СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконала:

Студентка групи ФІ-93

Ємець Єлизавета

**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.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп’ютерного практикуму No1, знайти 5 найчастіших біграм запропонованого шифротексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифротексту (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 шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5 .Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

Варіант завдання:

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоыомхзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщюзншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозоихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдвоэомюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстудвежюнхэджядшищвччощщвунойхзозпцэфтмефпшхтдпощщщыкдвуозеойбдэзэстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлыйбсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмшшзцтйищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднтжхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншшвуйжышьтджфицхеогбшшанжхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэстйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесдвейхаирбтюзсжжйбщддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотдднщддцбаабжукцеочтйхвюеыдйрббдфхдйыжхшшшщаышиткчсняощщуогбажбфьащелбхшзцтйищцюнхктсдждайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбвотдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщтокшеронцчшццнджфитджюкцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхетжютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтжджцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухвцщоыояоетктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждннььгррщюцйюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоьыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькюдурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсййбргшзцтйищцюжхинфиывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужхщюююетнобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхытцодгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцчшццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшммыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкцжхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднттюхлдшшшитщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдвеатлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсштввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэочоьбгцфпчочобоацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбрущоьыйбрбитшхыошсзхтдстнтыбюлпюьыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньщечощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпкдьоицжувундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсесдверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцситцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияжьзвотдучяоехфдвукдюткйтцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюкоушнбднеокоацяхжхитсюоюйянбэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфддйкдютгцитсдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюггжнбгхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбйщтцпвотдучвцйудйпрэвщдшдэыдйут

Можливі ключі:

(249:329) (377:329) (235:329) (404:329) (712:80) (128:80) (947:80) (155:63) (584:913) (833:913) (819:913) (27:913) (726:94) (14:94) (142:94) (169:94) (557:886) (806:63) (934:886) (792:886) (249:869) (377:869) (235:869) (404:869) (712:620) (128:620) (947:620) (155:603) (584:492) (833:492)(819:492) (27:492) (726:634) (14:634) (142:634) (169:634) (557:465) (806:603) (934:465) (792:465) (712:869) (584:869) (726:869) (557:869) (249:620) (833:620) (14:620) (806:603) (377:492) (128:492) (142:492) (934:492) (235:634) (947:634) (819:634) (792:634) (404:465) (155:603) (27:465) (169:465) (712:636) (584:636) (726:636) (557:636) (249:387) (833:387) (14:387) (806:370) (377:259) (128:259) (142:259) (934:259) (235:401) (947:401) (819:401) (792:401) (404:232) (155:370) (27:232) (169:232) (712:636) (584:636) (726:636) (557:636) (249:387) (833:387) (14:387) (806:370) (377:259) (128:259) (142:259) (934:259) (235:401) (947:401) (819:401) (792:401) (404:232) (155:370) (27:232) (169:232) (712:636) (584:636) (726:636) (557:636) (249:387) (833:387) (14:387) (806:370) (377:259) (128:259) (142:259) (934:259) (235:401) (947:401) (819:401) (792:401) (404:232) (155:370) (27:232) (169:232) (249:5) (377:5) (235:5) (404:5) (712:717) (128:717) (947:717) (155:700) 584:589) (833:589) (819:589) (27:589) (726:731) (14:731) (142:731) (169:731) (557:562) (806:700) (934:562) (792:562) (249:5) (377:5) (235:5) (404:5) (712:717) (128:717) (947:717) (155:700) (199:700) (584:589) (833:589) (819:589) (27:589) (726:731) (14:731) (142:731) (169:731) (557:562) (806:700) (934:562) (792:562) (712:5) (584:5) (726:5) (557:5) (249:717) (833:717) (14:717) (806:700) (377:589) (128:589) (142:589) (934:589) (235:731) (947:731) (819:731) (792:731) (404:562) (155:700) (27:562) (169:562) (249:5) (377:5) (235:5) (404:5) (712:717) (128:717) (947:717) (155:700) (584:589) (833:589) (819:589) (27:589) (726:731) (14:731) (142:731) (169:731) (557:562) (806:700) (934:562) (792:562)

Наш ключ:

(199:700)

Розшифрований текст:

отцеубийствокакизвестноосновноеиизначалыноягрестнглениечеловечестваиотделыноцочеловекавовсякомслучаеонфплавньйисточникчувствавиньнеизвестноединственньйлиисследованиямнеудалосыещеустановитыдушевноепроисхыждениевиньипотребностиискнгленияноотнюдынесзщественноединствебньйлиэтоисточнидгсихологическоеположениесложноинуждаетсявобясненияхотношениемалычикакоткукакмвповоримамбивалентнопомимоненавистииззакоторойхотелосыбьотцакаксигерникаустранитысзществуетобьчноншкотораядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосыбьзанятыместоотцщготомучтоонвьзьваетвосхищениехотелосыбьбьтыкаконипотомучтохочетсялпоустранитывсеэтонаталкиваетсянакрупноепрягятствиевигределебньймоментребенокначинаемгониматычтопопьткаустранитыотцакаксигерникавстретилабьсостороньотцанаказаниечерезкастрациюизстрахакастрациитоестывинтересахсовранениясвоеймужественностиребенокотказьваетсяотжеланияобладатыматерыюиотустраненияотцщгосколыцуэтыжеланиеостаетсявобластибессознателыноцоонояоляетсяосновойдляобразованиячувствавиньнамкажетсячтомьигисалинормалыньягроцессьобьчнуюсудыбутакназьваемоцоэдвговакомплшкюаследуетоднаковнестиважноедигвлнениевозникаютдалынейшиеосложненияеслиуребенкасилынееразвитконституциобньйфакторназьваемьйнамибиеексуалыностыютогдщгодщпрозогготеримужественностфчерезкастрациюукрягляетсятенденцияуклонитысявсторонуженствебностиболеетфпотенденцияпоставитысебянаместоматеривгеренятыеервлыкакобшкталюбвиотцаодналишзбоязныкастрацииделаетэтуразвязкуневозможнойребенодгонимаетчтоондолженвзятынасебяикастрированисеслионхочетбьтылюбимьмотцомкакженжинатакобршкаютсянавьтеснениеобапорьваненавистыкоткуивлюбленностывотцаизвестнашгсихологическаяразницаусматриваетсявтомчтоотненавистикотцуотказьваютсявследствиестрахщгередвнешнейопасностыюкастрациейвлюбленностожевотцаволгринимаетсякаквнутренняяопасностыпеэвфчноцопозьвакоторашгосутисвоейсновавозхращаетсяктойжевнешнейигасностистрахпередотцамделаетненавистыкоткунеприемлемойкастрацияужаснакаквкачествшкарьтакиценьлюбвиизобоихфактороввьтесняющихненавистыкоткупеэвьйнепосредствебньйстрахнаказанияикастрацииследуетназватынормалыньмпатогеническоеусилениепривноситсякаккажетсялишыдругиафакторомбоязныюженственнойустановкиярковьражебнаябиеексуалынаясклонностыстановитсятакимобразомоднимизусловийилиподтвержденийневрозаэтусклонностыочевидноследуетпризнатыиудостоевскоцоионалатентнаепомосшксуалыностыпрояоляетсявдозввленномвидевтомзначениикакоеимелавлпыжизнидружбасмужчинамивецодострабностинежномотношенииксоперникамолюбвиивлпигрекраснотгониманииположенийобяснимьхлишывьтесненноппомосшксуалыностыюкакнаэтоуказьваютмнфпочислебньепримерьизецопроизведенийсожалеюнонфчлпонемфпуизменитыеелвгодронностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозькастрациинесведзщемувпсихоанализечитателюпокажутсябезвкусньмиималовероятньмвгреюгвлжпаючтоимебнокомплшкскастрациибудетотклоненсилынсевслпоносмеюуверитычтигсихоаналитфческийопьтставитимебноэтиявлениявневсякфпосомненияинаходитвнихключклюбомунехрозуилгьтаемжсецовслучаетакназьваемойцгилягсиинашлпигисателянонашемусознаниютакчуждьтеяолениявооластикоторьхнаходитсянашабессознателынашгсихическаящизныуказабньмвьшенеисчекгьваютсявэдвговомкотглексягоследствиявьтесненияненавистикоткуновьмяоляетсяточтовконцеконцовотыждестолениесотцомзавоевьваетвнашемяпостоябноеместоэтоотыждестолениеволгринимаетсянашимянопредставляетсобойвнемособуюинстанциюпротивостоящуюосталыномусодержаниюнашецоямьназьваемтфпдаэтуинстанциюнашимсверхяипрвгисьваемейнаследницеродителыскоцоолияниянаиважнейшиефункцииеслиотецбьчсуровнасилыственжестокнашесверхшгеренимаетотнлпоэтикачестваивлпоотношениикясновавозникаетпассивностыкоторойкакразнадлежалобьбьтывьтеснебнойсверхясталосадистическимястановитсямазохистскимтоестывосновесвоейженствебнигассивньмвнашемявозникаетболышашготренностывнаказанииияотчастиотдаетсебякактаковоевралгоряжениесудыбьотчастиженаходитудовлетворениевжестокомобращенииснимсверхясознаниевинькаждаякараявляетсяведывосновесвоейкастрациейикактаковаяосущестолениемизначалынфпигассивнфпоотношениякотцуисудыбавконцеконцовлишыдалынейшаяпроекцияотцанормалыньеявленишгроисходяжиягриформированиисовестидвлжнхгоходитынаопиюабньездесыанормалыньенамещенеудалосыустановитыразгранфчениямеждунимизамечаетсячтонаибвлышаяролыздесывконечномитфпягриписьваетсяпассивньмэлементамвьтесненнойженствебностииещекакслучайньйфакторимсетзначениеяоляетсяливнушающийстрахотецивдействителыностиособебнонасилыственньмэтоотноситсякдостоевскомуфактлпоисключителыноцочувствавиньравнокакимазохистскфпообразажизнимьсводимкецоособенноярковьражебномукомпонентуженствебностидостоевскоцоможноопределитыследующимобразомособебносилынаябиеексуалынашгредрасположебностыиспосонностысособойсилойзажищатысяотзависимостиотчрезвьчайносуровоцоотцаэтотхарактербиеексуалыностимпдобавляемкрансеузнабньмкотгонентамецосуществарабнийситгтотгрипадковсмертиможнорассматриватыкакотождествлениесволпоясотцомдопущебноевкачественаказаниясостороньсверхятьзахотелубитыотцадабьстатыотгомсамомутягерытьотецноотецмертвьйобьчньймеханизмистерфческихсимптомовиктомужетеперытебяубиваетотецдлянашецоясимптомсмертиявляетсяудовлетворениеафантазиимужскфпыжеланияиодновремебномазохистскитгосредствомнаказаниятоестысадистическимудовлетворениемобаяисверхяопраютролыотцаидалышевобщемотношениемеждулфчностыюиобектомотцаприсохраненииецосодержанияперешловотношениемеждуяисверхяноваяинсценировканавторойсценетакиеинфантилыньереакцииэдвговакомплшкюамогутзжплохнутыеслидействителыностынедаетимвдалынейшемпижинохарактеротцаостаетсятемжесамьмнетонухудшаетсясцодамитакимобразомпродвлжаетоставатысяиненавистыдостоевскоцокотцужеланиесмертиэтомузломуоткустановитсяигасньмеслитакиевьтесненньежеланияосзществляютсянаделефантазиясталареалыностыювсемерьзащитьтягерыа

Найчастіші біграми ШТ:

ТД=78

РБ=54

ВО=52

ЩЮ=46

ЕТ=44