Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №3
Криптоаналіз афінної біграмної підстановки
Варіант 4

Виконали:
Студенти ФБ-01
Новак О. І.
Тостоган Є. Г.

Київ 2022

Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Постановка задачі:

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.

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.

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

Спершу ми написали необхідні математичні функції, такі як: знаходження оберненого за модулем числа, НСД двох чисел, розширений алгоритм Евкліда та розв'язання лінійного рівняння.
Для виведення 5 найчастіших біграм ШТ скористалися функцією frequency() з першої лабораторної роботи, та отримали такий результат:

```
['еш', 'еы', 'шя', 'ск', 'до']
```

Для того щоб знайти всі можливі ключі ми спочатку розбили біграми(5 найчастіших біграм ШТ і рос. мови) на пари уникаючи повторень. Але було трохи складно придумати алгоритм поділу біграм, для зручного відображення результату.

Функція kluchi() втілена для того щоб знайти можливі кандидати на ключ (a, b) для кожної пари шляхом розв'язку системи.
Отримавши всі можливі ключі ми намагаємося розшифрувати ШТ і якщо він проходить перевірку на розпізнавачеві мови, то в консоль виводиться і ключ(пара значень) і ВТ розшифрований цим ключем.

Для перевірки змістовності ВТ було використано такі умови:

1) перевірку частот частих літер «о», «а», «е»
2) перевірку частот рідкісних літер «ф», «щ», «ь»

Отриманий ключ: (390, 10)

Зашифрований текст

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипму
гфбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэ
йкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывдьмиыыяшцрбгянямз
юдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывч
фвэрфешмяояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбш
ящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквк
шятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдх
пезхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглт
доккжшскзыядншууезжурфешщпнзшятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусж
ощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозн
оюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочые
зыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощя
анбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфм
овоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбля
ьхзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссо
жзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрзд
вщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггднотлккжжипеызохл
щпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкб
азущпязхлдырйпоазсяслщяджипщплздджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзш
яцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхя
кзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшя
вжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжш
алтыбжхябжюакцопиышчыдншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюп
лвляешууяхщжпоной кыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзн
шзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряеш
бзкцколппотзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшй
фшщоцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяямзозхьпешьоаоеш
ывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзсккрздвюптжждшсэыпзь
цяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузяб
ряешйкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхезкбйкьосктлсзешь
оекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножяяоьоэмкзшяпдмыэзгпйшууе
шоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзцжжу
щпрфуяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомз
мятыямйшалтыеызоешыедвайнинзшязпкцрфешмяеыцпяовкрфекуяжубждоджгллкпыбжан
цйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшощ
жшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфб
ждоцпюдлвюпюпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмн
щеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмзюдайюдьм
иыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшя
рбптхямзюдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщк
поноюаающяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпокбчфн
одоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшяcжеьзоешрйэжпзжжбяаое
шывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешед
вдвлгфезшйдбряилгфеыхзсккчвкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызо
чбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюнешибряшяякжш

бчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзд
жипщчьоцыыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчко
жцчибзлжозномясктзлзмкжшбчшящкбяйбзбяшждцыцшдзщжэзччамекуяанюзскжуэыощлз
шящжбждояоратлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшуу
эжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекш
вуяджпоьфйказсшлячовунщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйу
фаляятфсчподояоносшншмоешдбждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлц
лыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныл
яыфчбюпповбнзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощк
порфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшншмоешдбждн
шайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопж
ипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчф
юшпфмяяявлвжипюпэышбмунрчфюшьосокыиыхзхпезпыщжмосоыыбжхядамофыюшотдов
кккшяабйчуцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяилщкцжжзщрэысяныбл
оцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгш
ьльфжшншмолдопсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхф
щжщлщяджипбжюпмуяззощуиврймзвожзпофотывдохлцюпядайхпимиыраыжнэюшсйокбя
жярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсы
яхщжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказ
хяанаоешезвжбякбмурфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлц
ечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшкопншфузхпмдьюшш
ящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуя
яоекзожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэ
пбжжущчхябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракбяо
щзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфлцабгяы
овояяфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыыядвзбр
яжзлжипюпоцчбптдохлибвоанаопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяц
яюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгяыкаяшябялбгцабхямз
юдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаое
шезвжпоноймйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвнш
юпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйскпонзшясшмышйсщжшзпсчанбчдайкрзш
яшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшя
анбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщ
чаоешезвжпоноэбкзешдбшярллзджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурф
лцтжбжюууфиыщчскподояоеыщжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюд
ншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномоф
шсжцкгяпзюнамзпеяпыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

Розшифрований текст

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточ
тоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодока
затьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидосто
евскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиунижений осужде
ниедостоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбыл
этознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслу
женногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондал
себянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправ
даниинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжажд
утнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказаниятоткто знаетсл
ожноеиизменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобить
сясмыслаприпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчт
оихпервоначальнаясущностьосталасьнеизменнойнесморянавсепоследующиенаслоениямо

жносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерен
иемубитьотцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсфе
рампокоющимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойонп
ришелкполномуподчинениюбатюшкецарюоднаждыразыгравшемуснимкомедиюубийствав
действительностинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяни
ебольшесвободыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведен
иямондопоследнейминутысвоейжизнивсеколебалсямеждуверойибезбожиемеговысокийум
непозволялемунезамечатьтетрудностиосмысливаниякоторымприводитверавиндивидуаль
номповторениимировогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосв
обождениеотгреховииспользоватьсвоисобственныестраданиячтобыпритязатьнарольхриста
еслионвконечномсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообще
человеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхинд
ивидуальнойсилыинемоглабытьпреодоленадажеговысокойинтеллектуальностьюздесьнас
казалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаип
одвергаемдостоевскогооценкеимеющейправонасуществованиелишьспристрастнойточкизр
енияопределенногомировоззренияконсерваторсталбынаточкузренияявеликогоинквизитора
иоценивалбыдостоевскогоиначеупрекправедливдляегосмягченияможнолишьсказатьчторе
шениедостоевскоговызваноочевиднозатрудненностьюегомышленияявследствиеневрозаедв
алипростойслучайностьюможнообяснитьчтотришедеврамировойлитературывсехвременгр
актуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамаз
овыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззажен
щиныпрямоевсегоконечноэтопредставленовдрамеоснованнойнагреческомсказанииздесьде
яниесовершаетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобработкан
евозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемсяприпсихоанал
изекажетсянепереносимымбезаналитическойподготовкивгреческойдраменеобходимоесмя
гчениеприсохраненииисущностимастерскидостигаетсятемчтобессознательныймотивгерояп
роецируетсявдействительностькакчуждоеемупринуждениенавязанноесудьбойгеройсовер
шаетдеяниенепреднамеренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеоб
стоятельствпринимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторен
иятогожедействиявотношениичудовищасимволизирующегоотцапослетогокакобнаруживае
тсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьеессебявзвалитьеенапринуждение
состоронысудьбынаоборотвинапризнаетсяикаквсецелаявинанаказываетсячторассудкумож
етпоказатьсянесправедливымнопсихологическиабсолютноправильнованглийскойдрамеэто
изображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпо
ступокнеявляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничес
твауженщиныненуждаетсявзавуалированииравноиэдиповкомплексгероямывидимкакбыво
траженномсвететтаккакмывидимлишьтокакоедействиепроизводитнагеропоступокдругого
ондолженбылбызаэтотпоступокотомстительностраннымобразомневсилахэтосделатьмызнаем
чтоегорасслабляетсобственноечувствовинывсоответствииихарактеромневротическихявлен
ийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособностивыполнитьэтоз
аданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивидуальнуюо
нпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэт
омнаправлениироманрусскогописателяуходитнашагдальшеиздесьубийствосовершенодруг
имчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновнимиотношениямикакиг
ероймитрийукоторогомотивсексуальногосоперничестваоткровеннопризнаетсясовершено
другимбратомкоторомукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболез
ньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротиквом
неотцеубийцаивотвречизащитниканасудетажеизвестнаянасмешканадпсихологиейонамолп
алкаодвухконцахзавуалировановеликолепнотаккакстоитвсеэтоперевернутьинаходишьглуб
очайшуюсущностьвосприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасу
дебныйпроцессдознаниясовершеннобезразличноктоэтотпоступоксовершилнасамомделепс
ихологияинтересуетсялишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветс

твовалипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпер
вичнымипозывамиискательнаслажденийполныйскепсисациникиэпилептическийпреступн
иквбратьяхкарамазовыхестьсценаввысшейстепенихарактернаядлядостоевскогоизразговор
асдмитриемстарецпостигаетчтодмитрийноситвсебеготовностькотцеубийствуибросаетсяпе
реднимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойо
тстраняетотсебяискушениеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяиипоэтомупе
реднимсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалеко
выходитзапределысостраданиянакотороенесчастныйимеетправоонанапоминаетблагоговен
иескоторымвдревностиотносилиськэпилептикуидушевнобольномупреступникдлянегопоч
тиспасительвзявшийнасебявинукоторуювдругомслучаенеслибыдругие

Висновки: у ході виконання лабораторної роботи ми навчились працювати з афінним шифром, а саме атаками на нього. Також ми поновили свої знання з модульної арифметики. Створили розпізнавач російської мови для того, щоб відрізнити змістовний текст російською мовою від тексту-шуму, що виникає при неправильному дешифруванні.