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:
студентки групи ФІ-94
Зацаренко А. Ю.
Футурська О.В.

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 варінтом.

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 потрібнокоректно обробляти випадок із декількома розв’язками, повертаючи їхусі.

2. За допомогою програми обчислення частот біграм, яка написана в ходівиконаннякомп’ютерного практикуму No1, знайти 5 найчастіших біграмзапропонованогошифротексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграмшифротексту (розглядаючи пари біграм із п’яти найчастіших).Для кожного співставленнязнайти можливі кандидати на ключ(a,b)шляхом розв’язання системи (1).

4. Длякожного кандидата на ключдешифруватишифротекст. Якщошифротекстне є змістовним текстом російською мовою, відкинути цього кандидата.

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

4. Опис труднощів

Реалізовуючи програмний код, ми зіштовхнулися з проблемою, що при повторювані кроків дешифрування текст виходив не змістовним для даної мови. Тому було прийнято рішення змінити кодування алфавіту шляхом побудови автоматичного розпізнавача російської мови (перевірку частот літер «о», «а», «е» в сукупності).

Також в процесі дешифрування ми помітили, що текст не парної 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 дорівнюють: 279, 899, 737, 511, 903.

Відповідно після переведення у літери це такі пари: «йа» «юа» «хц» «рп» «юд».

2. Опис роботи автоматичного розпізнавача російської мови

Для побудови 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 0,23113).

Згідно з правилами 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

Знайдене значення ключа: a=27, b=211

рйрщкагппрфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджь
йахещыйеьеюеэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшб
уойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекай
аэкяуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнх
жукчщысаэарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышка
юйзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэр
щбероюазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвит
ылшошрщышгпфуыуйацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазли
екдвифущлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэ
щйдшгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечш
юдушлсбубеюыхрдщндщфщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпы
мюенпчщроюаеймюбероюарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбх
щжачойатеащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпн
цмшяхукчкйбвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэеш
йарпхппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфк
шышвамносвиййдзырыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфч
гшйкпаюехдсджжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншга
шэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекммьлекдхй
ыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешбероюачпщылшыщдшэасуйаь
пымкуюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзырыщаыпмяызшх
пбьйацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричикзддрятар
щроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкгх
авклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашошз
сбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцрчийщпаю
еющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшщчсдхйыуыщйаудчикабпсаюезли

екдффыршдчимшлчлэфуюаззддрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымю
дкебдкйющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасй
юдаюнежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйл
енкссвссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызш
щфзсййымзсхажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказ
аэплахщдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсе
егпосщерпусдюйаюдбучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууока
йасазаопчичпнхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемч
тэхевателуцчисхпкучызшцшмейряжпшюешпщьбудшоылшищгамуыщюаешлуьпппррин
хдщцадуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцж
йацчушугрйхпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкны
цмйквыдщлагчмэашзщэиьчщщчшмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэр
щмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйас
андуссагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклз
щюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгесаьпюачпжжпш
юечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпропп
рчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйк
аешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэ
дкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаюьичбзлцчты
кйэщыштыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажат
ечшжьйацчтыкйдшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелш
цающашчопаюебушщькышзшвыйафщышхпцмдрщыыуюехакчщуиезафнщыаччбзстда
юрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшсб
ужичлщерпюабуашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэх
шстдаюриэщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэ
жичбзлэпрешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмху
эсдммэтдяавдчишхтаичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабу
осйещеэдсечушгцмпнщьбукаюдуыдщимюдкечушгмщрщашщппрэщкырйдщьлщеющв
пьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщццтвкчисжлзсйепртшййыуйаусйрпн
шдажйазмгьусффщлщрбезахемчтэлекмаюрщудеапамдосшсцпфжнлзуыщюазреызшэат
дрмхпщьбудшщыхубвчочпщаэщялчохехалюидвиаммсееапегкажлхехдпрчиилмечшшш
цкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйкишугрййкоыдднпрщышлсбубеаунккмнеж
скгцчтыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрйщызюимюдаюаыпмяызшцлг
пшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрмфукукчщгчилиачгшзсечмбрмфуэснар
пзючшпмвпфчбшмейрпныурщгпзхцмчэиорщэаэшшщрщхезакдььрмьрпнхщшдькюеде
фщроошкаюрпркдчэуырщлхчээпмеидбюхахщимюдюарппыщсрплаэщкаюытэтедщпуэ
щвкющиулаэиыйхллланажахоусиппрсеэщюхыййаькэиеыйееуйафмыущфзщжбглщейеуо
зсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюахйщфрпешбероюарущефпк
езарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейежпэиэщгэхувлуоыуыщи
мфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчитысазшйыжжйажлчпнхые
захаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасхйюдкемдсилэгерпйк
лижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерпимюдкеслщещцри
межагекаюрэпьчяфьеруюсхпымздюлщелшашфьымосьрчифшцкщедеюакайасажлнктеш
щэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюадуклзщачисюарех
еэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифусицлщ

еомхпипчушгмщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщроошэщнхлььюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюыщдшварчмэчиащварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

4. Розшифрування тексту

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизниприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокруженийимогуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтониказалосьчистотелеснымипричинамиэтисостояниямогутпервоначальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволненийкакнихарактернодляогромногобольшинстваслучаевинтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститкакэтаболезньчастосопряженасярковыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвитиемисклореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональногопониманиякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичииивесьмаразныхусловийкакпринарушениимозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболеваниитакипринедостаточномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотводараздраженияэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятоенесомненнотакжепоступаетивраспоряжениеневрозасущностькотороговтомчтобыликвидироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилептическийприпадокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидоизменяетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессатакимобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпрактическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедушевнаяжизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятночтоэпилепсиядостоевскогоотноситсяковторомувидуточнодоказатьэтонельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиевидоизмененияэтихприпадковадляэтогоунаснедостаточноданныхописаниясамихприпадковничег

онедаютсведенияосоотношенияхмеждуприпадкамиипереживанияминеполныичастопр
отиворечивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевде
тствечтоонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотряс
шегоегопереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепси
ибылобывесьмауместноеслибыоправдалосьточтоониполностьюпрекратилисьвовремяо
тбыванияимкаторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмежд
уотцеубийствомвбратьяхкарамазовыхисудьбойотцадостоевскогобросиласьвглазанеодн
омубиографудостоевскогоипослужилаимуказаниемнаизвестноесовременноепсихологи
ческоенаправлениепсихоанализтаккакподразумеваетсяименноонсклоненвидетьвэтомс
обытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпунктегоневрозаеслия
начнуобосновыватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымд
лявсехтехкомунезнакомыучениеивыраженияпсихоанализаунасодиннадежныйисходны
йпунктнамизвестенсмыслпервыхприпадковдостоевскоговегоюношескиегодызадолгод
опоявленияэпилепсииуэтихприпадковбылоподобиесмертиониназывалисьстрахомсмер
тиивыражалисьвсостоянииелетаргическогоснаэтаболезньнаходилананеговначалекогдао
нбылещемальчикомкаквнезапнаябезотчетнаяподавленностьчувствокаконпозжерассказ
ывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейчасжеумеретьивсамомд
еленаступалосостояниесовершенноподобноедействительнойсмертиегобратандрейрасс
казывалчтофедоружевмолодыегодыпередтемкаказаснутьоставлялзаписькичтобоитсяноч
ьюзаснутьсмертоподобнымсномипроситпоэтомучтобыегопохоронилитолькочерезпять
днейдостоевскийзарулеткойвведениеснамизвестнысмыслинамерениетакихприпадковс
мертиониозначаюттотождествлениесумершимчеловекомкоторыйдействительноумерил
исчеловекомживымещенокоторомумыжелаемсмертивторойслучайболеезначителенпри
падоквуказанномслучаеравноцененнаказаниюмыпожелалисмертидругомутеперьмыста
лисамиэтимдругимисамиумерлитутпсихоаналитическоеучениеутверждаетчтоэтотдруг
ойдлямальчикаобычноотецииименуемыйистериейприпадокявляетсятакимобразомсамон
аказаниемзапожеланиесмертиненавистномуотцуа

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.

При дешифровані шифротекст виявився не змістовним для російської мови. Тому знадбилося побудувати автоматичний розпізнавач мови по принципу перевірки частот частих літер (букви «а» «о» «е» перевірялися в сукупності).