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-81

Висіцький С.І. Скляр Б.Ю.

Перевірив:

Чорний О.

Київ-2020

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 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.

Методичні вказівки:

Студентам надається текст, що є результатом шифрування за допомогою афінної підстановки біграм відкритого тексту, написаного російською мовою без пробілів, знаків пунктуації та великих літер. Буква «ё» заміщена буквою «е», а «ъ» – буквою «ь» (або навпаки). Таким чином, алфавіт відкритого тексту складається з 31 букви, що занумеровані в алфавітному порядку: , , …, . 0 = а 1=б 30 = я
П'ятьма найчастішими біграмами російської мови (в порядку спадання частот) є біграми «ст», «но», «то», «на», «ен». Перевірте ці відомості за допомогою програми підрахунку частот біграм з комп'ютерного практикуму №1.
Під час дешифрування виникне потреба відрізнити змістовний текст російською мовою від тексту-шуму, що виникає при неправильному дешифруванні. Вважаючи на доволі велику кількість можливих варіантів ключів, для цієї задачі необхідно побудувати автоматичний розпізнавач російської мови. Створення та принцип роботи такого розпізнавача залишається на ваш розсуд; традиційно використовують такі критерії змістовного тексту:
1) перевірку частот частих літер («о», «а», «е», частоти можуть розглядатись окремо або в сукупності);
2) перевірку частот рідкісних літер («ф», «щ», «ь», частоти також можуть розглядатись окремо або в сукупності);
3) перевірку частот біграм, підраховану для біграм «на перетині» (у вищенаведених позначеннях – біграм виду
4) перевірку частот триграм та довільних *l*-грам.

Зашифровані файли за варіантами завдань містяться в папці "variants". Зашифровані файли, що містяться у папці "for_test", є більш простими для аналізу, ніж основні варіанти, їх можна використовувати для тестування або налаштування ваших програм.

Алфавіт, що використовується:

['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с',

'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ы', 'ь', 'э', 'ю', 'я']

Найчастіші біграми в російськомовних текстах:

‘ст’, ’но’, ’ен’, ’то’, ’на’

Найчастіші біграми ШФ:

‘тд’, ‘рб’, ‘во’, ‘щю’, ‘кд’

В процесі виконання практикуму найсуттєвішими труднощами було трактування заданих функцій та їхня коректна взаємодія мовою програмування.

ШФ:

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоыомхзотхэтоовцлшвуджозчх

йбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзю

жмьгнхщюзншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозо

ихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдвоэомюфожхетжютдцюгршшкд

эйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстуд

вежюнхэджядшищвччощщвунойхзозпцэфтмефпшхтдпощщщыкдвуозеойбдэээстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоео

хсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлыйб

суодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмшшзцтй

ищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднт

жхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвцхндн

шбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншшвуйжышьтджфицхеогбшшан

жхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэ

стйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэыс есдвейхаирбтюзсжжйб

щддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотддншддцбаабжукцеочтйхвюеыдйрббдфхд йыжхшшшщаышиткчсняо

щщуогбажбфьащелбхшзцтйищцюнхктсджайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйотгрб арбдкбзцбаююэттдвюко

стщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжх етжютдхшкдыспнкчнжрбво

тдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбдntцэющощщтокше ронцчшццнджфитджюкцтй

вмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрб межоатсбгцфпбхьньзвоыо

эозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхк тсджхетжютдхшкдысжх

кйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцме ввнмжхетжютдхшкдысбхьнэл

жхэоейфитдтхыбэлтдntзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшухж цлжрбгхкйпнвопюшцлшшш

этихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюыхнцхтцпет щцжжйбвотддцитвожюшцбд

шшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтждцжжйбвотдромхжюгбгцлхкссдкй рретфпасйотдухвцщоыояо

етктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждnн ььгррщюцйюгдткуюгаюет

мютхыойотдntыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоыыйбсунбцюэозо ихщюмолесбсуммяюепдэйх

сбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюл чозтлхтбйбьзньйбйужь

кюдурбщдфхгжеыникоьбгцэюйбрбдntцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгх хсййбргшзцтйищцюжхинфиывйу

гнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзюшхыбфшв уйжышэшзцтйищцювснхео

кшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлх щюцнжхвцлшжьгцвужхщююует

нобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхыт цодгжабйбхфйужцбретщюуд

шшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцч

шццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгх

чощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфо

човсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытц

ончхшхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшммы

дйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкц

жхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбр

щюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдри

анлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттдnттюхлдшшш

итщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощйекд

ютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзх

жхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдве

атлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсштввюлтднт

нойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндн

шблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдух

вцщоыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэочоьбгцфпчочо

боацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйшюыхнцхтцпвотдсуыищаднсейузйнбьх

дретыбрущоыыйбрбитшхыошсзхтдстнтыбюлпюыыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньще

чощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпкдьоицжувундэыдйлдюойхфб

пойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэю

цнсесдверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцси

тцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияжьзвотдучяоехфдвукдюткй

тцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюкоушнбднеокоацяхжхитсюююйянбэюцпчэ

дйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфддйкдютгцит

сдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюггжнб

гхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбй

щтцпвотдучвцйудйпрэвщдшдэыдйут

BT(key:190,700):

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекавовсякомслучае

оноглавныйисточникчувствавинынеизвестноединственныйлиисследованиямнеудалосьещёустановитьдушевноепрои

схождениевиныипотребностиискупленияноотнюдьнесущественноединственныйлиэтоисточникпсихологическоеполо

жениесложноинуждаетсявобъясненияхотношениемальчикакотцукакмыговоримамбивалентнопомимоненавистииззако

торойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекотораядолянежностикнемуобаотношениясливаю

тсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипот

омучтохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймоментребенокначинаетпо

ниматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказаниечерезкастрацию изстрахакаст

рациитоестьвинтересахсохранениясвоеймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустр

анениятцапоскольуэтожеланиеостаетсявобластибессознательногооноявляетсяосновойдляобразо ваниячувства

винынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбутакназываемогоэдиповакомп лексаследуетоднако

внестиважноедополнениевозникаютдальнейшиеосложнениеслиуребенкасильнееразвитконституц ионныйфакторназ

ываемыйнамибисексуальностьютогдаподугрозойпотеримужественностичерезкастрациюукрепляет сятенденцияукло

нитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместоматерииперенятьеёрольк акобъекталюбв

иотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчтоондолженвзят ьнасебяикастри

рованиеслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснениеобапорыванена вистькотцуивлюблен

ностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютс явследствиес

трахапередвнешнейопасностьюкастрациейвлюбленностьжевотцавоспринимаетсякаквнутренняяоп асностьпервично

гопозывакотораяпосутисвоейсновавозвращаетсяктойжевнешнейопасностистрахпередотцамделает ненавистькотцу

неприемлемойкастрацияужаснакаквкачествекарытакиценылюбвиизобоихфактороввытесняющихн енавистькотцуперв

ыйнепосредственныйстрахнаказанияикастрациисследуетназватьнормальнымпатогеническоеусилен иепривноситсяк

аккажетсялишьдругимфакторомбоязньюженственнойустановкиярковыраженнаябисексуальнаяскл онностьстановитс

ятакимобразомоднимизусловийилиподтвержденийневрозаэтусклонностьочевиднодолжноследуетпризнать иудостоевского

ионалатентнаягомосексуальностьпроявляетсявдозволенномвидевтомзначениикакоеимелавегожизн идружбасмужчи

намивегодостранностинежномотношениихсоперникамвлюбвиивегопрекрасномпониманииположе нийобъяснимыхлишьв

ытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведенийсо жалеюноничегоне

могуизменитьеелиподробностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозы кастрациинесведу

щемувпсихоанализечитателюпокажутсябезвкуснымиималовероятнымипредполагаючтоименноком плекскастрациибуд

етотклоненсильнеевсегоносмеюуверитьчтопсихоаналитическийопытставитименноэтиявлениявнев сякогосомнения

инаходитвнихключклюбомуневрозуиспытаемжеговслучаетакназываемойэпилепсиинашегописате лянонашемусознан

иютакчуждытеявленияповластикоторыхнаходитсянашабессознательнаяпсихическаяжизньуказанн ымвышенеисчерпы

ваютсявэдиповомкомплексепоследствиявытесненияненавистикотцуновымявляетсяточтовконцекон цовотождествле

ниесотцомзавоевываетвнашемяпостоянноеместоэтоотождествлениевоспринимаетсянашимянопред ставляетсобойвн

емособуюинстанциюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстан циюнашимсверхяипри

писываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецбылсуровнасильств енжестокнашесвер

хяперенимаетотнегоэтикачестваивегоотношениикяснованозникаетпассивностькоторойкакразнадле жалобыбытьвы

тесненнойсверхясталосадистическимястановитсямазохистскимтоестьвосновесвоейженственнопасс ивнымвнашемя

возникаетбольшаяпотребностьвнаказанииияотчастиотдаетсебякактаковоевраспоряжениесудьбыот частиженаходи

тудовлетворениевжестокомобращениисниmсверхясознаниевинykаждаякараявляетсяведьвосновесв оейкастрациейи

кактаковаяосуществлениемизначальногопассивногоотношениякотцуисудьбавконцеконцовлишьда льнейшаяпроекци

яотцанормальныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаописанныезд есьанормальныенам

ещёнеудалосьустановитьразграниченияmеждунимизамечаетсячтонаибольшаярольздесьвконечном итогеприписывае

тсяпассивнымэлементамвытесненнойженственностиищекакслучайныйфакторимеетзначениеявляе тсяливнушающийс

трахотецивдействительностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключ ительногочувст

вавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраженномукомпоненту женственностидос

тоевскогоможноопределитьследующимобразомособенносильнаябисексуальнаяпредрасположенностьиспособностьс

особойсилойзащищатьсяотзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкра

неузнаннымкомпонентамегосуществараннийсимптомприпадковсмертиможнорассматриватькакотождествлениесвое

гоясотцомдопущенноевкачественаказаниясосторонысверхятызахотелубитьотцадабыстатьотцомсамомутеперьтыот

ецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужетеперьтебяубиваетотецдлянашегоясимптомсме

ртиявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазохистскимпосредствомнаказаниятоесть

садистическимудовлетворениемобаяисверхяиграютрольотцаидальшевобщемотношениемеждуличностьюиобъектомот

цаприсохраненииегосодержанияперешловотношениемеждуяисверхяноваяинсценировканавторойсценетакиеинфанти

льныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедаетимвдальнейшемпищинохарактеротца

остаетсятемжесамымнетонухудшаетсясгодамитакимобразомпродолжаетоставатьсяиненавистьдостоевскогокотцуж

еланиесмертиэтомузломуотцустановитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделефантазияст

алареальностьювсемерызащитытеперьу

Висновки:

В ході виконання роботи проаналізовано роботу частотного аналізу на прикладі розкриття моноалфавітної підстановки.

Під час виконання лабораторного практикуму отримано навички дешифрування текстів, що зашифровані методом афінної підстановки, на основі частотного аналізу біграм.