КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Варіант 4

Виконали: ФБ-04 Ковальчук Єгор

ФБ-04 Омелянович Олександр

Криптоаналіз афінної біграмної підстановки

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.

Результати роботи:

Ключ: 390, 10

Зашифрований текст:

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощк

яоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывд

ьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмяояйывщ

еыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомы

жуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдхп

езхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезжурфешщпнз

шятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгф

кшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмск

мзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопз

аоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбляь

хзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюш

шомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггд

нотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхл

дырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхз

иоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахп

езфщпмшявжядтцйэоцбчазгфыпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыц шййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыд

ншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщж поноЙкыпюшщчмысклзыцбчмялзоцнрряешиыфсхя

даыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйккк шячхдосажуюшимйшлыпутцурряешбзкцколппотз

уыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйф шщоцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушс

ешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгяла эышйлвмксаанжутоаонзскккрздвюптжждшсэы

пзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщк баекшйбчншузябряешйкешзоешчбгяыоиыоцпм

зямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжус жюуэжцышсдондпмкзшягожурфлцеызоноожя

яоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощз шяекшэйфбждоцпюдлвляскмздбкзцжжущпрф

уяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпи ыщомзмятыямйшалтыеызоешыедвайнинзшязпкц

рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлз фуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдш

чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйк бэйканпдпуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэж

йуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюз вждвждмызхзосшзбкззжокуцеыюпщуыйтодыюп

иызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяо шйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямзюдеч

рэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкп оноюаающяекшйбчжучбгяыоиыоцпмяднщжшбчтз

чзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощ ждчвхеыхзжусжфрйктзшясжеьзоешрйэжпзжж

бяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфсс ешмяпзюнзоешедвдвлгфезшйдбряилгфеыхзсккч

вкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбифрйбж хяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэ

ешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййш
мштцедзббжнзмоошууеыщчдонорзлзджипщчьоцы

ыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчко
жцчибзлжозномясктзлзмкжшбчшящкбяйбзбяш

жддыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншм
яскжупмскжшбчцдвдвжьглцечмяскскщкбаекжш

бчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсо
еецызбйкмяюнзоекшвуяджпоьфйказсшлячову

нщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчп
одояоносшншмоешдбждтззпсчжшбчншщзнэйсеш

ьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеыч
яратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчб

юпповбнзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяп
ндощкпорфссешмяабяопмьосяцызвмуйчмоешдбжд

щуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьма
йтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсч

жшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбя
лчуцеыйсжулямрчфюшпфмяяявлвжипюпэышбмунр

чфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелж
рбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяил

щкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрч
фюшажкжщкгфсймовккцивыйгшьльфжшншмолдоп

сшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщ
лщяджипбжюпмуяззощуиврймзвожзпофотывдохлц

юпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьф
жяюуйсгдншуулвайншопэзцжбкюнзоносочзсыях

щжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшм
ущжзовказхяанаоешезвжбякбмурфоцхпэесопж

ипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхз
фшайтцлбгцабхявыцпяохяупайтзншщзнэйсшк

опншфузхпмдьюшшящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхззоск
фопбоцщкчфылидмышкбмщпбкуяяоекзожзуяпо

нзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэп
бжжущчхябфбждоцпюдлвямэжглцяекжшскчйфи

бяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуя
уыжддосшншмоешдбждсожзбигцскыкфотфлцаб

гяыовояяфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезнос
ожзбиеыыядвзбряжзлжипюпоцчбптдохлибвоан

аопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйч
бямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдаб

гяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскя
птжязджпзчзшяжкйкгшмускбфсчаоешезвжпо

нопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдв
ншюпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйск

понзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшн
хдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшя

анбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочж
шбчгявбйшщчаоешезвжпоноэбкзешдбшярллзджип

юшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскпод
ояоеыщжлкешраояазжшжущпщоскскможяскжшбцзв

лвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыай
дбкзешдбшянфсчтзномофшсжцкгяпзюнамзпея

пыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

Розшифрований текст:

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьпод
тверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылк
араеминымобразомнодоказатьэтоневозможноскорееэтойнеобходимостьювна
казаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесл
омленнымчерезэтигодыбедствийиунижениййосуждениедостоевскоговкачестве
политическогопреступникабылонесправедливымиондолженбылэтознатьноон
принялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслу
женногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонак
азанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлени
еопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамо
мделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавля
ясебятакимобразомотсамонаказаниятотктознаетсложноеиизменчивоезначени
еистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприп
адковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчто
ихпервоначальнаясущностьосталасьнеизменнойнесморянавсепоследующиен

аслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызени
йсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопределило
такжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгос
ударственномуавторитетуикверевбогавпервойонпришелкполномуподчинени
юбатюшкецарюоднаждыразыгравшемуснимкомедиюубийствавдействительн
остинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяние
большесвободыоставалосьунеговобластирелигиознойпонедопускающимсомн
енийсведениямондопоследнейминутысвоейжизнивсеколебалсямеждуверойиб
езбожиемеговысокийумнепозволялемунезамечатьтетрудностиосмысливанияк
которымприводитверавиндивидуальномповторениимировогоисторическогор
азвитияоннадеялсявидеалехристанайтивыходиосвобождениеотгреховииспольз
оватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконеч
номсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщеч
еловеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглауне
госверхиндивидуальнойсилыинемоглабытьпреодоленадажееговысокойинтел
лектуальностьюздесьнасказалосьбыможноупрекнутьвтомчтомыотказываемся
отбеспристрастностипсихоанализаиподвергаемдостоевскогооценкеимеющей
правонасуществованиелишьспристрастнойточкизренияопределенногомирово
ззренияконсерваторсталбынаточкузренияявеликогоинквизитораиоценивалбыд
остоевскогоиначеупрексправедливдляегосмягченияможнолишьсказатьчторе
шениедостоевскоговызваноочевиднозатрудненностьюегомышленияявследств
иеневрозаедвалипростойслучайностьюможнообяснитьчтотришедеврамирово
йлитературывсехвременктрактуютоднуитужетемутемуотцеубийствацарьэдипс
офоклагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраскрывае
тсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсегоконечн
оэтопредставленовдрамеоснованнойнагреческомсказанииздесьдеяниесоверш
аетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобработка
невозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемс
яприпсихоанализекажетсянепереносимымбезаналитическойподготовкивгреч
ескойдраменеобходимоесмягчениеприсохраненииисущностимастерскидостига
етсятемчтобессознательныймотивгерояпроецируетсявдействительностькакчу
ждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамер
енноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельств
принимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторе
ниятогожедействиявотношениичудовищасимволизирующегоотцапослетогока
кобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьееесеб
явзвалитьеенапринуждениесостороныисудьбынаоборотвинапризнаетсяикаквсе
целаявинанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихо
логическиабсолютноправильнованглийскойдрамеэтоизображеноболеекосвен
нопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнея
вляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперни
чествауженщиныненуждаетсявзавуалированииравноиэдиповкомплексгероям

ывидимкакбывотраженномсвететаккакмывидимлишьтокакоедействиепроизв
одитнагерояпоступокдругогоондолженбылбызаэтотпоступокотомститьностр
аннымобразомневсилахэтосделатьмызнаемчтоегорасслабляетсобственноечув
ствовинывсоответствиисхарактеромневротическихявленийпроисходитсдвиги
чувствовиныпереходитвосознаниесвоейнеспособностивыполнитьэтозаданиеп
оявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуальн
уюонпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамкто
уйдетотпоркивэтомнаправлениироманрусскогописателяуходитнашагдальшеи
здесьубийствосовершенодругимчеловекомоднакочеловекомсвязаннымсубит
ымтакимижесыновнимиотношениямикакигеройдмитрийукоторогомотивсекс
уальногосоперничестваоткровеннопризнаетсясовершенодругимбратомкоторо
мукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобы
эпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротик
вомнеотцеубийцаивотвречизащитниканасудетажеизвестнаянасмешканадпсих
ологиейонамолпалкаодвухконцахзавуалировановеликолепнотаккакстоитвсеэ
топеревернутьинаходишьглубочайшуюсущностьвосприятиядостоевскогозасл
уживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершен
нобезразличноктоэтотпоступоксовершилнасамомделепсихологияинтересуетс
ялишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветствовали
поэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимы
йпервичнымипозывамиискательнаслажденийполныйскепсисациникиэпилепт
ическийпреступниквбратьяхкарамазовыхестьсценаввысшейстепенихарактерн
аядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитрийноситвс
ебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлять
сявыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискуш
ениеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсм
иряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадал
ековыходитзапределысостраданиянакотороенесчастныйимеетправоонанапом
инаетблагоговениескоторымвдревностиотносилиськэпилептикуидушевнобол
ьномупреступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругом
случаенеслибыдругиеаа

Висновки:

У ході роботи ми ознайомилися з роботою шифра афінної біграмної підстановки, набули навичок частотного аналізу, опанували прийомами роботи в модулярній арифметиці.