникасущественныдвечертыбезгран
ичноесебялюбиеисильнаядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляих
проявленийявляетсябезлюбовностьнехваткаэмоциональнооценочногоотношениякчеловекуту
тсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотребностьвлюбвииег
оогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшуюемулюбитьипо
могатьтамгдеонимелбыправоненавидетьимститьнапримерпоотношениюкегопервойженеиеел
юбовникунотогдавозникаетвопросоткудаприходитсоблазнпричисленияядостоевскогокпреступ
никамответиззавыбораегосюжетовэтопреимущественнонасильникиубийцыэгоцентрическиех
арактерычтосвидетельствуетосуществованииитакихсклонностейвеговнутреннеммиреатакжеиз
занекоторыхфактовегожизнистрастиегоказартнымиграмможетбытьсексуальногорастлениянез
релойдевочкиисповедьэтопротиворечиеразрешаетсяследующимобразомсильнаядеструктивна
яустремленностьдостоевскогокотораямоглабысделатьегопреступникомбылавегожизнинаправ
ленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизнутриитакимобразомвыразила
сьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчертвыявляющихсяве
гораздражительностимучительстванетерпимостидажепоотношениюклюбимымлюдяматакжев
егоманереобращениясчитателемитаквмелочахонсадиствовневажномсадистпоотношениюкса
момусебеследовательномазохистиэтомягчайшийдобродушнейшийвсегдаготовыйпомочьчелов

еквсложнойличностидостоевскогомывыделилитрифактораодинколичественныйидвакачестве нныхегочрезвычайноповышеннуюаффективностьегоустремленностькперверзиикотораядолжн абылапривестиегоксадомазохизмуилисделатьпреступникомиегонеподдающееесяанализутворч ескоедарованиетакоесочетаниевполнемоглобысуществоватьибезневрозаведьбываютжестопро центныемазохистыбезналичияневрозовпосоотношениюсилпритязаниипервичныхпозывовипр отивоборствующихимторможенийприсоединяясюдавозможностисублимированиядостоевског овсеещеможнобылобыотнестикразрядуимпульсивныххарактеровноположениевещейзатемняе тсяналичиемневрозанеобязательногокакбылосказаноприданныхобстоятельствахновсежевозн икающеготемскореечемнасыщеннееосложнениеподлежащеесостороныческогояпреодо лениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтоонопритойпопыткепоплатилосьс воимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназывалсебясамидруги етакжесчиталиегоэпилептикомнатомосновании чтоонбылподвержентяжелымприпадкамсопро вождавшимисяпотерейсознаниясудорогамиипоследующимупадочнымнастроениемвесьмавер оятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневрозакоторыйвтакомслучаесл едуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполнойувере нностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпадковтакназыва емойэпилепсиидостоевскогонедостаточныиненадежныавовторыхпотомучтопониманиесвязан ныхсэпилептоиднымиприпадкамиболезненныхсостоянийостаетсянеясныма

Висновки: Набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанували прийоми роботи в модулярній арифметиці.