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

КРИПТОГРАФІЯ

Лабораторна робота №3

Криптоаналіз афінної біграмної підстановки

Варіант 5

Виконав :
студент фб-91 Єльський Іван

Київ – 2021

Мета роботи

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

Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. 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.
3. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму No1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
4. 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).
5. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
6. Повторювати дії 3 - 4 доти, доки дешифрований текст не буде змістовним.

5 найчастіших біграм в шифртексті
['вн', 'тн', 'дк', 'хщ', 'ун']

Для розпізнавання внятного тексту було використано функцію "avto_rozpiznavach" яка перевіряє чи зустрічається нашому дешифрованом у тексті 5 підряд приголосних або 5 підряд голосних отже якщо в дешифро ваному тексті зустрічається наприклад ' кцртп ' тоді цей текст скоріш за все не вірний і в такому випадку вона повертає значення False якщо ж інакшке тоді True .

Ключ: a = 654, b = 777.

Висновки: під час виконання комп’ютерного практикуму я навчився провидити успішні атаки на шифр афінної підстановки біграм. Крім цього, я поновив теоретичні знання з деяких тем дискретної математики: пригадав як обчислювати обрернений за модулем елемент.

Шифрований текс :

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввн
сдуэммндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддк
ясввццтнавпьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзц
юсфспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсг
цыззфрщихзтчщрихнэпозтгфккчщкдмклыоьеынуййлцяьэрхнмкпмдкйыпоиэуныэнсмн
мсхэццьедктництндуццоэивупхюфйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящисс
бинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшд
екхндуаошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтсп
ьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнб
жжцрнмющькккюиеуяэзтьяяреурндуьцоэгкмбобмщкскехюксдцтсывзтмсунйьксщиссшн
чщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйнмсуншснхту
йнццмсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавоз
улбутнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьй
нвнцхркпрыожврщьянкиюджкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяыш
внунхщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыу
мщмбриввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьа
взтьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбьеелфеипвидий
дкяязщпузобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпь
ювюсисцйвнихчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжл
ывьктзихывуллвовявшньсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшияз
иебчлвацлотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцш
ншвюийдьяшншвосюсчязиьсунуллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгй
рщтнгбфдзйьцэибусчжвавмнззфдыоиюшсосюдритьйьнсхщтньцмнрнннстрсосуллвзтвд
нкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшнищюиьсщожсюд
гнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшвнюдцф
вдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьм
взтьсйядуццщщцспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвын
уняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыц
тнавчзфдыожяшсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщнь
юсстгнхщщщфддбтьпнзкьеэдхнщьжвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйд
ццхифсчсхдййрснсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьс
цклжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпв
пьызмбйнвнцхпнуцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокн
ирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьавтулцибсчннисозфд
ыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфсчсщьавпьскггыою
щлхвииспьвиулбутнзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфии
бкзенуьпьбцрныгщйеуйнзщшьявхщеуеидебупьесузющдкясюэсцэиьцзттнмслдроавежб
щяйрщйуюйлцеищьккффдкфьнхчщмщявисчтжьамаофисрябсчшижслбубщэншфдэмсщя

бубчзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхс
овпннчубакакхуямдкяяхсвнхбжсмкщнщьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсв
ьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьвнбкубьебчсвйнжнд
уеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснсибссвддц
йнчсщнэпозцфибссщщубссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклак
аолржцяьзтхдицфптнхщыглозфьцэидктнунэибунсхщавьвлващеутнищлрдцбщшдыцйнв
нцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпноулцфрынщхыщмснфжврйвньр
кзскыщссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилва
цшвьичдрщдкикгбмщбущстссвйьшвоейулцгйщщфкнхдкбщщйвнихобсчшибщекбщэюн
хзциссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзищссы
ршьудццрреулфщщаефдхссироюовяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнмспб
мщбущськмюннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябз
щбукзунгэщьккгнввшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньбиулбу
нхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщ
бущсфрмщчяовупмюосшнкуаохщмсэкццзтбыыьмнжннуыфрыэиьсфсчсщьавозщсосгйлц
мктзулынйнуйаихщавиэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкх
юдрошджсюсунынмсйкмбкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсун
сццьблшэннбвамозмщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтс
зкиющьккбыоскчицпьявицчзивяьочлцсвпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодунк
ющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьфзтнуноьюддкнхживналбуыодкеиочоь
лхэфдкфыпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщбакксйнбжрисц
вджцмнщькмыгьяьехщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсст
шнюдкшвнгьерынньэьынавэкиютыннькиютноьакеишдщщшвпвмндтихжцшнйнюирсыэ
ьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяф
жсюсунтсчтгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсч
сгэлнцнерссжофкеиябпвистнпвюскиосырынщэгожсгцмефдфмжяосзкццзтпытнрсакьлм
щриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщцсунхдицяедьакхуумжсвнчрлвньзтьяйк
чзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлсиьпвтснф
юирыюсцьаккнивжошижсмкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэи
улбунхмокздцрнфзфпдкяспнчкхуцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиосэщ
ублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнвввввшнмьвврщозенйсуньей
пфкаьтныоеущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлх
чярщтсчтрьйнвнцхмьакггмщшджсунлххэхьзтлрэчбудквввзнввшнжьжврщунынжвжрцци
счцэиаьмчвврщищссркжэжвмндтфрлцяьклхнгцязвэкьзцэиьшсвмдьцюяусиебчдуьешдри
езмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпьгбубсвйнавдьос
пншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжй
внакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшьыоарфдрижлццэччсавпьз
ншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекццжлывйквэпн
шнхщынгспныэрнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьг
сунмщпвюдцфюирыусунлрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьц
эидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщья
шнынйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчс
жвюсстибдцньтсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзцц
зтвииярщьякбньависйщкзхщхуиюшннуяетнхщюиакфккчлспьыопьрцмнрншбынлсюдри
зьяуфкшдвчсксчавзтрщхсщв

Відкритий текст :

убиватьбольшененадопослетогокаконужеубилнаследуетемубытьблагодарныминачеп
ришлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаос
нованииодинаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепен
исмещенныйнарциссизмэтическаяценностьэтойдоброты этимнеоспариваетсяможетбы
тьэтовообщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособенн
ояснопроступающийвчрезвычайномслучаеобремененногосознаниясвоейвиныписател
янетсомнениячтоэтасимпатияпопричинеотождествлениярешительноопределилавыбо
рматериаладостоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновен
ногопреступникаполитическогоирелигиозногопреждечемкконцусвоейжизнивернуться
кпервопреступникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопублико
ваниеегопосмертногонаследияидневниковегоженыяркоосветилоодинэпизодегожизни
товремякогдадостоевскийвгерманиибылобуреваемигорнойстрастьюдостоевскийзарул
еткойявныйприпадокпатологическойстрастикоторыйнеподдаетсяиной оценкенискакой
сторонынебылонедостаткавоправданияхэтогостранногоинедостойногоповедениячувст
вовиныкакэтонередкобываетуневротиковнашлоконкретнуюзаменувобремененностид
олгамиидостоевскиймоготговариватьсятемчтоонпривыигрышеполучилбывозможность
вернутьсявроссиюизбежавзаключениявтюрьмукредитораминоэтобылтолькопредлогд
остоевскийбылдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтом
признатьсяонзналчтоглавнымбылаиграсамапосебевсеподробностиегообусловленного
первичнымипозывамибезрассудногоповедениялужаттомудоказательствомиещекоеч
емуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготакжесредствомсамона
казаниянесчетноеколичествораздавалонмолодойженесловоиличестноесловобольшен
еигратьилинеиграть вэтотденьионнарушалэтословокаконарассказываетпочтивсегдаесл
ионсвоимипроигрышамидоводилсебяиеедокрайнебедственногоположенияэтослужил
одлянегоещеоднимпатологическимудовлетворениемонмогпереднеюпоноситьиунижа
тьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогреш
никаипослевсейэтойразгрузкисовестинаследующийденьиграначиналасьсноваимолода
яженапривыклакэтомуциклутаккаказаметилачтотоотчеговдействительноститолькоимож
нобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшечемпослеп
отеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнонепонима
лакогдаегочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговор
илтогдаисчезалазатрудненностьвработетогдаонпозволялсебесделатьнесколькошаговн
апутикуспехурассматриваярассказболеемолодогописателянетрудноугадатькакиедавно
позабытыедетскиепереживаниянаходятвыявлениявигорнойстрастиустефанацвейгапос
вятившегомеждупрочимдостоевскомуодинизсвоихочерковтримастеравсборникесмяте
ниечувствестьновелладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпока
зываеткакбудтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеу
дивительныедлянеесамойзакононарушенияеетолкаетнеожиданноежизненноевпечатл
ениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднако
безтакойоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечелов
ческоеилискорееобщемужскоеитакоетолкованиестольявноподсказаночтонетвозмож
ностиегонедопуститьдлясущностихудожественноготворчествахарактерночтописательс
которымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчтоупо
мянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврасск
азвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэт

ойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережи
тьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеене
нуждалисьотказавшаясяоткакихбытонибылонадежднасороквторомгодужизнионапопа
даетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногде
средивсехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредст
венностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукик
расивогоюношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосына
наблюдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающего
залчтобывпаркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставля
етженщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаодн
уизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепок
идаетегоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономе
реотеляиразделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитк
азалосьбыуспокоившемусяюношедатьейторжественноеобещаниечтоонникогдабольш
енебудетиграться снабжаетегоденьгаминаобратныйпутьисосвоейстороныдаетобещаниев
стретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуждаетсябольшаянежн
остькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешает
отправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиепомех
изадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприхо
дитвигорныйдомисвозмущениемобнаруживаеттамтежерукинаканувевозбудившиевне
йтакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообе
щаниионодержимыйстрастьюонбранитсорвавшуюегоигрувелитейубиратьсявонишвыр
яетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаетгородавпоследств
ииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивир
овкенаписаннаяновеллаимеетконечноправонасуществованиекактаковаяинеможетнеп
роизвестиначитателябольшоговпечатленияоднакопсихоанализучитчтоонавозникланао
сновеумопострояемоговожделенияпериодаполовогосозреванияокаковомвожделении
некоторыевспоминаютсовершенносознательносогласноумопострояемомувожделени
юматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопа
сениявредаонанизмастольчастыесублимирующиехудожественныепроизведениявытек
аютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрастиударе
ниепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомотв
одеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребно
стивонанизмениоднимсловомкромесловаигранельзяназватьетееаа