МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет України

«Київський політехнічний інститут»

Фізико-Технічний Інститут

Криптографія

Лабораторний практикум №3

Завдання варіанту №3

Виконали студенти групи ФБ-82

Дигас М.В

Кудрик Е.В

Перевірив:

Чорний О.М

Завдання:

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 №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:

1. Реалізували програми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь.
2. Визначили 5 найчастіших біграм шифротексту варіанту 3 (табл. 1); Та знайшли кандидатів на ключ.
3. Для кожного знайденого кандидата на ключ дешифрували текст та зробили перевірку(чи є змістовним текстом російською мовою). Перевірку здійснили шляхом розрахунку індексу відповідності, для кожного з отриманих після дешифрування текстів (індекс відповідності мав бути більшим за 0.055). Для підтвердження коректності обраного методу в табл. 2 наведені деякі значення ключів і індекси відповідності для текстів, що були розшифровані з цими ключами.

Шифрований текст	Розшифрований текст
кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэы охтдшылхщютзгжантзкцхнлюкднхцпвоыомхзотхэт оовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншб чбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужх риажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщю зншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывк цхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоу юмхэшухэозоихщюкцзоюбзюгсвичхшццнщащцжх щюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсуж ушюстлхэдвоэомюфожхетжютдццюгршшкдэйолной хзозпцэкдютэтнцхыдйщюэтжцтйнбшддцывкцхнцхе оцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощх щющцяюстудвежюнхэджядшищвччощщвуной хзозп цэфтмефпшхтдпощщцыкдвуозеойбдээстсдоожмив рбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрс тднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыб дтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлый бсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтв цтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднтт юрюецтйвмшшзцтйищцюеокцфпжюэддйкцвмчоьйн брбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвек дихктщюжонжсиодгуоддйучяожстднтжхщюжощщ щыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбре тйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйей свцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээ ыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыан шшвуйжышьтджфицхеогбшшанжхтдпнягвофихыы жжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюай барбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйет зэстйуэлетмюшюыхнцхтцпвотдучеощищынийькосо тыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесд вейхаирбтюзсжжйбщддццнтдэййбюгрбтдтхыбгцэю болхсджькдрбнхцщйеэотдднщддцбаабжукцеочтйхв юеыдйрббдфхдйыжхшшшщаышиткчсняощщуогба жбфьащелбхшзцтйищцюнхктсджданершецшмбзнбр фоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаю юэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощцв уэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэо аэстжхетжютдхшкдыспнкчнжрбвотдбнкдютрртхтде тмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдву гдпоябрбднтцэющощщтокшеронцчшццнджфитджю кцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэн кчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрб межоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоо хлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцт йвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхб жйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшш ущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхет жютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшер нбйедшзцтйищцюджфицхяберстфпвоэуажкбруатео ахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцт жбфоилсуюыяшшеокояащелбучиххцхнрбвонстдньба нсюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотдд цитвожюшцбдшшсущантсофогбсурржцзожюдюяюэ оддтххгнхщюжбзнкофтждцжжйбвотдромхжюгбгц лхксдкйрретфпасйотдухвцщоыояоетктйхэдетэьвуг	отцеубийствокакизвестноосновноеиизначальноепре ступлениечеловечестваиотдельногочеловекавовсяк омслучаеоноглавныйисточникчувствавинынеизвест ноединственныйлиисследованиямнеудалосьещеуст ановитьдушевноепроисхождениевиныипотребности искупленияноотнюдьнесущественноединственныйл иэтоисточникпсихологическоеположениесложноин уждаетсявобъясненияхотношениемальчикакотцукак мыговоримамбивалентнопомимоненавистииззакото ройхотелосьбыотцакаксоперникаустранитьсуществ уетобычнонекотораядолянежностикнемуобаотноше нияслываютсявидентификациюсотцомхотелосьбыза нятьместоотцапотомучтоонвызываетвосхищениехо телосьбыбытькаконипотомучтохочетсяегоустранит ьвсеэтоналкиваетсянакрупноепрепятствиевопреде ленныймоментребенокначинаетпониматьчтопопытк аустранитьотцакаксоперникавстретилабысостороны отцанаказаниечерезкастрациюизстрахакастрациито естьвинтересахсохраниясвоеймужественностиреб енокотказываетсяотжеланияобладатьматерьюиотус транениятцапосколькуэтожеланиеостаетсявобласт ибессознательногооноявляетсяосновойдляобразова ниячувствавинынамкажетсячтомыописалинормальн ыепроцессыобычнуюсудьбутакназываемогоэдипова комплексаследуетоднаковнестиважноедополнениев озникаютдальнейшиеосложненияеслиуребенкасиль нееразвитконституционныйфакторназываемыйнами бисексуальностьютогдаподугрозойпотеримужестве нностичерезкастрациюукрепляетсятенденцияуклон итьсявсторонуженственностиболеетоготенденцияпо ставитьсебянаместоматериперенятьеероликакобек талюбвиотцаоднализьбоязнькастрацииделаетэтура звязкуневозможнойребенокпонимаетчтоондолженв зятьнасебяикастрированиеслионхочетбытьлюбимы мотцомкакженщинатакобрекаютсянавытеснениеоба порываненавистькотцуивлюбленностьвотцаизвестн аяпсихологическаяразницаусматриваетсявтомчтоот ненавистикотцуотказываютсявследствиестрахапере двнешнейопасностьюкастрациейвлюбленностьжево тцавоспринимаетсякаквнутренняяопасностьпервич ногопозывакотораяпосутисвоейсновавозвращаетсяк тойжевнешнейопасностистрахпередотцамделаетнен авистькотцунеприемлемойкастрацияужаснакаквкач ествекарытакиценылюбвиизобоихфакторовытесня ющихненавистькотцупервыйнепосредственныйстра хнаказанияикастрациисследуетназватьнормальнымп атогеническоеусилениепривноситсякаккажетсялиш ьдругимфакторомбоязньюженственнойустановкияр ковыраженнаябисексуальнаясклонностьстановитсят акимобразомоднимизусловийилиподтвержденийнев розаэтусклонностьочевидноследуетпризнатьиудост оевскогоионалатентнаягомосексуальностьпроявляе тсявдозволенномвидевтомзначениикакоеимелавего жизнидружбасмужчинамивегодостранностинежном отношениикоперникамвлюбвиивегопрекрасномпо ниманииположенийобяснимыхлишьвытесненнойго

цышшсажкбгцфпкйщеьжкхшщцнйовныжрбвоенэиз	мосексуальностьюкакнаэтоуказываютмногочисленн
неожретмхщюдшшшухсугждннььгррщюцйюгдткую	ыепримерыизегопроизведенийсожалеюноничегоне
гаюетмютхыойотдntыбгцэюжхюбвукдвощхщюдшч	могуизменитьеелиподробностионенавистиилюбвик
обхдбдшжуьжгажюпннъхыохзйзцвоыыйбсунбцюэоз	отцуиобихвидоизмененияхподвлияниемугрозыкаст
оихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсаж	рациинесведущемувпсихоанализечитателюпокажут
кбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсу	сябезвкуснымиималовероятнымипредполагаючтои
дйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькю	меннокомплекскастрациибудетотклоненсильнеевсе
дурбщдфхгжеыникоьбгцэюйбрбдntцэюлжгажющо	гоносмеюуверитьчтопсихоаналитическийопытстави
щщкющанмжюйорршхжхщюфмэощняюабгххсййбр	тименноэтиявленияявневсякогосомненияинаходитвн
гшзцтйищщюжхинфиывйугнрцнмттетяюххаюитйхк	ихключклюбомуневрозуиспытаемжеговслучаетакн
чэоэтесшцраирушжцчэмюсуажандйщеябруеыохпы	азываемойэпилепсиинашегописателянонашемусозн
ыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеок	аниютакчуждытеявлениявовластикоторыхнаходитс
шзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонб	янашабессознательнаяпсихическаяжизньуказанным
ажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцн	вышенеисчерпываютсявэдиповомкомплексепоследс
жхвцлшжьгцвужхщююоетнобюхнщютшкчншкчбо	твиявытесненияненавистикотцуновымявляетсяточт
хсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуол	овконцеконцовотождествлениесотцомзавоевываетв
сылжэыпюшбхфньхытцодгжабйбхфйужцбретщюуд	нашемяпостоянноеместоэтоотождествлениевосприн
шшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеет	имаетсянашимянопредставляетсобойвнемособуюин
штехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбр	станциюпротивостоящуюостальномусодержаниюна
удэщхжхтцмхрыонцчшццнйиеыанвущоыылхнцэыгц	шегоямыназываемтогдаэтуинстанциюнашимсверхя
лхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкх	ипринисываемейнаследницеродительскоговлияния
шцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощщвуф	наиважнейшиефункцииеслиотецбылсуровнасильств
тоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдь	енжестокнашесверхяперенимаетотнегоэтикачестваи
жрбгхооюывющючтсдвеетнюяевокйфитдднсесдчоб	вегоотношениикяснованозникаетпассивностькоторо
оэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпво	йкакразнадлежалобыбытьвытесненнойсверхясталос
хсчонххгнбвчетщхыошучберончхпджьмтждкюхцит	адистическимястановитсямазохистскимтоестьвосно
цщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдй	весвоейженственнопассивнымвнашемявозникаетбо
нищдгждцщоыоьжйещюаблюстюбхлнююямбощцю	льшаяпотребностьвнаказанииияотчастиотдаетсебяк
кцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшм	актаковоевраспоряжениесудьбыотчастиженаходиту
мыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюд	довлетворениевжестокомобращенииснимсверхясоз
есбанднбрщюэтсдатлцпнвотдхшкдэйолэтэйеретхжв	наниевиныкаждаякараявляетсяведьвосновесвоейкас
гажщаиашдбншдкцжхыболиндйчетдажгцситцэюмх	трацийикактаковаяосуществлениемизначальногоп
эшсущцитвожюшщшуерюмтцшцсюпдухтдбнгцвотх	ассивногоотношениякотцуисудьбавконцеконцовли
инухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбо	шьдальнейшаяпроекцияотцанормальныеявленияпро
цпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхш	исходящиеприформированиисовестидолжныпоходи
цбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгр	тьнаописанныездесьанормальныенамещенеудалось
бвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбс	установитьразграниченияямеждунимизамечаетсячто
уиндйчечолбнбгхжючээтвиюэятнтцнсесдветхшпоос	наибольшаярольздесьвконечномитогеприписываетс
банкцоохлэттдnттюхлдшшшитщостжошсзхтдьжрбг	япассивнымэлементамвытесненнойженственности ии
хмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкю	ещекакслучайныйфакторимеетзначениеявляетсялив
шсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощй	нушающийстрахотецивдействительностиособеннон
екдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэу	асильственнымэтоотносится кдостоевскомуфактего
мйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвх	исключительногочувствавиныравнокакимазохистск
пикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйе	огообразажизнимысводимкегоособенноярковыраже
рййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфю	нномукомпонентуженственностидостоевскогоможн
екоцппикцбнщожхвбвущджьэыювфюнэстсдвеатлцп	оопределитьследующимобразомособенносильнаяби
нчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтн	сексуальнаяпредрасположенностьиспособностьсосо
цислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсш	бойсилойзащищатьсяотзависимостиотчрезвычайнос
тввюлтдntнойхтюмихлтджюйхцпвотдяочоехыбйбз	уровогоотцаэтотхарактербисексуальностимыдобавл
цлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдн	яемкранееузнаннымкомпонентамегосуществаранни
ьзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсое	йсимптомприпадковсмертиможнорассматриватькак
ютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуй	отождествлениесвоегоясотцомдопущенноевкачеств
щодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдух	енаказаниясосторонысверхятызахотелубитьотцадаб
вцщоыофоюбпокйфигжщддцлхксввсущантсофочое	ыстатьотцомсамомутеперьтыотецноотецмертвыйоб
хыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгц	ычныймеханизмистерическихсимптомовиктомужет
фптцэочоьбгцфпчочобоацлжолфтьюжтфпвекдфтжю	еперьтебяубиваетотецдлянашегоясимптомсмертияв
пюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфд	ляетсяудовлетворениемфантазиимужскогожелания
дйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбру	иодновременномазохистскимпосредствомнаказания

щоыыйбрбитшхыошсзхтдстнтыбюлпюыыеоыывюато шанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлх щюкцооньщечощщвуйоюсзхыбухушпзкцхнрбшшер нбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасц итфпкдьоицжувундэыдйлдюойхфбпойхнудйхнэлща щзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихй хбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэ юцнсесдверианлххнэйрбгхыянбитйюсуюгэшжььгж нбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвует этфтщюбдухтддцситцэюмхэшсурианлххнэйрбгхфо дтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсф рбгхшхвияжьзвотдучяоехфдвукдюткйтцюмнтжхщю гхыочонххгнбйебхохвжанкдвощхщюйувгксююиндй чевостююхцяхщюкоушнбднеокоацяхжхитсюоюйян бэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэсцркьз озбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхо фйуфюьювортнтфддйкдютгцитсдвейхагкцжуружхе огсослфчхшцщцыомтмюитсюфоойервукйниыжзтсд гцитстфпвешбрбднтцфпйотдухвцщоыощощщюггж нбгхкудйэюждвудрзохскдыстднбанщдвехызцчэшхд жщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнх лхгтэдерйетдажбйщтцпвотдучвцйудйпрэвщдшдэыд йут	тоестьсадистическимудовлетворениемобаяисверхяи граютрольотцаидальшевобщемотношениемеждулич ностьюиобектомотцаприсохраненииегосодержания перешловотношениемеждуяисверхяноваяинсценир овканаторойсценетакиеинфантильныереакцииэдип овакомплексамогутзаглохнутьеслидействительност ьнедаетимвдальнейшемпищинохарактеротцаостаетс ятемжесамымнетонухудшаетсясгодамитакимобразо мпродолжаетоставатьсяиненавистьдостоевскогокот цужеланиесмертиэтомузломуотцустановитсяопасн ымеслитакиевытесненныежеланияосуществляютсян аделефантазиясталареальностьювсемерызащитытеп ерьа

Значення ключа

КЛЮЧ: (199 , 700)
I(X)= 0.059761126644656395

Табл. 1: П’ять найчастіших біграм шифртексту

№	Біграма
1	тд
2	рб
3	во
4	щю
5	ен

Табл. 2: Значення ключів і індекси відповідності для текстів, що були розшифровані з цими ключами

Key	I(X)
(199 , 700)	0.059761126644656395
(899 , 848)	0.038838537224361175
(606 , 46)	0.03942416557081949
(761 , 139)	0.044516042833873296
(255 , 102)	0.03869592738256094
(317 , 195)	0.03839218745532289
(455 , 309)	0.0386213308551899
(606 , 294)	0.0411630855772869

Висновки:

Під час виконання даної роботи ми набули навичок частотного аналізу на прикладі моноалфавітної підстановки. Навчились дешифрувати афінний шифр