Міністерство освіти і науки України
НТУУ«Київський політехнічний інститут»
Фізико-технічний інститут

Лабораторні роботи

з предмету «Криптографія»
Варіант 4

Виконали:
Студенти III курсу
ФТІ групи ФБ-84
Гайворон О.О.
Солдатов В. А.
Перевірив:
Чорний О. М.

Київ 2021

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:

Ознайомившись з теоретичними відомостями і методичними вказівками, та переглянувши деякий додатковий матеріал, було обрано мову програмування Java.

Для виконання завдання поставленого в ЛР було створено:

Main – клас, що запускається на виконання користувачем.

Analyzer – клас інструментів, що використовуються для обробки інформації.

Linalg – клас, що виконує лінійні порівняння, враховує випадки із декількома розв'язками.

Service – клас допоміжних/між етапних функцій.

Найчастіші п'ять біграм у шт варіант 4:

«еш», «еы», «шя», «ск», «до»

Ключ 390 10

ШТ	ВТ
щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцм	еслиправдачтодостоевскийвсибиринебылп
одпмурзфбряцкмдыйдосштцмижбчфипмугфбз	одверженприпадкамтоэтолишьподтверждае
чшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзн	тточтоегоприпадкибылиегокаройонболеев
ыертзилгфоцбчполфмэдцщкйкшйэысйрэйкчо	нихненуждалсякогдабылкараеминымобразо
зычфждьмйшотдотзьоюйсщзоюдууюзсшшстзр	мнодоказатьэтоневозможноскорееэтойнео
эыосяфоешыенывдьмиыыяшцрбгянямзюдшскд	бходимостьювнаказаниидляпсихическойэк
мыайыяаоешезвжпонорэкжцчжшбчдофшщофбя	ономиидостоевскогообясняетсяточтоонпр
оязфыщжвонцеырайхмучмсшывчфвэрфешмяоя	ошелнесломленнымчерезэтигодыбедствийи
йывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешж	униженийосуждениедостоевскоговкачеств
змоуяхямзюдлвзбкзешдбшящксавотзябйкжз	еполитическогопреступникабылонесправе
шцопсйкоефтцрзюэдцсшямсканзомыжуэыыцс	дливымиондолженбылэтознатьноонпринялэ
шмычмэжглрзщыезскщквкшятоьэйштибяшкоч	тонезаслуженноенаказаниеотбатюшкицаря
щкфмыйеыйывдьмиыщчвккцощеызонорйвкхпш	какзаменунаказаниязаслуженногоимзасво

сзунрмоншзоязшяэдхпезхлсопжипеызохлнш	йгрехпоотношениюксвоемусобственномуот
плбйщждоыкфоскщквкшягоефоцэзччскщквка	цувместосамонаказанияондалсебянаказат
нвказешюшлцромглтдоккжшскзыядншууезжу	ьзаместителюотцаэтодаетнамнекотороепр
рфешщпнзшятоужертцлвяхщжпофожущпккшяэ	едставлениеопсихологическомоправдании
ывдьмиыйсжусжощккшйжррэсзешьоктдоскык	наказанийприсуждаемыхобществомэтонаса
фотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшс	момделетакмногиеизпреступниковжаждутн
кщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэ	аказанияеготребуетихсверхяизбавляясеб
цшвдрйрэйкчофолжыймывдьмиыщчдорддокыб	ятакимобразомотсамонаказаниятотктозна
злжвочыезыяюйеытяьочмскмзшядяешмуяхщж	етсложноеиизменчивоезначениеистеричес
бягжрйашайюпмогйжшфшайрмлзнntзхаокшйб	кихсимптомовпойметчтомыздесьнепытаемс
чаощяанбччйтжмкжучбуфпошфбждоцпюдлвюп	ядобитьсясмыслаприпадковдостоевскогов
юпэзкбтцзопзаоешйшохзодонофшайсщзожур	овсейполнотедостаточнотогочтоможнопре
фмовоцяанфшляйбмуьосклкюнсккжеьзоешшо	дположитьчтоихпервоначальнаясущностьо
ешоцэжлыдяюйеызопыщжфоочсквжаббжнзбля	сталасьнеизменнойнесморянавсепоследую
ьхзсккцезшяййсщзоюдьмйшнхдоаоешезвжбя	щиенаслоенияможносказатьчтодостоевски
ршвдшяполфзятзбжьоиосяйжгоелзурмеыйсс	йтакникогдаинеосвободилсяотугрызенийс
ожзешопхпимсжсказкзшяшйнэюшшомглтдонз	овестивсвязиснамерениемубитьотцаэтоле
пксзеыэжюпщжхявушйгожурфлцгцншвдрздвщ	жащеенасовестибремяопределилотакжеего
оцыыиеыхзнфылтфаляыжфзйквбждэечяыжхы	отношениекдвумдругимсферампокоющимсян
хоцыыиеыыяпомггднотлккжжипеызохлщпдор	аотношенииикотцукгосударственномуавтор
япзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзо	итетуикверевбогавпервойонпришелкполно
хлмофхэыеынеткзеадьгпуротынщйайкбазущ	муподчинениюбатюшкецарюоднаждыразыгра
пязхлдырйпоазсяслщяджипщплзджипюшлцлы	вшемуснимкомедиюубийствавдействительн
бжхяскыосяэищеештцедууьмншйкрзшяцпдвз	остинаходившуюстолькоразотражениевего
бряцкмдррхфщжэпмуапзчвомощкхыхзиоюняз	припадкахздесьверхвзялопокаяниебольше
хпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяя	свободыоставалосьунеговбластирелигио
мзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфо	знойпонедопускающимсомненийсведениямо
ефзббжнзтыссжяилнахпезфщпмшявжядтцйэо	ндопоследнейминутысвоейжизнивсеколеба
цбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтз	лсямеждуверойибезбожиемеговысокийумне
моыптцыцшййычмыйзхйшмшжшалтыбжхябжюак	позволялемунезамечатьтетрудностиосмыс
цопиыщчыдншуусйжуопчфюшжзйкмяефопифбк	ливаниякоторымприводитверавиндивидуа
юнзовбюпдокзшярйдуюплвляешууяхщжпоной	льномповторениимирового исторического гор
кыпюшщчмысклзыцбчмялзоцнрряешиыфсхяда	азвитияоннадеялсявидеалехристанайтивы
ыосябжьоиогфеыхзншзунрюпыяябтцюмюпйша	ходиосвобождениеотгреховииспользовать
жьосжрэешжзщыцзешйкккшячхдосажуюшимйш	своисобственныестраданиячтобыпритязат
лыпутцурряешбзкцколппотзуыайжхжшеыабр	ьнарольхристаеслионвконечномсчетенепр
яязодхпрэчфдяешоцкзвдаямымуайдосщщочч	ишелксвободеисталреакционеромтоэтообя
дыозлжцшшйфшщоцьзхлцюпзхщжщккжюыюпцчз	сняетсятемчтообщечеловеческаясыновняя
пэыиывдншуушсешяоюшбчкзуяяяямзозхьпеш	винанакоторойстроитсярелигиозноечувст
ьоаоешывмкйыдвбжжзщрэысямяблоцлышсгял	водостиглаунегосверхиндивидуальнойсил
аэышйлвмксаанжутоаонзскккрздвюптжждшс	ыинемоглабытьпреодоленадажееговысокой
эыпзьцяделоцлыбжанхмлзннскюдьмоцбжпэс	интеллектуальностьюздесьнасказалосьбы
йсщзодбкзвыкшэпдойхдоюанщщкбаекшйбчнш	можноупрекнутьвтомчтомыотказываемсяот
узябряешйкешзоешчбгяыоиыоцпмзямодпмуч	беспристрастностипсихоанализаиподверг
кшйаоешезвжпоновгеыьзрйхесзкбйкьосктл	аемдостоевскогооценкеимеющейправонасу
сзешьоекшялцмиажжусжюуэжцышсдондпмкзш	ществованиелишьспристрастнойточкизрен
ягожурфлцеызоножяяоьоэмкзшяпдмыэзгпйш	ияопределенногомировоззренияконсерват
ууешоцсаскдондымкзшязплццдлвляудмяйяд	орсталбынаточкузренияявеликогоинквизит
ойккощзшяекшэйфбждоцпюдлвляскмздбкзцж	ораиоценивалбыдостоевскогоиначеупрекс
жущпрфуяшфсчдвбждчвхеыщчфочытцмиажщкв	праведливдляегосмягченияможнолишьсказ
канфшууфиеыхзаоешезвжпонодаыпиыщомзмя	атьчторешениедостоевскоговызваноочеви
тыямйшалтыеызоешыедвайнинзшязпкцрфешм	днозатрудненностьюегомышленияв следств
яеыцпяовкрфекуяжубждоджгллкпыбжанцйсщ	иеневрозаедвалипростойслучайностьюмож
зорэкжшяанфшншряязлзфуыйдуюпшсуяпзйке	нообяснитьчтотришедеврамировойлитерат
лиавжнрфушйеыюувделдшчфилюшощжшшйкшшй	урывсехвременттрактуютоднуитужетемутем
цомгулщяджипюгпуотсяужзюждмкчкнцжшязц	уотцеубийствацарьэдипсофоклагамлетшек
жюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюпюп	спираибратьякарамазовыдостоевскоговов
эзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтло	сехтрехраскрываетсяимотивдеяниясексуа
цлыезсочзсыяхщжипляэмнщеычяражуййюзвж	льноесоперничествоиззаженщиныпрямеевс
двждмызхзосшзбкззжокуцеыюпщуыйтодыюпи	егоконечноэтопредставленовдрамеоснова
ызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюп	ннойнагреческомсказаниииздесьдеяниесов
муюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчп	ершаетсяещесамимгероемнобезсмягченияи
мщпбкуяяоекшярбптхямзюдечрэйкиордиыцп	завуалированияпоэтическаяобработканев
ямфочыхордяожзщыезжупмскшяцпсказкзшял	озможнаоткровенноепризнаниевнамерении

лщяанншшкщкпоноюааощяекшйбчжучбгяыоиы	убитьотцакакогомыдобиваемсяприпсихоан
оцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщ	ализекажетсянепереносимымбезаналитиче
жпокбчфнодоздопзузхщжпоьфйказтзрэыося	скойподготовкивгреческойдраменеобходи
фощждчвхеыхзжусжфрйктзшясжеьзоешрйэжп	моесмягчениеприсохранениисущностимаст
зжжбяаоешывбзлжцшшйфшрэщжсокыйшлцлыкс	ерскидостигаетсятемчтобессознательный
фохямвмуйчжуезаяалжшбчшфссешмяпзюнзое	мотивгерояпроецируетсявдействительнос
шедвдвлгфезшйдбряилгфеыхзсккчвкщыезтл	тькакчуждоеемупринуждениенавязанноесу
ыниоовмушссожзбибзвфвчшяеыабкзтыыймуе	дьбойгеройсовершаетдеяниенепреднамере
ызочбюпээбпифрйбжхяузыпуяхыщчрзхьэыэя	нноиповсейвидимостибезвлиянияженщиныи
вжкщитдоешзхеыхзрэешйчпзюнешибряшяякж	всежеэтостечениеобстоятельствпринимае
шбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутг	тсяврасчеттаккаконможетзавоеватьцариц
эййшмштцедзббжнзмоошууеыщчдонорзлзджи	уматьтолькопослеповторениятогожедейст
пщчьоцыыиеыыявлаомярктяшптцпмдущесзно	виявотношениичудовищасимволизирующего
ншшкмокцжшлвждвдрэскалцяекжшбчкожцчиб	отцапослетогокакобнаруживаетсяиоглаша
злжозномясктзлзмкжшбчшящкбяйбзбяшждды	етсяеговинанеделаетсяникакихпопытоксн
цшдзщжэзччамекуяанюзскжуэыощлзшящжбжд	ятьеессебявзвалитьеенапринуждениесост
ояоратлынсаскрэууншмяскжупмскжшбчцдвд	оронысудьбынаоборотвинапризнаетсяикак
вжьглцечмяскскщкбаекжшбчфшууэжтлмдэйс	всецелаявинанаказываетсячторассудкумо
щжшмощквканбчтзябйкжзшцопсйзоужертцлв	жетпоказатьсянесправедливымнопсихолог
яхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфй	ическиабсолютноправильнованглийскойдр
казсшлячовунщеырэтцюзпохпеызомоешдбжд	амеэтоизображеноболеекосвеннопоступок
сожзбибзлжхыщжыйрйшзяошйуфаляятфсчпод	совершаетсянесамимгероемадругимдлякот
ояоносшншмоешдбждтззпсчжшбчншщзнэйсеш	орогоэтотпоступокнеявляетсяотцеубийст
ьовбптдохлжурфбжффюшлцлыксфохявжядтло	вомпоэтомупредосудительныймотивсексуа
цлылвбжзбмушямзешекощеычяратзилгфбзлж	льногосоперничествауженщиныненуждаетс
зпвкылоцдуюпиыыяйкныляыфчбюпповбнзцжш	явзавуалированииравноиэдиповкомплексг
зяоййппифрйщкжэппншйкрзщыайхпжшжшвдщк	ероямывидимкакбывотраженномсветететакка
хйппифрйуяпндощкпорфссешмяабяопмьосяц	кмывидимлишьтокакоедействиепроизводит
ызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавк	нагерояпоступокдругогоондолженбылбыза
сшншмоешдбждншайешюшлыбжюуиырафовуьма	этотпоступокотомстить ностраннымобразо
йтзвжгцррсшбжлзмканюакыбзйхдодвууэжкц	мневсилахэтосделатьмызнаемчтоегорассл
мэсчжшсопжипеызозхьпешьомяравжщоипжше	абляетсобственноечувствовинывсоответс
шмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжу	твиисхарактеромневротическихявленийпр
лямрчфюшпфмяяявлвжипюпэышбмунрчфюшьос	оисходитсдвигичувствовиныпереходитвос
окыиыхзхпезпыщжмосоьыбжхядамофыюшотдо	ознаниесвоейнеспособностивыполнитьэто
вкккшяабйчуцжелжрбрякывдюшлвохдошзяоб	заданиепоявляютсяпризнакитогочтогерой
пбжжуэырйбзщтелмяилщкцжжзщрэысяныблоц	воспринимаетэтувинукаксверхиндивндуал
лыщемыжучмдубзвфаляяоышйеыюзмзыжйэозк	ьнуюонпрезираетдругихнеменеечемсебяес
цкогрчфюшажкжщкгфсймовккцивыйгшьльфжш	лиобходитьсяскаждымпозаслугамктоуйдет
ншмолдопсшайскжущпнзшядуайиыалшжпоною	отпоркивэтомнаправлениироманрусскогоп
яыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджип	исателяуходитнашагдальшеиздесьубийств
бжюпмуяззощуиврймзвожзпофотывдохлцюпя	осовершенодругимчеловекомоднакочелове
дайхпимиыраыжнэюшсйокбяжярзьазонырйко	комсвязаннымсубитымтакимижесыновнимио
цыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайн	тношениямикакигеройдмитрийукоторогомо
шопэзцжбкюнзоносочзсыяхщжипхордяожзщы	тивсексуальногосоперничествао ткровенн
збрякыбзлжкжюпмуяззощуиврйвуйшайподоя	опризнаетсясовершенодругимбратомкотор
охлщкбяьшмущжзовказхяанаоешезвжбякбму	омукакинтереснозаметитьдостоевскийпер
рфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзу	едалсвоюсобственнуюболезньякобыэпилеп
жнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхз	сиютемсамымкакбыжелаясделатьпризнание
фшайтцлбгцабхявыцпяохяупайтзншщзнэйсш	чтомолэпилептикневротиквомнеотцеубийц
копншфузхпмдьюшшящкскткллзокрзпмжзешск	аивотвречизащитниканасудетажеизвестна
хыэжазадиыуфужертцлвхззоскфопбоцщкчфы	янасмешканадпсихологиейонамолпалкаодв
лидмышкбмщпбкуяяоекзожзуяпонзяыншвдщк	ухконцахзавуалированновеликолепнотакка
цждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэо	кстоитвсеэтоперевернутьинаходишьглубо
хфсфлчжеьзоешэпбжжущчхябфбждоцпюдлвям	чайшуюсущностьвосприятиядостоевскогоз
эжглцяекжшскчйфибяншкеынтзужертцлвщчэ	аслуживаетнасмешкиотнюдьнепсихологияа
жффйэракбяощзшжаокыиыщчсожзбиеызоузсу	судебныйпроцессдознаниясовершеннобезр
ьмуяуыжддосшншмоешдбждсожзбигцскыкфот	азличноктоэтотпоступоксовершилнасамом
флцабгяыовояяфяьшмущжвзлжыцмимшшйгшез	делепсихологияинтересуетсялишьтемктое
новжьошйэээфщзрзмкуягшзбезносожзбиеыы	говсвоемсердцежелаликтопоегосовершени
ядвзбряжзлжипюпоцчбптдохлибвоанаопоьш	иегоприветствовалипоэтомувплотьдоконт
йкешзокюывруххкнзеявжйэйканэущпзомязон	растнойфигурыалешивсебратьяравновинов
ыйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлы	ныдвижимыйпервичнымипозывамиискательн
эжмкгфеыйсмофыксюдабгяыкаяшябялбгцабх	аслаждений полныйскепсисациникиэпилепт

ямзюдйсжущжеляыцдсэйканюрщкйкякчодазз	ическийпреступниквбратьяхкарамазовыхе
ешажщзскяптжязджпзчзшяжкйкгшмускбфсча	стьсценаввысшейстепенихарактернаядляд
оешезвжпонопмйкйвюпууэжжйюшряшйешпуьг	остоевскогоизразговорасдмитриемстарец
моешывбзшхдожйюшряпыбжюшвжйэдвншюпзое	постигаетчтодмитрийноситвсебеготовнос
шеднщщзнэйсешылбэяоыкжшбччзкзтырйскпо	тькотцеубийствуибросаетсяпереднимнако
нзшясшмышйсщжшзпсчанбчдайкрзшяшйьомрш	лениэтонеможетявлятьсявыражениемвосхи
ьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцч	щенияадолжноозначатьчтосвятойотстраня
жшншэзччсжрлязшядяябтцшяанбчжучмкзшяш	етотсебяискушениеисполнитьсяпрезрение
йрлщяегдяуярймоаышийшажфямосшайдбмурф	мкубийцеилиимпогнушатьсяипоэтомуперед
шяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзе	нимсмиряетсясимпатиядостоевскогокпрес
шдбшярллзджипюшлцлырэчмзуиыяхскмыуфоц	тупникудействительнобезграничнаонадал
ядюпжрчфюшвкжурфлцтжбжюууфиыщчскподоя	ековыходитзапределысостраданиянакотор
оеыщжлкешраояазжшжущпщоскскможяскжшбц	оенесчастныйимеетправоонанапоминаетбл
звлвюпеыхзюдншуусйшфкзныбжхяншзогяуян	агоговениескоторымвдревностиотносилис
нетюянзашцдияблязнырэтцлыайдбкзешдбшя	ькэпилептикуидушевнобольномупреступни
нфсчтзномофшсжцкгяпзюнамзпеяпыэжйээпэ	кдлянегопочтиспасительвзявшийнасебяви
ыгдншуущешфалноыжгллкеыщжуясащуивхзак	нукоторуювдругомслучаенеслибыдругие

Висновок:

В ході опрацювання ЛР отримали практичні навички по роботі з модульною арифметикою, та біграмно-афінним шифром.