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 5

Виконали:
студенти групи ФБ-93
Приходько Андрій
Шахова Катерина

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.

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 :

У ході роботи було реалізовано всі функції , що передбачались у завданнях. Знайдено 5 біграм , що найчастіше зустрічались у шифр тексті, а саме : ['вн', 'тн', 'дк', 'хщ', 'ун']. Розглядаючи їх разом з найчастішими біграмами відкритого тексту було отримано деяку кількість можливих ключів. Далі для кожного ключа було розшифровано текст. Аналіз тексту проводився за допомогою частотного аналізу літер «о» та «а». Під час лабораторної роботи 1 ми дізналися що у відкритому тексті російською мовою їх частота приблизно дорівнює 0.1 та 0.08 відповідно. Тому поставивши певні рамки для цих частот ми змогли відфільтрувати тексти та знайти той єдиний, що нас цікавить. Ключ (654;777)

Зашифрований текст :

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэммндтихкеюибщыцязкзх
швносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввццтнавпьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэкж
лрибуждэмхимьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкцдзтчщиюцншумщошяьщкщнфрхуюижсгцыз
зфрщихзтчщрихнэпозтгфккчщкдмклыоьеынуййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивупхю
фйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнв
нгоьцэииспьтуумщщшдекхндуаошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьбиши
ыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющькккюиеуяэзтьяяреурндуь
цоэгкмбобмщкскехюксдцтсывзтмсунйькщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбк
фипьйнмсуншснхтуйнццмсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцн
улцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюджкеспьибуб
июхщбуакикяеэдакаоццсвлбеилрлвцофкяяышвнунхщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчса
бьешижсоэосыумщмбриввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнак
дуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбеелфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуа
омнщоццвнфиибхюихтоццсввныклрынпьювюсисцйвнихчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяак
ккйдищжлывьктзихывуллвовявшньсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвацлотнуншн
мстспьицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсчязиьсунуллвихывхдсккл
мщубшскуаохщрнрцязакубсчфкяяосгйршгнгбфдзйьцэибусчжвавмнззфдыоиюшсосюдритьйьнсхщтньцмнрнннстрсосул
лвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшнищюиьсщожсюдгнуцрнчзшрынулцхдвмь
цнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшвнюдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкясп
нззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуццщщцспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвын
уняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожяшсввдуюизбыв
щшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсстгнхщщщфддбтьпнзкьеэдхнщьжвзтфрлцдкяяхьовюсстх
щрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьсцкл
жшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвпьыэмбйнвнцхпнуцязьсйядуулриб
увдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщш
ьавтулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфсчсщьавпьскггыоющлхвиис
пьвиулбутнзцнулцяьжцюсчвввймюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшьявхщеуе
идебупьесузющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищькккффдкфьнхчщмщявисчтжьамаофисрябсчшижслб
убщэнщфдэмсщябубчзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхсовпннчубакак
хуямдкяяхсвнхбжсмкщнщьжвэкссщькккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйны
эвнхбрифкйыунрншьвнбкубьебчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмс
нсибссвддцйнчсщнэпозцфибссщщубссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфп
тнхщыглозфьцэидктнунэибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэир
щввпноулцфрынщхыщмснфжврйвньркзскыщссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввни
щрилвацшвьичдрщдкикгбмщбущстссвйьшвоейулцгйщшфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдф
ишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзищссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролв
тнрицнмскмжяявзтсиюгщхтнмспбмщбущськмюннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцб
уябзщбукзунгэщькккгнввшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньбиулбунхнчйдпнввкцйнуншвэьтн
щоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщбущсфрмщчяовупмюосшнкуаохщмсэкццзтбыыьмнжннуы
фрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихщавиэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкх
юдрошджсюсунынмсйкмбкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамозмщбвскаь
шнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкиющькккбыоскчицпьявицчзивяьочлцсвпдгсуфдкфьяэюдао
рибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяякадункчзжсюсбчкнбквьфзтнуноьюддкнхживналбуыодкеиочоьлхэф
дкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрн
хщбщыцвиклаккзеущнюсияоусчтсйьзтклларццюсстшнюдкшвнгьерынньэьынавэкиютыннькиютноьакеишдщщшвпвмн
дтихжцшнйнюирсыэьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунтсч
тгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпвюскиосыр
ынцэгожсгцмефдфмжяосзкцдзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщцсунхдицяедьакхуумжс
внчрлвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлсиьпвтснфюирыюсцьаккн
ивжошижсмкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяспнчкхуцфюижсшщя
зюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнвввшнмьвврщоз
енйсуньейпфкаьтныоеущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхм
ьакгтмщшджсунлххэхьзтлрэчбудкввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяьклхнгцязвэ
кьзцэиьшсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпьгбубсвйна
вдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкриж
эпншнхщынгспнунрнгошддкяяфсшьыоарфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдк
тнянккбщшдекццжлывйкквэпншнхщынгспныэрнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгс
унмщпвюдцфюирыусунлрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбры
яьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшныйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмк
лытсющшдекццзтиэярчсжвюсстибдцньтсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзццзтвии
ярщьякбньависйщкзхщхуиюшннуяетнхщюиакфккчлспыюпьрцмнрншбынлсюдризьяуфкшдвчскчавзтрщхсщв

Розшифрований текст :

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлосьбыубиватьсамому
этонеоднолишьдоброесостраданиеэтоотождествлениенаоснованииодинаковыхимпульсовкубийствусобственног
оворялишьвминимальнойстепенисмещенныйнарциссизмэтическаяценностьэтойдобротыэтимнеоспаривается мо
жетбытьэтовообщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособенноясноступающи
йвчрезвычайномслучаеобремененногосознаниясвоейвиныписателянетсомнениячтоэтасимпатияпопричинеотож
дествлениярешительноопределилавыборматериаладостоевскогоносначалаонизэгоистическихпобужденийвывод
илобыкновенногопреступникаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопрест
упникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертногонаследияидневн
иковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманиибылобуреваемигорнойстрас
тьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеподдаетсяинойоценкенискакойсто
ронынебылонедостаткавоправданияхэтогостранногоинедостойногоповеденияучувствовиныкакэтонередкобывает
уневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймоготговариватьсятемчтоонпривы
игрышеполучилбывозможностьвернутьсяврассиюизбежавзаключенияятюрьмукредитораминоэтобылтолькопре
длогдостоевскийбылдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналч
тоглавнымбылаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассудногоповедени
яслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготакжесред
ствомсамонаказаниянесчетноеколичествораздавалонмолодойженесловоиличестноесловобольшенеиграть илинеи
гратьвэтотденьионнарушалэтословокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяиее
докрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудовлетворениемонмогпередне
юпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаип
ослевсейэтойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутакк
акзаметилачтотоотчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепродвига
лосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнонепони
малакогдаегочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговорилтогдаисчезалазатрудн
енностьвработетогдаонпозволялсебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодогоп
исателянетрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорнойстрастиустефана
цвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтримастеравсборникесмятениечувствестьн
овелладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываеткакбудтолишьтокакимбезответств
еннымсуществомявляетсяженщинаинакакиеудивительныедлянеесамойзаконо нарушенияеетолкаетнеожиданное
жизненноевпечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобезтако
йоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилискореообщемужскоеита
коетолкованиестольявноподсказаночтонетвозможностиегонедопуститьдлясущностихудожественноготворчеств
ахарактерночтописательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчтоупо
мянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврассказвплетенынекоторыедетал
икакбырассчитанныенаточтобыуказыватьнатайныйследвэтойновеллевеликосветскаяпожилаядамаповеряетписат
елюотомчтоейпришлосьпережитьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейбол
еененуждалисьотказавшаясяоткакихбытонибылонадеждснорокворомгодужизнионапопадаетвовремяодногоиз
своихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредивсехдиковинеевниманиеприковываютдве
рукикоторыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувства
рукиэтирукикрасивогоюношиписательказкбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдающ
ейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпаркепокончитьсосвоеюбез
надежнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвседляегоспасения
онпринимаетеезаоднуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидае
тегоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостель
послеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноео
бещаниечтоонникогдабольшенебудетиграть снабжаетегоденьгаминаобратныйпутьисосвоейстороныдаетобещан
иевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовап
ожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпутешествиевместотого
чтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеона
сноваприходитвигорныйдомисвозмущениемобнаруживаеттамтежерукинаканувевозбудившиевнейтакуюгорячу
юсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещаниииноодержимыйстрастьюонбранитс
орвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокида
етгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивировкен
аписаннаяновеллаимеетконечноправонасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговп
ечатленияоднакопсихоанализучитчтоонавозникланаосновеумопострояемоговожделенияпериодаполовогосозрев
аниякаковомвожделениинекоторыевспоминаютсовершенносознательносогласноумопострояемомувожделению
матьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопасениявредаонанизмастольч
астыесублимирующиехудожественныепроизведенияявытекаютизтогожепервоисточникапороконанизмазамещает
сяпорокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэт
омотводеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивонанизмениодни
мсловомкромесловаигранельзяназватьетееаа

Висновок: виконуючи даний комп’ютерний практикум ми отримали навички аналізу біграмного шифру афінної підстановки. Змогли розшифрувати текст, що був зашифрований даним шифром. Також згадали модульну арифметику та змогли реалізувати функції з цього розділу