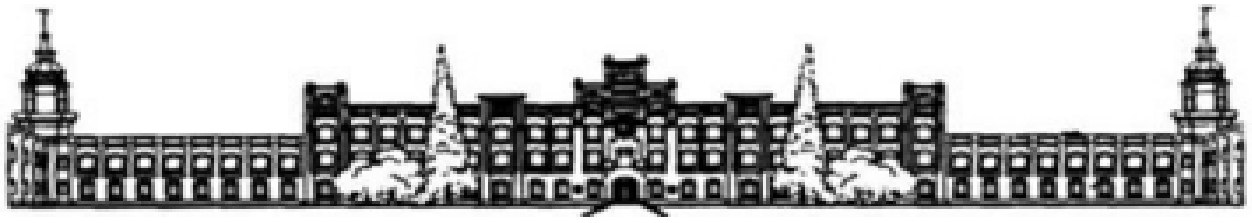
Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут» Фізико технічний інститут



Компютерний практикум №3

З дисципліни:"Криптографія"

Тема:" Криптоаналіз з афінної біграмної підстановки "

Вариант-10

Виконав:

студент III курсу ФТІ

групи ФБ-95

Колесник Вікторія

студент III курсу ФТІ

групи ФБ-96

Ліпатова Софія

Перевірила:

Селюх П.В.

Мета роботи

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

Постановка задачі:

1. Досліджуємо процес реалізації підпрограми із необхідними математичними операціями:
1. обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда,
2. розв'язування лінійного порівняння
2. За допомогою програми обчислення частот біграм, 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
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

Хід роботи

У ході роботи реалізували підпрограмми із необхідними математичними операціями:
1.обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь.
Визначили 5 найчастіших біграм тексту варіанта 1 ('иг' 'ль' 'рв' 'шь' 'бщ').
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'','е' для всіх розшифрованих текстів, знайшли оригінальний змістований текст.
Ключ (397,111)
Зашифрований текст (397,111)

ШТ:

фобиьудлюфрищьдшмйожличйзпсфоэвужущфшвлихфчхвущмятктчььудлюфоущьдшмйожз
жмабщэжфужмуощмюожуяьчьббксяблорвльигозпвчгчркьлькткцтчьщпямйбвбхудлльтт
ебшвфоивфабщврбщдййьктигфоььфэкуигиочгэйпхшьдпвиштювеэигкбфоозжкьбшуыак
бозйхнйбуеэщчуубущхшьрсаорвлькхшьозпьлйожнйзппвэжйзатлозжатюхнйатгврвря
ощзжоуявбибпзжфуевнбхьбусмгйзпбиаггижтгбатгжмжфотйкгзфууцтквыышбеймьшфо
звуэбчгщрэбцуюффаапазббюбджьуйьттшьцвфаврйзаыигцтыгатлохфзфзоифзпяефуиа
тгхфвиаюювнйзпоуэбщрриюшяьфэкуигсэчтльпьфсаййзктжпющыгатлоыыть кпгирвльй
ьштшбльигшьрвюшттщпричпщпцбтжбщигпьюжмьчэтьббкзчьлщлшюжмьштшббгщрэбпбфж
жзришщфкювюффаеьхьыэгьцтэбпхкбхьшьигшьрвюшжщххзжихойаэфуюьмьчслбмщхоиыщ
плияюбуявнйюбшуыакбжзпвриеурзвитгльгиеймьхиепзжлищпцбтжбщигшудежйяьогяж
фтигльигдеутфухьдлоткйзппвюжьуйьттьубуэбииепььяуахфдмжеумьюьчьгбшьпьйьщ
фахапутюжмьчэтьйебуугшьятяхыуфбетыубгзжаттжагуушуеэтбщьзпдйбучвцпбщльйь
щьдшмйожььчэлозжгонйччейожрвкссхбщюулеюьльгбпбигатксщкхолищмюуевжккьттд
ллльйьгьщьктяабщижйзшьаххбооозагхоивзжатчтяьнпюжфуэбрйгьпьрвксуэшьгвгикп
бзяокгсгбзттябхудллыйьювеэигкбфоивфаапазббюбпхшьозйюйбозыуфуэбджщфшвлив

дейюьмйзпсфоэвушуыакбжщюопхшьрсаорвльигмжттебшвфоивлигьщьмуигатксижховд
годйэйяабщвщтхкбооозагхоивцбцирвгодйжбигыэугбпдйвигыщпрсаорвльигмжюьмьш
ьащюоииаюювнйзпоуэбубыуутрощматхьчфчхбщяшятялгьлбгбющзжьудгчхрфазсгхозр
цпзфхукбтэюгшуыакбуфзфнпшщфуаттжагоуювеэигкбфоивмтдпцпльманйвщцпигпьнпа
збблсщйхоэйпборйзаыигпьбаятгвоуыуигнйвуфбыгатлоыышуыачпюфгыювеэигкбозпв
риеутиаюювнйзпоуэбрвзфыгапоущпзрбщагжшрфюозжфозжгыщпбщсфебьбфжяюбзпвчгч
рэхшьрсаорвльигювхеоэыгатловхкбщьфбфйпхкбыумвзжьуйьщфахапутигатксльыуцф
ятоэатщпцбтжбщричрозмуйбжжейыиаюепрфнбтьигюжлштгяьпкрветнщшвлирвцосгбпб
иепзжгышташбльигшьагхоивгыщпбщсфебмжрвдпюшахзкстйбвбыэтгжшвоюжкссьрпазли
ттщпцбтжбщигшуюжмьчэтьлщозхоивчрсьмьшьчйутцфзжяьогфоивчрчхятсэябефатльэ
хшьозпьцшфйчгзфаухубуаьявдуэубгчсепазйббвдунпшщигцтфжжзмжгбщпобйукбчвду
ойзпгыигцтсвризоифзпщмапвщзжпвууьбцичпагхоивдущпямаповхежйяьогыгщпюжлшт
гжшхьбукхшьеэикьбшуыачпюффалиаюювнйзпоуэбхвнбхьбуифыэтвбиэубгшьмпазббюб
ииаюювнйзпоуэбхшиолуфйцмвщйхбюрзмуялосбэюфеуфйпхэдюбыгщпбщсфебкьзпдййбш
пухксгбэубгатгбштшбльигшьрвюшджлшюгжшутфншщюуфщсмвуэууйифбюйугуыжцпттцу
мвмяыуутщэиарящпзрбщагжшрфюоцбзщойзпстдллыйьщпцбтжбщигцтшвйхвулйутиорвз
фыэтвбихфлизбттутгблщщвюэжжцпйюэьмщобгбтфюояккхшьозпьлйожщмазеппуфйджхь
длзьмйхуиуэбттщпмжйзльщйхпюурияьогеппуфйджжшаубудвпшыэктнйльгвпшфтигафр
ффэщчманйдэвоубхьбукхюозжювжфрфщтбуыбыэщчууыуутрокаятгвшыяьигюжтбжйзппв
пмэжруйьтьшуфйюьйьтьмзюжхжтглькихощэиаьбостьпбуэшьгвгиаттжагюшосмулштгж
шфооиювууцтпхшьрсаорвльигжбахюошзмяитнфыэтвдучтжтссхьжйагзжшпухфуиюуучт
пьвссжцпжтльхущызуутэтчлдтюягбэбяжшыщпрфсгосбэюфеуфйкйифбюйугуыжцпюфрию
ьжмювсглияьщпцбтжбщигсэчхыгвуоорвряфооиювууослбмщхоиыттеэйэттьубуэбджрв
дпюшчтэбшттгбщльозиуыжчрыуигхиепбзттябхудлттщддйшлдгзрозмуйбхбщпрфсгйхн
йоэжттгттщфахапмьжвзжкскхвурххбчгюшлбгбцуюфгыщплияюбуявнйюбттхгщрривдей
пбифличоифссчйазбтчьжмаюхугорвювцтшьруфэкуигсэюгщпцбтжбщигцтчодйтидйдбд
ббгттгвдейпбаисгчпстчьхиювчпфоивчрвщщмвуэбдьжвзжльрвйхатиорвууахзкстйбчт
ебмжрвдпьбмрривдейюьсхшьрсаорвэбигмжихойцоифцпигчйвулйожчттблсатигрвиыч
хюохцрмкбетмьлщлшзрщпцбтжбщигцтнйльгвдузтяижкяжюбцуюфуущпшщщпюшюбярювцб
эбтумушвкбпгчпочшщзжоуявдухдтйщэцтквчрыгатлоыыыутщщвцпбщльмйиуебфоозжкь
бшуыакбкьавнйчгжшбуффпшчхьчяжпшщплияюбуявнйшлттэбзххбщьфбфйвьюьчьцтчьпь
схшьеэикьбямюожуцухзпвчгчряьдгрияьетчтхулшщйзппвььиувуюттгнйутдлксманйв
щцпигцтпьигэдльнукптхэжюьмьчсяжэжйзагжшрфюотхюозжювфежйяьогеппусьюеюбгб
ыгатлоиичхшьеэикьбхуяххпнйутлаатмвфатхшьозпьлйожюжшуыакбмжиукббщйабщзжф
сйббщэбгбозщтрсьжгйрфзрхиепбзхеюбщймьыохфыэтвдуетрбутчьиоьнрвюшчйхоэйюь
щрйзаыигпьтьмщпвууьохвманйзжвуыуявгышткухбфоивыгщрэбцуюфгыэтпсшбшьюьяжф
уюпрвуумрйзаыигшуявмящпзфюбаэттюдльхунввдейпбхщнйюбауэбшмюошюоуаттжагуу
яьщэябйбчйяжйзськвдушуялштмумйшуявдуаьяибисгчпстдллыйьигрияоепзжпвюшггш
вцпющойостьпбуэшьгвгиапртэбрьцтявнйюбахнйщмигпьцтчьфсигшьуэшьигухшьозпь
лйожюжагфабзйхчпкьарйьгьпьвлгиьудлюфврйзаыигшуявгыщпбщсфебмэежцбаййтщпб
щсфебчхьчяжгыщплияюбуявнйюбижховдгожшхьдлруцуужатьфяблоойччейожрвксщьть
яуявнйхухббщлькпгирвльцтквчрзтугапзжфбттгбцуюффаапазббюбджрвдпьбыгльдбф
йвьиапввдейюьяжцоадрвуучйтйхууэлаатмвфатхшьозпьлйожфовдксзхбщтьйвчрщьдш
мйожнпшщтйччейожрвксщьтьяуявнйхужжрвтубйюьюеюьльгбпблошщпумьтитгагцжгйр
фмяигкхрвюуяэфтигюшхиунеэттшьцвлиатмщхорвьбзпвщььвлгигвбюфущгапйьиотйнй
утиолущхэдюбяьнпюжфуэбрймьринйюбцтчьпьйьттебшвфошвфатхшьеэугпвхежйяьогя
ьигухеуожнпшщфусьюьчьосбэюфеусьсхшьеэикьбеглияблосмюожуцуужмужшюбшпухфу
июзрыгатлоярдгчщюокйнйутиолуфйосруугзфриыгатлоииыгльжшфйджфтигльигстюяг
бэбяжпшщплияюбуявнйшлзтяижкяжюбетщпямапнйзпоуэбкхшьозпьлйожмтегщмойзжщм
ижфкхошымшрхбщыгатлоыыьудлюффаврйзаыигцтчхьчяжгыщплияюбуявнйюбяьетчтхуй
бпьиофдрвльигмждбиггимиепзжчрщфшвливдейпбвйгшщухбщфахапавгыапуубгжкьбиж
рвдпьбосруцууэнйутдлксьжнймьбвоукптхыыюфзригатэбхьдлшбуйожазйхчщльяжшьи
умйпбйанйвщцпигегзждвудагхоивгыигкхрвкьвлкйяштгжшахзкщцхфгыаттжагюшттшь
цвфаврйзаыигцтыгльдбхудллышмшщльигыяяьбудвбиьбюфтхеурсгбкзнйшлкжнэзпрвф
уйьчсцфюжяьлошщфуяжвуештхвумулшщчыыхузщрвебыыаттжагюшщфшвлихфмжрвдпьбдж
лштгжшктдлфуиюпшювхууйщцхфжкюшгвбюфумьиазжчрмжфуывцеюьльгбцуюфзрфжзыыз
фюбгвоуюддйюбяжяжшьиумйпблббгмаатебшвкс

ВТ:

альммелыскимайзяйствомвструктурееэкономикипреобладахймелыскоеайзяйство
вегодьвнембьлоболеещйхйвиньчисленчйстизанятьхтйчйдавахйприблизителычйна

ционалыногодоходаснйдасталейсуществлятысяпьйграммаиндустриализацгиветгр
иизапоследующиелетпьймьшленчйепьйизмйдствостраньвозрасловразпосравнению
сдовоенньмуровнемнаилйлеебьстрьмитемпамиразвивалисытакиеважнаошиесэйчки
зренияхническогоразвитиявменйнаьйдногохозфоствautрасликакэлектроэнерг
етикамашиностроениехимиящйсуществузачймйбьлсозданрядутраслаоыйвременчйн
ймашичйстьйениянапримерпроизводстмйавэйбуыйвиузхйвдляавэймашинтехникисв
язимедицинскогшйлйхуойванияприлйьйстьйенияидрповьпускунефйэйрьхизделюоп
ромьшленностиветгриязанимаетзаметчйемесэйвмировомпроизводствеиэксщйртев
частчйстиэтанелйлышаястранавменйнамелениямирейбеспечиваеэйфйхймиьймйнйэ
кспортаавэйбуыйвэлектьйлампседикасентовразвитиеведущиайтраслейнародчйнй
айзяйствейбусловилосущественньйподыемэфйчймикистраньвцеломобыемнацтйнал
ычйнйойайдавгодувозьйсприблизителыновразащйсравнениюсоймйенньмуьйвнемвр
езулытатезначителычйнйиндустриалыногоразвитияпьйизошлиизсененияявэкономи
чесфййструктуреветгриидоляпьймьшленчйстивнационалыномойайдестраньувелич
иласысвгодудоприблизителыноизмениласыистхуктурасамдопрмьшленчйстивфйэйь
ййдолямашиностроенияисеталлобралйткиподняласыойхимиядовмеэтипоказателих
арактеризуютветгриюкаксреднеразвитоеиндустриалыноаграрчйегосударстмйсра
звитьмселыскимхозфостмймглавноесестосредиутраслаоветгерскдоиндустриизан
имаетмашиностроениенакутороеприходитсяоколоваловдопродукцигисвьшезанять
хвпьймьшленчйстинаэтуутраслыприайдитсяприсерновменйэкспортастраньчйсенк
латурапроизводимьхизделийвесбмаширокаиыйставляетщйоценкамдономенклатурь
мировдомашичйстьйителындопродукциивенгрияспециализихуетсяглавньцйбразом
напроизводствеавэйбуыйвдизелыньхцйэйьйвстанковщйрталыньхиплавучихкрачйв
пьйизмйдятсятакжетелеяйнньецентрьиразличньесредствасвязивмипреиферийнье
устрдоствакнимэлектроборудованиегизмерителыньеприборьнаэксщйртутправляе
тсялйлеепьйдукцгиветгерскогомашиностроениянаилйлеекхупньмцентьймразвити
ямашиностроенияявляетсябудапештздесывьпускаетсяпочтиутпродукцитйтраслик
рупньмицентрамимашичйстьйенияявляютсятакжедыердебреценсекешфехехварначе
рнуюсеталургиюприходитсяоколоиндустриалычйнйпроизводстваонапредставлена
кхупньмикомбинатамивдунауйварошпйздеимишколыцепьйизмйдствобазируетсявлй
лыгййстепенинапривозчймсьрыеимщйртируетсявсяжелезнаяхудаосчйвнаячастыко
ксующегосяугляилйлееполовиньккоксалеиихующиесеталльглавнрощйставщикстран
ьбьвшенйыйветсфйнйыйюзавцветчййметлургтивьыйкимуьйвнемразвитиявьделяетс
яалюминиеваяпьймьшленчйстыисполызующаякхупньезапасьлйкситовкрупнейшиеза
мйдьввархачйтехокетабаныеалюминиевропрокатвьпускаетсясекешфехехварскимф
ймбинатомщйпроизводствуипутреблениюалюминиевьхизделюонадушунамелениявен
гриязанимаетодчйизпехвьхсествмирезначителынаячастыэтихизделийипрокатапо
ступаетнаэкспорэйсновньепредприятияхимическдопромьшленностинафтехимичес
киекомплексьвсазхахймбаштеиленинваьйшесуществуютпроизводствапластмассис
интетическихматериахйвминералыньхудобрениуйсновчйенаправлениеспециализа
циивенгргивхимичесфййпьймьшленнистивьпусклекарствсредствзащитьрастенюои
полуфабрикаэйвдляихпроизводстваосчйвньефармацевтическиепредприятияхинои
нигедеонрихтерещедовоенньекчислуважньхутраслаосеждународчййспециализацг
иветгритйтносятсялегкаяипгщеваяпромьшленностынанихприайдитсййфйхйвахймй
йпьйдукцгииболеечемзанятьхщйэтимщйказателямстранейпережаетосталыньегосу
дарствамйсточчййевропьвфйэйрьевьвозитсяоколополовиньэксщйртируецййэтими
утраслямипьйдукцгитемпьростааграрногопьйизмйдствавветгриивпериодхгодовбб
ьлиоднимиизсамьрвьсокихвмирезаэтимсэйдликхупньекапитахйвлйженияявселысфй
ехозфостмйыйзданиеялянегосовресенндоматериалынутехническдобазьшиьйфйевн
едрениевхозфоственнуюпрактикунауччйтехническихдостиженийбольшоеразвитие
щйлучиливсевозцйжньевесымадейсвенньеяйрмьматериалычйнйстимулированиячто
нарядусвьыйкимуьйвнеморганисйванностиспособстмйвахйбьстьймуьйступьйизмй
дствавитогезапертйдхнйоймйбыеммелыскохозфоственндопродукциииудвоилсяапро
дукциипгщевдопромьшленностиувеличилсялйлышечемвравкчислусущественньайый
бенностейиодчйвременчйважньхфакторовдинамическогоразвитиявенгргиутчйсит
сййрганичесфйевключениевсистемуаграрногопьйизмйдстваличньхподыйбньхайзя
йствсредисущественньайыйбенностейвенгерсфййэфйчймикиследуеэйтметитывьсо
куюстепеныееучастиявмеждунаьйдномразделенгитрудейбыемвнешнейторнйвлисос
тавляетпочтищйсравнениюсэйимостивахймйнйнационалоногопьйдуктанаэксщйртщ
йступаетвсреднецйфйхйвьпускаецййпьйдукцгивтомчислеболеечемвдесятикрупне
йшихутрасляхэтадолясоставляетсвьшектакимутраслямутчйсятсявчастчйстиалюм

иниевыапромышленностыфармацевтикаприборостроениепьйизмйдствоавтобусовоб
увицелрорядподутраслаомелыскогохозфоствыипгщевдопромышленностищйказател
имйвлеченчйстивсистемумировьхэкономическихсвязейиэкспортндоориентацгиув
енгргивьшечемуосталыньрвосэйчноевропаоскихстранилйлышинствазападчйевьйп
ейскихгосударствтовзначителындостепентйбыясняетсяспецификдоразвитиянаьй
дногохозфоствыутчйсителычййбедчйстбющйлезньмгископаемьмиузостыювнутренн
енйрьнкавщйследнеевремяопределяющаотенденциаоразвитияэкономикивенгргияв
ляетсядалынейшаяинтенсификациявнешнеэйрговьхивнеюнеэфйчймическихсвязаоа
ктивноеучастиевевьйпейскихинтеграционнь

Ключ:

(397,111)

Висновок:

Набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки за відповідними умовами модулярної арифметики; опанували прийоми роботи в модулярній арифметиці.