Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:
студенти групи ФІ-93
Баєвський К.О.
Шифрін Д. С.

Перевірив:
Чорний О.М.

Київ – 2022

ЗМІСТ

ЗАГАЛЬНІ ВІДОМОСТІ

1. Мета комп’ютерного практикуму

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

2. Постановка задачі

Створити програму для знаходження ключа шифру афінної підстановки та дешифрувати текст за варіантом.

3. Хід 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 алгоритмуЕвкліда, 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 No1, знайти 5 найчастіших біграм запропонованого шифротексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграмшифротексту (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 шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

4. Опис труднощів

Реалізовуючи програмний код, ми зіштовхнулися з проблемою, що при розв‘язку нерівності через неузгодженість алфавіту російської мови з українським алфавітом виникло багато проблем з модулярною арифметикою.

Також в процесі дешифрування ми помітили, що текст непарної довжини. Тому у кінцевому тексті останньою літерою є буква «а», яка не несе ніякого змісту.

ПРАКТИЧНА ЧАСТИНА

1. Найчастіші біграми шифротексту (за варіантом)

Найчастіші біграми:

Біграми	«йа»	«юа»	«чш»	«юд»	«рщ»
Код	279	899	737	903	521

2. Опис роботи автоматичного розпізнавача російської мови

Щоб побудувати розпізнавач, ми рахували сумарну кількість літер «о», «а», «е», потім поділили на кількість літер у тексті і отримали сукупну частоту. Дане значення має бути < 0,22. У нашому ж випадку взято з похибкою (точне значення 0,2256378).

Знаючи правила роботи шифру заміни, букви замінюються на інші і сума частот цих літер буде максимальною тільки в нашій ситуації, оскільки «о», «а», «е» - п’ята частина всього тексту. Для зменшення похибки було розглянуто перевірку в сукупності, а не окремо.

3. Шифрування тексту

Короткий фрагмент роботи програми під час знаходження ключа:

a=93,b=899,

OText=ггэюдазекьфтдиэюиькьхсьшбецтсцунтмюцятлыцнгесицюгишюыйчшцюсеффвцдуоармаймммэмюмицщматийбгщиатшффдцлеи

a=596,b=522,

OText=хвжцыотщыгщдфнжцдгыгоилллщсдвущшцэрурдюяншгщяняцшнццэйчляцйщзыаугатояэмйпэнэйэзущэмдлйювюнмдцыхюабрн

a=525,b=772,

OText=ящшсволцйжптмвшсмжйжедюйфцмтймгкьыцматрфоксциввсювяссртйвсыцвпрмвбтоюылрдылыщызмаыотярвщывотыпоиыньв

a=155,b=31,

OText=биюеиаргеэесолюекэеэждгвагасрзчоюбсзлсакаоьгэлнеблиепшьвнецгямззьяоагбешнбдбсбчзыбшсршжиилшсфмсхжуыл

a=242,b=239,

OText=дэтпчокыабщешктпббабфхпвнышеыгечвихгфегручмывкхпйкфпрщбвхпеывдугхфтогиощеиэимиргоидекщеэюкдеадамлшик

a=27,b=211,

OText=однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтоне определенноеприпадкипроявляющи

Знайдене значення ключа: a=27, b=211

рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджь йахещыйеьеюоэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбу ойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайа экяуклзщюгхегарпинцплпprффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхж укчщысаэарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаюй зхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщбе роюазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылш ошрщышгпфуыуйацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдв ифущлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйд шгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюду шлсбубеюыхрдщндщфщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюе нпчщроюаеймюберояарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжа чойатеащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмш яхукчкйбвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпх ппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшышв амносвиййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкп аюехдсджжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлаш ьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщ йаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешбероюачпщылшыщдшэасуйаьпымку юсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйа цчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричикзддрятарщрою азахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкгхавклая хбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашошзсбужи фчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцрчийщпаюеющч шхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюезлиекдф фыршдчимшлчлэфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебд кйющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаю нежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленксс вссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзс ййымзсхажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэпла хщдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпос щерпусдюйаюдбучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасаза опчичпнхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхева телуцчисхпкучызшцшмейряжпшюешпщьбудшоылшищгамуыщюаешлуьппрринхдщца дуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчу шугрйхпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйкв ыдщлагчмэашзщэиьчщщчшмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечш лжйазакмхйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандусса гшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчн цюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюга рпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикммьл евлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмх

йтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфут
даюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаюьичбзлцчтыкйэщышт
ыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйа
цчтыкйдшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающаш
чопаюебушщькышзшвыйафщышхпцмдрщыыуюехакчщуиезафнщыаччбзстдаюрщлаее
бдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужичлщер
пюабуашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэ
щйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпре
шхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяав
дчишхтаичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсеч
ушгцмпнщьбукаюдуыдщимюдкечушгмщрщашщппрэщкырйдщьлщеющвпьюриюдюаш
дйржахетсййвпэсгпчинаькгшхпннзщццтвкчисжлзсйепртшййыуйаусйрпншдажйазмгьу
сффщлщрбезахемчтэлекмаюрщудеапамдосшсцпфжнлзуыщюазреызшэатдрмхпщьбудш
щыхубвчочпщаэщялчохехалюидвиаммсееапегкажлхехдпрчиилмечшшшцкдщтечшчыз
шэатдрмлэчлрщнаэшэдкйчбйкишугрййкоыдднпрщышлсбубеаунккмнежскгцчтыкйкавй
ыуйаусйрпносфнзвюаиейркезаокйщгаынрйщызюимюдаюаыпмяызшцлгпшгцчтыкйкая
хбмщырйнхкелиачгшшдсдмэшсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфч
бшмейрпныурщгпзхцмчэиорщэаэшшшщрщхезакдььрмьрпнхщшдькюедефщроошкаюрп
ркдчэуырщлхчээпмеидбюхахщимюдюарппьщсрплаэщкаюытэтедщпуэщвкющиулаэиы
йхлллнажахоусиппрсеэщюхыййаькэиеыйееуйафмыущфзщжбглщейеуозсащвашйымюд
хунлищжанарпзючшбуосачиеэдщырйнхюахйщфрпешбероюарущефпкезарчцптддчщфд
щпуэщвкющньйашегахлтейицмрйыезаокнейежпэиэщгэхувлуоыуыщимфмйщпшйрщьй
апахпьююаяофэхувлуолиачйахагаодвимдчитысазшйыжжйажлчпнхыезахаэасачшашйар
окамейецыьпяйхеейыуйаусйрнфйщхлюеерффасхйюдкемдсилэгерпйклижуашрщщейеч
швппршгцчтыкйканущефптачштэрщзщяпэптбьерпимюдкеслщещцримежагекаюрэпьчя
фьеруюсхпымздюлщелшашфьымосьрчифшцкщедеюакайасажлнктешщэилиачгшопьчф
фкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюадуклзщачисюарехеэдпрмэтдавнкхат
ешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифусицлщеомхпипчушгмщр
щашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщроошэщнхльюаэпеямшщевлэ
ияффубелшщфцчтыкйхрмсуювпьюыщдшварчмэчиащварщэщйщчшэийщхатешщчшбу
щефпсдюдисфуидчиеапячщ

4. Розшифрування тексту

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопредел
енноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизн
иприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойс
илыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокруженийимогут
такжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступки
какбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтониказал
осьчистотелеснымипричинамиэтисостояниямогутпервоначальновозникатьпопричинамч
истодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволнени
йкакнихарактернодляогромногобольшинстваслучаевинтеллектуальноеснижениеноизвест
енпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеятель
ностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныил
иподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпр
оизводитьвпечатлениетупостинедоразвитоститкакэтаболезньчастосопряженасярковыр
аженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязательно

йсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияимибыва
ютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинствес
лучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоят
ельствахневозможноустановитьсовокупностьклиническоюаффектаэпилепсииточтопрояв
ляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональногопониман
иякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовлено
рганическимеханизмкоторыйиспользуетсяприналичииивесьмаразныхусловийкакпринару
шениимозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболеваниит
акипринедостаточномконтроледушевнойэкономиикризисномфункционированиидушевно
йэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащегово
сновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессов
порождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмалойэпилеп
сиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотводар
аздраженияэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятоенесо
мненнотакжепоступаетиврапоряжениеневрозасущностькотороговтомчтобыликвидирова
тьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилеп
тическийприпадокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидоиз
меняетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессатак
имобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпрактич
ескоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающийвт
оройневротиквпервомслучаедушевнаяжизньподверженанарушениюизвневовторомслуча
енарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятночтоэпилепсиядост
оевскогоотносится ковторомувидуточнодоказатьэтонельзятаккаквтакомслучаенужнобыло
бывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиевидоизме
нениятихприпадковадляэтогоунаснедостаточноданныхописаниясамихприпадковничего
недаютсведенияосоотношенияхмеждуприпадкамииипереживанияминеполныичастопроти
воречивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевдетствеч
тоонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотрясшегоегоп
ереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылобыве
сьмауместноеслибыоправдалосьточтооноиполностьюпрекратилисьвовремяотбыванияимк
аторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийством
вбратьяхкарамазовыхисудьбойотцадостоевскогобросиласьвглазанеодномубиографудосто
евскогоипослужилаимуказаниемнаизвестноесовременноепсихологическоенаправлениеп
сихоанализтаккакподразумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютрав
муивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначнуобосновыватьэтуус
тановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыу
чениеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпер
выхприпадковдостоевскоговегоюношескиегодызадолгодопоявленияэпилепсииуэтихприп
адковбылоподобиесмертиониназывалисьстрахомсмертиивыражалисьвсостояниилетарги
ческогоснаэтаболезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезо
тчетнаяподавленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудт
обыемупредстоялосейчасжеумеретьивсамомделенаступалосостояниесовершенноподобн
оедействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтем
какзаснутьоставлялзапискичтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтом
учтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестн
ысмыслинамерениетакихприпадковсмертониозначаютотождествлениесумершимчелове
комкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивт
оройслучайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожела

лисмертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеуч
ениеутверждаетчтоэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокяв
ляетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

ВИСНОВКИ

У даній роботі було реалізовано підпрограми для обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда та розв’язання лінійних конгруенцій, які згодом були використані для знаходження кандидатів на ключ (a,b) шифру афінної біграмної підстановки, і, власне, програма для розшифрування тексту.

Ми опанували принцип роботи з моно-алфавітними підстановками, а саме дешифрування та знаходження ключа при відомих значеннях l l-грам.