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 ушюстлхэдвоэомюфожхетжютдцюгршшкдэйолной хзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхе оцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощх щющцяюстудвежюнхэджядшищвчощцвунойхзозп цэфтмефпшхтдпощщщыкдвуозеойбдэзэстсдоожмив рбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрс тднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыб дтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлый бсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтв цтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднтт юрюецтйвмшшзцтйищцюеокцфпжюэддйкцвмчоьйн брбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвек дихктщюжонжсиодгуоддйучяожстднтжхщюжощц щыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбре тйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйей свцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээ ыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыан шшвуйжышьтджфицхеогбшшанжхтдпнягвофихыы жжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюай барбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйет зэстйуэлетмюшюыхнцхтцпвотдучеощищынийькосо тыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесд вейхаирбтюзсжжйбщддццнтдэйййбюгрбтдтхыбгцэю болхсджькдрбнхцщйеэотдднщддцбаабжукцеочтйхв юеыдйрббдфхдйыжхшшшщаышиткчсняощщуогба жбфьащелбхшзцтйищцюнхктсдждайершецшмбзнбр фоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаю юэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощцв уэтегрбьюетитщоойышцчшцабднщдкцжхщюцодтэо аэстжхетжютдхшкдыспнкчнжрбвотдбнкдютррттхтде тмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдву гдпоябрбднтцэющощщтокшерончшццнджфитджю кцтйвмцыдйфиибшфжхмоатсбгцфпюшзцтйищгхэн кчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрб межоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоо хлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцт йвмбхохйощцжунхктсджхетжютдхшкдысжхкйгхб жйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшш ущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхет жютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшер нбйедшзцтйищцюджфицхяберстфпвоэуажкбруатео ахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцт жбфоилсуюыяшшеокояащелбучиххцхнрбвонстднба нсюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотдд цитвожюшцбдшшсущантсофогбсурржцзожюдюяюэ оддтххгнхщюжбзнкофтжджцжжйбвотдромхжюгбгц лхксcдкйрретфпасйотдухвцщоыояоеткт йхэдетэьвуг	отцеубийствокакизвестноосновноеиизначальноепре ступлениечеловечестваиотдельногочеловекавовсяк омслучаеоноглавныйисточникчувствавинынеизвест ноединственныйлиисследованиямнеудалосьещеуст ановитьдушевноепроисхождениевиныипотребности искупленияноотнюдьнесущественноединственныйл иэтоисточникпсихологическоеположениесложноин уждаетсявобяснениях отношениемальчикакотцукак мыговоримамбивалентнопомимоненавистииззакото ройхотелосьбыотцакаксоперникаустранитьсуществ уетобычнонекотораядолянежностикнемуобаотноше ниясливаютсявидентификациюсотцомхотелосьбыза нятьместоотцапотомучтоонвызываетвосхищениехо телосьбыбытьконипотомучтохочетсяегоустранит ьвсеэтонаталкиваетсянакрупноепрепятствиевопреде ленныймоментребенокначинаетпониматьчтопопытк аустранитьотцакаксоперникавстретилабысостороны отцанаказаниечерезкастрациюизстрахакастрациито естьвинтересахсохранениясвоеймужественностиреб енокотказываетсяотжеланияобладатьматерьюиотус транениягоотцапосколькуэтожеланиеостаетсявобласт ибессознательногоонoявляетсяосновойдляобразова ниячувствавинынамкажетсячтомыописалинормальн ыепроцессыобычнуюсудьбутакназываемогоэдипова комплексаследуетоднаковнестиважноедополнениев озникаютдальнейшиеосложненияеслиуребенкасиль нееразвитконституционныйфакторназываемыйнами бисексуальностьютогдаподугрозойпотеримужестве нностичерезкастрациюукрепляетсятенденцияуклон итьсявсторонуженственностиболеетоготенденцияпо ставитьсебянаместоматерииперенятьееролькакобек талюбвиотцаоднализшьбоязнькастрацииделаетэтура звязкуневозможнойребенокпонимаетчтоондолженв зятьнасебяикастрированиеeслионхочетбытьлюбимы мотцомкакженщинатакобрекаютсянавытеснениеоба порываненавистькотцуивлюбленностьвотцаизвестн аяпсихологическаяразницаусматриваетсявтомчтоот ненавистикотцуотказываютсявследствиестрахапере двнешнейопасностьюкастрациейвлюбленностьжево тцавоспринимаетсякаквнутренняяопасностьпервич ногопозывакотораяпосутисвоейсновавозвращаетсяк тойжевнешнейопасностистрахпередотцамделаетнен авистькотцунеприемлемойкастрацияужаснакаквкач ествекарытакиценылюбвиизобоихфакторроввытесня ющихненавистькотцупервыйнепосредственныйстра хнаказанияикастрацииследуетназватьнормальнымп атогеническоеусилениепривноситсяаккажетсялиш ьдругимфакторомбоязньюженственнойустановкияр ковыраженнаябисексуальнаясклонностьстановитсят акимобразомоднимизусловийилиподтвержденийнев розаэтусклонностьочевиднoследуетпризнатьиудост оевскогоионалатентнаягомосексуальностьпроявляе тсявдозволенномвидевтомзначенииикакоеимелавего жизнидружбасмужчинамивегодостранностинежном отношенииксоперникамвлюбвиивегопрекрасномпо ниманииположенийобяснимыхлишьвытесненнойго

цышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэиз
неожретмхщюдшшшухсугждннььгррщюцйюгдткую
гаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшч
обхдбдшжуьжгажюпнньхыохзйзцвоыыйбсунбцюэоз
оихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсаж
кбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсу
дйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькю
дурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющо
щцкющанмжюйорршхжхщюфмэощняюабгххсййбр
гшзцтйищцюжхинфиывйугнрцнмттетяюххаюитйхк
чэоэтесшцраирушжцчэмюсуажандйщеябруеыохпы
ыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеок
шзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонб
ажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцн
жхвцлшжьгцвужхщюююетнобюхнщютшкчншкчбо
хсжхыйбркююышдчхагьхыювцислтсдшшетзэстйуол
сылжэыпюшбхфньхытцодгжабйбхфйужцбретщюуд
шшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеет
штехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбр
удэщхжхтцмхрыонцчшццнйиеыанвущоыылхнцэыгц
лхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкх
шцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощщвуф
тоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдь
жрбгхооюывющючтсдвеетнюяевокйфитдднсесдчоб
оэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпво
хсчонххгнбвчетщхыошучберончхпджьмтждкюхцит
цщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдй
нищдгждцщоыоьжйещюаблюстюбхлнююямбощцю
кцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшм
мыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюд
есбанднбрщюэтсдатлцпнвотдхшкдэйолэтэйеретхжв
гажщаиашдбншдкцжхыболиндйчетдажгцситцэюмх
эшсущцитвожюшщшуерюмтцшцсюпдухтдбнгцвотх
инухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбо
цпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхш
цбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгр
бвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбс
уиндйчечолбнбгхжючээтвиюэятнтцнсесдветхшпоос
банкцоохлэттднттюхлдшшшитщостжошсзхтдьжрбг
хмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкю
шсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощй
екдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэу
мйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвх
пикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйе
рййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфю
екоцппикцбнщожхвбвущджьэывюфюнэстсдвеатлцп
нчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтн
цислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсш
тввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбз
цлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдн
ьзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсое
ютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуй
щодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдух
вцщоыофоюбпокйфигжщддцлхксввсущантсофочое
хыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгц
фптцэочоьбгцфпчочобоацлжолфтьюжтфпвекдфтжю
пюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфд
дйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбру

мосексуальностьюкакнаэтоуказываютмногочисленн
ыепримерыизегопроизведенийсожалеюноничегоне
могуизменитьеелиподробностионенавистиилюбвик
отцуиобихвидоизмененияхподвлияниемугрозыкаст
рациинесведущемувпсихоанализечителюпокажут
сябезвкуснымиималовероятнымипредполагаючтои
меннокомплекскастрациибудетотклоненсильнеевсе
гоносмеюуверитьчтопсихоаналитическийопытстави
тименноэтиявленияявневсякогосомненияинаходитвн
ихключклюбомуневрозуиспытаемжеговслучаетакн
азываемойэпилепсиинашегописателянонашемусозн
аниютакчуждытеявленияввластикоторыхнаходитс
янашабессознательнаяпсихическаяжизньуказанным
вышенеисчерпываютсявэдиповомкомплексепоследс
твиявытесненияненавистикотцуновымявляетсяточт
овконцеконцовотождествлениесотцомзавоевываетв
нашемяпостоянноеместоэтоотождествлениевосприн
имаетсянашимянопредставляетсобойвнемособуюин
станциюпротивостоящуюостальномусодержаниюна
шегоямыназываемтогдаэтуинстанциюнашимсверхя
ипринисываемейнаследницеродительскоговлияния
наиважнейшиефункцииеслиотецбылсуровнасильств
енжестокнашесверхяперенимаетотнегоэтикачестваи
вегоотношениикясновавозникаетпассивностькоторо
йкакразнадлежалобыбытьвытесненнойсверхясталос
адистическимстановитсямазохистскимтоестьвосно
весвоейженственнопассивнымвнашемявозникаетбо
льшаяпотребностьвнаказаниииияотчастиотдаетсебяк
актаковоевраспоряжениесудьбыотчастиженаходиту
довлетворениевжестокомобращенииснимсверхясоз
наниевиныкаждаякараявляетсяведьвосновесвоейкас
трациейикактаковаяосуществлениемизначальногоп
ассивногоотношениякотцуисудьбавконцеконцовли
шьдальнейшаяпроекцияотцанормальныеявленияпро
исходящиеприформированиисовестидолжныпоходи
тьнаописанныездесьанормальныенамещенеудалось
установитьразграниченияміжунимизамечаетсячто
наибольшаярольздесьвконечномитогеприписываетс
япассивнымэлементамвытесненнойженственностии
ещекакслучайныйфакторимеетзначениеявляетсялив
нушающийстрахотецивдействительностиособеннон
асильственнымэтоотносится кдостоевскомуфактего
исключительногочувствавиныравнокакимазохистск
огообразажизнимысводимкегоособенноярковыраже
нномукомпонентуженственностидостоевскогоможн
оопределитьследующимобразомособенносильнаяби
сексуальнаяпредрасположенностьиспособностьсосо
бойсилойзащищатьсяотзависимостиотчрезвычайнос
уровогоотцаэтотхарактербисексуальностимыдобавл
яемкранееузнаннымкомпонентамегосуществаранни
йсимптомприпадковсмертиможнорассматриваткак
отождествлениесвоегоясотцомдопущенноевкачеств
енаказаниясосторонысверхятызахотелубитьотцадаб
ыстатьотцомсамомутеперьтыотецноотецмертвыйоб
ычныймеханизмистерическихсимптомовиктомужет
еперьтебяубиваетотецдлянашегоясимптомсмертияв
ляетсяудовлетворениемфантазиимужскогожелания
иодновременномазохистскимпосредствомнаказания

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

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

Висновки:

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