Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:
Студенти ФБ-01
Сотнікова П.О.
Струкало В.В.

Київ – 2022

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.

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.

----------Зашифрований текст----------

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцп
воыомхзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрб
чэшжцюлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибуххйзюжмьгнхщюзншбхюэотйбаво
тдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшух
эозоихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушю
стлхэдвоэомюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкц
хнцхеоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстудвежюнхэджядшищвччо
щщвунойхзозпцэфтмефпшхтдпощщщыкдвуозеойбдээзстсдоожмиврбгхнойхзозпцэцэфпэт
щощюэоеохсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбуххйэыбдтджюзнхы
охнхлхыбэлфошхэдохехвоубпзшбчхлыйбсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэт
вцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмшшзцтйищцюеокцфпжюэд
дйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуод
дйучяожстднтжхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойб
щеьжкхшцжосбанолхжжоойераннбйейсвцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээы
кояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншшвуйжышьтджфицхеогбшшанжхтдпнягво
фихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщ
яоыбэлгтфдэйетзэстйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбво
тдьздйирэттднттющсзйэысесдвейхаирбтюзсжжйбщддццнтдэййбюгрбтдтхыбгцэюболхсд
жькдрбнхцщйеэотддншддцбаабжукцеочтйхвюеыдйрббдфхдйыжхшшшщаышиткчсняощщуогб
ажбфьащелбхшзцтйищцюнхктсдждайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйотгрб
арбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшц
абдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбвотдбнкдютрртхтдетмыпюнозоуюмх
эшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщтокшеронцчшццнджфитджюкцтйвм
щыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстй
рбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжх
пбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхбжйуолэттднттюзсзтсб
шшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокоянщдкцмеввнмжхетжютдхшкдысбхьн
элжхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщю
мхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстд
нбансюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсурржц
зожюдюяюэоддтххгнхщюжбзнкофтждцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухвц
щоыояоетктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдш
шшухсугждннььгррщюцйюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдш
жуьжгажюпннъхыохзйзцвоьыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшс
ажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвххйсудйхюххыокйзювнфирбюлчозтлхтбйб
ьзньйбйужькюдурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфм

эощняюабгххсййбргшзцтйищцюжхинфиывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжц
чэмюсуажандйщеябруеыохпыыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкб
ьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлш
жьгцвужхщююютнобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуол
сылжэыпюшбхфньхытцодгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвм
нищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцчшццнйиеы
анвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщо
цщанкдьгнхтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгх
ооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгц
итцпвохсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончх
шхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцп
тдтхнгкцеоубхфкцтхшммыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщю
этсдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкцжхыболиндйчетдажгцситцэюмх
эшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбр
щюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрб
гхшсшпцэкдлттдкгрбвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгх
жючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднттюхлдшшшитщостжошсзхтдьжрбгхмю
лбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощ
йекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуо
фюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржу
тзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдвеатлцпнчэсклхшхэджу
дэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсшт
ввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвц
щохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпоойерягррщюкэин
нисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюбпокй
фигжщддцлххсввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэо
чоьбгцфпчочобоацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскооыокдютждкдрт
нтфддйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбрущоьыйбрбитшхыошсзхтдстнтыбюл
пюьыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньщечощщвуйоюс
зхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощцсиюасцитфпкдьоицжу
вундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйх
бхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсесдверианлххнэйрбгхыянбитйюсу
югэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцситцэюмх
эшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияжьз
вотдучяоехфдвукдюткйтцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйче
востююхцяхщюкоушнбднеокоацяхжхитсюююйянбэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэс
цркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьюьвортнтфддйкдютгцитсд
вейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтц
фпйотдухвцщоыощощщюггжнбгххудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэ
йхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбйщтцпвотдучвцйудйпрэвщдшд
эыдйут

Ключ: a = 199, b = 700

----------Дешифрований текст----------
отцеубийствокакизвестноосновноеиизначалыноягрестнглениечеловечестваиотделы
ноцочеловекавовсякомслучаеонфплавньйисточникчувствавиньнеизвестноединствен
ньйлиисследованиямнеудалосыещеустановитыдушевноепроисхыждениевиньипотребно
стиискнгленияноотнюдынесщественноединствебньйлиэтоисточнидгсихологическое
положениесложноинуждаетсявобясненияхотношениемалычикакоткукакмвповоримамби
валентнопомимоненавистииззакоторойхотелосыбьотцакаксигерникаустранитысщес
твуетобьчноншкотораядолянежностикнемуобаотношениясливаютсявидентификациюсо
тцомхотелосыбьзанятыместоотцщготомучтоонвьзьваетвосхищениехотелосыббьтыка
конипотомучтохочетсялпоустранитывсеэтонаталкиваетсянакрупноепрягятствиевиг
ределебньймоментребенокначинаемгониматычтопопьткаустранитыотцакаксигерника
встретилабьсостороньотцанаказаниечерезкастрациюизстрахакастрациитоестывинт
ересахсовранениясвоеймужественностиребенокотказьваетсяотжеланияобладатымат
ерьюиотустраненияотцщгосколыцуэтыжеланиеостаетсявобластибессознателыноцоон
ояоляетсяосновойдляобразованиячувствавиньнамкажетсячтомьигисалинормалыньяг
роцессьобьчнуюсудыбутакназьваемоцоэдвговакомплшкюаследуетоднаковнестиважно
едигвлнениевозникаютдалынейшиеосложненияеслиуребенкасилынеразвитконституц

иобньйфакторназьваемьйнамибиеексуалыностыютогдщгодщпрозогготеримужественно
стфчерезкастрациюукрягляетсятенденцияуклонитысявсторонуженствебностиболеет
фпотенденцияпоставитысебянаместоматеривгеренятыеервлыкакобшкталюбвиотцаодн
алишзбоязныкастрациииделаетэтуразвязкуневозможнойребенодгонимаетчтоондолжен
взятынасебяикастрированисеслионхочетбьтылюбимьмотцомкакженжинатакобршкаютс
янавьтеснениеобапорьваненавистыкоткуивлюбленностывотцаизвестнашгсихологиче
скаяразницаусматриваетсявтомчтоотненавистикотцуотказьваютсявследствиестрах
щгередвнешнейопасностыюкастрациейвлюбленностожевотцаволгринимаетсякаквнутр
енняяопасностыпеэвфчноцопозьвакоторашгосутисвоейсновавозхращаетсяктойжевне
шнейигасностистрахпередотцамделаетненавистыкоткунеприемлемойкастрацияужасн
акаквкачествшкарьтакиценьлюбвиизобоихфакторовввьтесняющихненавистыкоткупеэв
ьйнепосредствебньйстрахнаказанияикастрациисследуетназватынормалыньмпатогени
ческоеусилениепривноситсякаккажетсялишыдругиафакторомбоязныюженственнойуст
ановкиярковьражебнаябиеексуалынаясклонностыстановитсятакимобразомоднимизус
ловийилиподтвержденийневрозаэтусклонностыочевидноследуетпризнатыиудостоевс
коцоионалатентнаепомосшксуалыностыпрояоляетсявдозввленномвидевтомзначениик
акоеимелавлпыжизнидружбасмужчинамивецодострабностинежномотношенииксоперник
амолюбвиивлпигрекраснотгониманииположенийобяснимьхлишывьтесненноппомосшксу
алыностыюкакнаэтоуказьваютмнфпочислебньепримерьизецопроизведенийсожалеюнон
фчлпонемфпуизменитыеелвгодронностионенавистиилюбвикотцуиобихвидоизменениях
подвлияниемугрозькастрациинесведзщемувпсихоанализечитателюпокажутсябезвкус
ньмиималовероятньмвгреюгвлжпаючтоимебнокомплшкскастрациибудетотклоненсилын
севслпоносмеюуверитычтигсихоаналитфческийопьтставитимебноэтиявленияявневсяк
фпосомненияинаходитвнихключклюбомунехрозуилгьтаемжсецовслучаетакназьваемой
цгилягсиинашлпигисателянонашемусознаниютакчуждьтеяоленияволастикоторьхнах
одитсянашабессознателынашгсихическаящизныуказабньмвьшенеисчекгьваютсявэдвг
овомкотглексягоследствиявьтесненияненавистикоткуновьмяоляетсяточтовконцеко
нцовотыждестолениесотцомзавоевьваетвнашемяпостоябноеместоэтоотыждестоление
волгринимаетсянашимянопредставляетсобойвнемособуюинстанциюпротивостоящуюос
талыномусодержаниюнашецоямьназьваемтфпдаэтуинстанциюнашимсверхяипрвгисьвае
мейнаследницеродителыскоцоолияниянаиважнейшиефункцииеслиотецбьчсуровнасилы
ственжестокнашесверхшгеренимаетотнлпоэтикачестваивлпоотношениикясновавозни
каетпассивностыкоторойкакразнадлежалобьбьтывьтеснебнойсверхясталосадистиче
скимястановитсямазохистскимтоестывосновесвоейженствебнигассивньмвнашемявоз
никаетболышашготренностывнаказанииияотчастиотдаетсебякактаковоевралгоряжен
иесудыбьотчастиженаходитудовлетворениевжестокомобращенииснимсверхясознание
виньказдаякараявляетсяведывосновесвоейкастрациейикактаковаяосуществолениеми
значалынфпигассивнфпоотношениякотцуисудыбавконцеконцовлишыдалынейшаяпроекц
ияотцанормалыньеявленишгроисходяжиягриформированиисовестидвлжнхгоходитынао
пиюабньездесыанормалыньенамещенеудалосыустановитыразгранфчениямеждунимизам
ечаетсячтонаибвлышаяролыздесывконечномитфпягрипись ваетсяпассивньмэлементам
вьтесненнойженствебностиищекакслучайньйфакторимсетзначениеяоляетсяливнуша
ющийстрахотецивдействителыностиособебнонасилыственньмэтоотносится кдостоевс
комуфактлпоисключителыноцочувствавиньравнокакимазохистскфпообразажизнимьсв
одимкецоособенноярковьражебномукомпонентуженствебностидостоевскоцоможноопр
еделитысследующимобразомособебносилынаябиеексуалынашгредрасположебностыиспо
сонностысособойсилойзажищатысяотзависимостиотчрезвьчайносуровоцоотцаэтотха
рактербиеексуалыностимпдобавляемкрансеузнабньмкотгонентамецосуществарабний
ситгтотгрипадковсмертиможнорассматриватыкакотождествлениесволпоясотцомдопу
щебноевкачественаказанияссторонысверхятьзахотелубитыотцадабьстатыотгомсам
омутягерытьотецноотецмертвьйобьчньймеханизмистерфческихсимптомовиктомужете
перытебяубиваетотецдлянашецоясимптомсмертиявляетсяудовлетворениеафантазиим
ужскфпыжеланияиодновремебномазохистскитгосредствомнаказаниятоестысадистиче
скимудовлетворениемобаяисверхяопраютролыотцаидалышевобщемотношениемеждулфч
ностыюиобектомотцаприсохранениицосодержанияперешловотношениемеждуяисверхя
новаяинсценировканавторойсценетакиеинфантилыньереакцииэдвговакомплшкюамогу
тзжплохнутыеслидействителыностынедаетимвдалынейшемпижинохарактеротцаостает
сятемжесамьмнетонухудшаетсясцодамитакимобразомпродлжаетоставатысяиненавис
тыдостоевскоцокотцужеланиесмертиэтомузломуоткустановитсяигасньмеслитакиевь
тесненньежеланияосзществляютсянаделефантазиясталареалыностыювсемерьзащитьт
ягерыа

Висновки:

У даній лабораторній роботі ми працювали з частотним аналізом розкриття моноалфавітної підстановки. Також опановували навички в модулярній арифметиці