Варіант 2

Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут» Фізико-технічний інститут

Компютерний практикум №3

З дисципліни:”Криптографія”

Тема:” Криптоаналіз з афінної біграмної підстановки ”

Перевірила:
Селюх П. В.
_____

Виконали:
студенти III курсу
групи ФБ-95
Корольова В.Р.
групи ФБ-96
Гуменюк О.О.

Варіант 2

Мета:Засвоїти механізм роботи частотного аналізу за умовами Афінного шифру (моноалфавітна підстановка),з освоєнням підтехнік,що грунтуються на прийомах модулярної арифметики.

Постановка задачі: У даному практичному практикумі,досліджуємо процес розифрування афінної підстановки за знаходження пари ключів,через прийоми модулярної арифметики,а саме використовуючи систему рівнянь,за яким якою визначаємо елемент а ,який є парою ключа розшифровування.Отримавши відоме значення а,за рівнянням знаходим в,який є другим елементом з пари ключа розшифровування.За відомими (а,в) -елементами ключа переходимо до розшифрування,яке забезпечується оберненим перетворенням за розширеним алгоритмом Еквкліда**.**При цьому,ми розробляємо розпізнавач тексту,який буде відрізняти випадкові тексти від змістовного тексту ,використовуючі критерії змістовного тексту.Нам відомо,що розшифрування тексту базується на знанні шифротексту,тому в цьому скористаємось частотним аналізом .Адже на афінний шифр покладається статистичні характеристики ,у нашому випадку,російської мови.Тому вважатимемо ,що найбільш вживані біграми ВТ переходять у найбільш вживані біграми ШТ.

Хід роботи:

1. Нажимаємо F5

2. Запускається функція обрахунку всіх можливих варіантів запису 1 2 3 4 5.

3. Записуємо всі можливі варіантні значення ключів, беручі до уваги, що дешифровані завжди йдуть константними,

*приклад

то ен но на ст 1 2 3 4 5

йа юа чш юд рщ 1 2 3 4 5

то ен но на ст 1 2 3 4 5

йа юа чш рщ юд 1 2 3 5 4

і так далі

4. Після цього перебираємо всі отримані ключі на вірогідність біграм, які не можуть часто зустрічатись в російській мові. Ми вважали те,що, якщо у тексті більше ніж 1% “заборонені” біграми, то цей текст нам не підходить.Далі перевіряєм усі тексти на індекс відповідності, і знаходимо бажаний ,той у якого він був між 0,05 до 0,06, що дуже наближено до російської мови.

Проблеми

Труднощі_1:

Коли ми записували з першим елементом біграмку(string), то в map разставляється в порядку алфавіту, а якщо чисел - зростання. Тому була проблема з тим що ми не могли витягнути реальні варіанти, а завжди отримували лише один у порядку алфавіту

ен на но ст то

2 4 3 5 1

або ж якщо першим елементом був інт

1 2 3 4 5

то ен но на ст

Рішення:

Створили мап, на перше місце якого поставили ключ - лічильник, а на друге місце поставили мап з нашими значеннями.

Пять найчастіших біграм шифртексту

-йа

-юа

-чш

-юд

-рщ

Варіант 2

Розпізнавач російської мови:

1.Визначали “заборонені” біграми. Якщо вони зустрічались більш ніж 1% зі всіх(25 біграм у нашому тексті), то ми їх відкидали(мається на увазі тексти з ними).

2.Взяли тексти отримані з 1 пункту і шукали індекси відповідності. Знаходили текст ,який мав індекс від 0.,05 до 0,06 .Тобто знаходимо наш шуканий текст.

ШТ:

щоыкцрылжцьштхъогзцуэцъмщкубфющъуытфьбахсюьувчузюмопощквкъмьчтмусуьшюхуцтрцоэитсуряхяьъыежърцярос
ыотюрщмчщсфьйоыоюыуъоэиъташйдхъьъхефярцйыхявэцьщзхщцыфущкборяэййшдцчмцубжцюхшмяилхэвгшсоьлмтшц
ытъиоуянюбкрширчюгмчфщцшбвъинзьтьтэчшлцциучеутьхаюятужифкчтщььэщявтчлшообцуафъцгепхщумямщмьйэужй
энмдъптрчрмърйюхьпцйыхрувлейжннчщйувфюцмапыэчпьлыюыыцнцйрмйщьтьфььюльйякофахъбъьцьшрэиудыхлвэцю
пнжхмьдщгыроюцлптъхзмйямюгьоаыуцхккящхфряшяцнъышйхшчобьуьщцаьцфебшахщоьупдьнфашпэюбоэшкстэлдазува
цьжцонпйпнтцжэсцькфнщчжямъяэпсохтпнфтьщрхбыцъхдпрфаывчвкрмьэмцфйзашяэщдвнпыщехщъершыяшуцикдхжп
чяэецчшжищбмгуоуэрглпктхйлййообъсоерхкцйшзахтьбуоуыгьчрбюаюяошшнънкъмщмъххтдшнрххйхахщмщьюрмснясц
уткэпегщтйщцпйаийвлцввнхшнцдцфутэхэщлсыцшфулуычанхчтюрфаымурщаяьрдоноуюхпюяъяэепмйчфцшцуьогзкжхяи
уьфцьпмющсстхощрзарфавурямхорькбяяьъэнснчицйряыэчфрцйэччхъхаафщвржйьцнськцяэтхррсыщутъиьвчыылфйюцуу
ьлпаэящцзжыпнчгяоуьбьнфйэннмцшехцлгщьцыщчжущняэттыуххушйюмтбэпяффйюцуьокыгърархйсъвйафьякаскцаьцтр
ощкбсьпэксйъосцфускщяшныгтлчсупхьфыщцухйзштэчуцьуэюухяилдщшнэпецэзйэъчрятьхчяглттпрфтягрбфгяцуиъноуоч
ьвыьцоуииэйсцжбцфыцыехюнсжотяпруьжстоуйышхърщьыйьмщрсзщзъшэямъепюзцдэмяюцюстзйэхьжжпяммаянцйрмй
уюхзхюящаупылсыушшшчяылчапгюттцьчптщкцитуйпжзсшсййррснъщйапчгяьуртаюыхфосотрувбзйяхднщзпшяцюэнлзн
нйыфйесюцчкстфудъмыэкгацнцъиноьщьакъщькфтучсцошюфхсьчяпаойымпющьцоййьцудъфмббуьурмюдляяхгичувэкеш
рштгхфшфысъхморыячуьаэхячзалхчоэмюхяьвзуотбоьокрвэюяфцпысъчъчоъпшсчксъгтпоицачыгшеоэгфмэмюхющцэксъг
ожущршчукрфйэкднятьщвфцшконфоскъфхаацшамытцдхфоъэъмрццтхдрьшшюсяыщитыьсхофьзььфщйтфццдрмсюабэрх
йдхчрьищшжкцъухшннсцуббчщцрсгпглдщпщбоцшьшрэиудрчуръкюжорхшшфнуьтщотутйялохучоапхдчкйящиьуыбцфя
щпкпптщйятуроэягецикйгягявэньъкфтмцмъфбъпшылптъфчзъмыпээцыкихъежулкюьэягкпъишгавчбъьълдсняйпрвгюуцгз
нлюыхфосоъэсхлдчпрнйщюаювацмдсхяозьфуяэщдвейяящихшзхръсцькфсипйымсыотршертхицьййифщщтцчщшйоофояян
эюгмфчицькьбъърнтдюъчгзпчьчюршкхщцмхшчйвлбхузптхсгтзевэацмдчсрлпнмапюьчлрушнадъпышжуфщтйамсжщжув
фяьуийюнщлоььэфааыкуымцйящцьуывйхуэррчымсюрбхрчтршчрывчткпяыдтдницаъфьуэсяшклъизмлщьюрцхшухчирдщку
бфювкйарцщттмдъччрькпъишфьщцттуврхдюучкцтюгщцюлптшнцгглоцфсяцужацшчящцырбхэужднхцьюбтааущздшщлт
мйцэвоюэусвщщтжпчыпсуькзсинтящцупугьзттлчрькбйфягнежъыпсьмрафъръпдфифьуыэющоюрццнхоькубфяуцшкхяицй
жгяшъкюркуытйсушарьуйзцмшдцйуфуюсщспкйедляяущыофукньцудымътъохркьйкдхжмчьпсщросткфйхмжмсьалцсинх
йящогбуткцмяыйъцжбэчшсцбснзыяэхэръэяпусьцхтюацыаншлппмъсйвъоапыгжццнуляяяцьыофщсстйьибюцъмаячшзыгьч
жйутрвацмдйюъехцтофпамюсйтаеймъэапрькчахъчыахалаабюйтщмопотюрькйрчйьнщаымяюааснргтъшфьищхыяыщрачц
ыяэчьскщюльйякофахъбъьцьшрэиудцшцфчжнхеоърлыууыхрйулртъцлтащьзфсяэастыхйщчоэлжцщтлнфчпезщпьодвшхй
йчфцшцуьогзкжхяъоооояюрыщгъттчсдхртауаынлъизцещьпууьлглъиамамщмьйцюцутэстщгсрарцэрдъинйщзуилщцоптьш
слызщуфяцычяунцйяхрбфъщпнтяяытпвыхяошннжнъехнфьбфчилццихйуьуцэпуйзсстхотэваээсянуихъопнсьвэюмффтшлч
иоцьъпасцщгъипмсъщпдцупхчрщопхзюгъкфщгтдхчзыыуаяобутйяэькуооавщнхефйнщськьбпъяьздшикйщзхрсувщсжскох
апаюьыиэууыурйашусфэяьфмэифмрвучхоцэнлчищаучорянхщсуэцшдящктаьгшгртъщтрзарырюумчтмьцтчбучувлстюкйп

Варіант 2

йхтээаущкстkофыхуфсцчртмтшолшпчяряыуцэыфгцтцфяьфшшжеиисоцуфпщщшузнчфтгхпгуугнцйщччсцуоооошщнтчш

хчгрййбзццшкфпифхниьачящотдядожцюлвэрмчксмцыуюзршъцуъузыхзлосьббуъкчйозцмрюуььудъхйчизмэварнянчттрц

хчызбзчаньпдфифзушуачтянупйхчсуцьбъухщздянфаыхтюроуурщыъецйхтэпфхжнтятйлотяпрйгзстхфьыуфцъэръхтщцф

ыотьвщюмнфдьтьжутцъччфрцйэпйжнойтпщгрцйщтссоиоэбцыкуеъищчфпщзфамыкхпнпйыгшшфукрфдвхьэцмашюьфые

шютчншчобщьъоелтъцяуййафхыущдчщсцюпвюбьфыешхрыфцййафхыужяшрцдофсыччвхуръицмгжцбэябрйтяцамщшнт

юубншвыяофулкяфюулджишолшээафтвэежшэфдяхпюшшяыуцчызлоуувщбяъхтхщбйящршчргюхмюъсыушшюыогэхдчю

стымэюухцчкпйзбтатоэуцщхеомччснтрнбьэтежтмосцптюсьъзттяиумпзырькющсжншсдыщуъэъюлчяюъщдгзцчцогръсхяо

хшпгэфэяцеиытштсппавявхнняыщмящэюухцчкпйзкящпхрщюмэауыусъцжэаэряпнцэиъхщмтюсоюукмпгихыжувьугцнжя

шйзулцшсцюжфйэщчсототбьблдлнфоцшзплъоыюйдьцнфьиыхфэбщчйвхсыушшшфыцъупнмумбнуэфпмцусхщфтрзахщяг

мапънхсьншюабжщздягхионуяфтсшчмдхдряфоапяглгэхфлтщфуэчуэкффыясцотевээяонеертирзтжпащъдцхуоцыпчтчшгщ

ВТ:

однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптонеичреьеленноепрвчадкипроявляющиесярезколчрикусьваниемусиливающиесядоопасногодляжизнвчриводящ
егоктяжкомусамокалечениюмогутвсежевнекоторьхслучаяхнедостигатьтакойсильцслабляясьдократкихсцстоянийабсансадобьстричроходящихголовокруженийимогуттакжесменцтысякратк
имвчериодафикогдаболынойсовершаешпуждьеегоприродячцступкикакшьнаходясывовластибессознателыногообуславливаясывобщемкакбьстранноэтониказалцсбпистотелесньмвричинаф
иэтисцстояниямогумчервоначалыновозникатфчичричинатпистодушевньмиспугилимогутвдалынейшемнаходитыйявзависимцстиотдушевньхволненийкакнихарактернодляогромногобольш
инствасллщпаевинтнллектуалыноеснижениеноизвестезчокрайнеймереодинслщпайкогдаэтотнедлгненарушигвьсшейинтнллектуалыной йеятелыностигнлымгольцдругиеслучаивотношениик
отжрьхутверждалосытожесамоененадежньилвчодлежатсомнениюкакислучайсамогодцстоевскоголицастрадающиеэпилепсиеймогутпроизводитывпечатлениетупостинеджразвитоститаккак
эыаболезнбпастосопряженасярковьраженньмидиотизмомикрупнейшифимозговьмидефэкыафинеявляясыконлпнообязатнлыной состав ноппастыюкартиньболезниноэтипрвчадкисовсемисво
имивидоизмененияфишьваютиудрлгихлицулиосполньмдушевньмразвитиефискжреесосверхошьчнаявболышинствеслщпаевнедцсыаточноуправляемойимиаффэктивнцстыхнеудивительыноч
тичриыакихобстоцтнлыствахневозможноусыановитысовокупнцстыклиноп ескоюаффэкыацчилячсиитфптопроявляетсяводнороднцстиуказанньхсимптомовтребуемчовидимомуфункционал
ыногопониманиякакеслишьмеханизманжрмалыноговьсвобожьенишчервичньхпозьвовбьлподготовленорганопескимеханизмкоторьйилчолызуетсшчриналичиивесымаразньхусловийкадчри
нарушениимозговойдеятелыностьчритяжкомзаболеваниитканейилитоксопескодзаболеваниыакипринедцсыаточномконтроледушевнойекономиикризисномфункционированиидушевнобэн
ергиизаэтимразднлениемнадвавидамьчувствуемньентопностымеханизмалежащеговосновевьсвобожденияпервопньпчозьвовэтотмеханизмнедалекиотсексуалыньпчроцессовпорождаемьхвс
воейосноветкоксическиужедревнейшиевюпинаызваликоитусмалойцчилячсиейивидлившполовомактесмяйпениеиадаптациювьсвобожьенияэпилептопескогоотводараздраженияэпилептопес
каяреакцияякаковьфименемможноназватьвсеэтовместевзятоенесомненнотакжепостчнаетивраспоряжениеневрозасущнцстыкотороговтомчтобьликвидироватысоматическимассьраздражени
яскоторьфиневрознеможетсправитысшчсихическиэпилептопескигчрипадоксыановитсцтакимобразомсимптомомистериииеюадщчтируетйяивидоизменяетсшчодобнотомукакэтопроисходит
принжрмалыномтлпениисексуалыногопроцессаыакимобразоммьлчолньжчравомразличаемжргаческуюиаффэктивнуюцчилячсиачрактопескоезначениеэтогоследующеестрадающигчерво
гчжраженболезныюмозгастрадающийвторойневротиквпервомслщпаедушевнаяжизнфчодверженанарушениюизвневоторомслучаенарушениеявляетйявьражениемсамойдушевнойжизнивес
ымаверотночтоэпилепсиядостоевскогоотноситсяковторомувидуточнодоказатыэтонелызяыаккакктакомслщпаенужнобьлобьвклдпитывцелокупнцстыегодушевнойжизниначалопрвчадкови
последующиевидоизменениятихпрвчадковадляэтогоунаснедостатфпноданньхичисаниясафипчрипадковничегонедаютсведенияцсоотношенияпнмеждупрвчадкафивчереживанияфинеполньи
частичротиворечивьвсеговероятнеепредположенилптопрвчадкиначалисьыдцстоевскогоужевдетствечтоонивнюпалехарактеризовалисыболееслашьфисижчтомафиитолыкичцслепотрясшего
егичереживаниянавосемнадцатомгодужизниубийстваотцапринялифжрмуцчилячсиибьлобьвесымауместноеслишьичравдалцсытфптоонвчолностыюпрэкратилисывовремяотбьванияимкатор
гивсибириноэтомнчротиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратыяхкарамазовьхись дгбойотцадостоевскогобрцсиласывглазанеодномубиографьдцстоевскогоипос
лужилаимуказаниемнаизвестноесовременноепсихологопескоенщчравлениепсихоаналиэтаккадчодраяумеваетйяименноонсклоненвидетывэтомсошьтиитягчайшуютравмуивреакциидцстоев
скогонаэтоклдпевойпунктегоневрозаеслияначнуобосновьватыэтуусыановкнчсихоаналитопескиичасаюсычтоокажусынепонятньмдлявсехтехкомунезнакомьучениеивьраженишчсихоанализа
унасодиннадежньйисходньгчунктнафизвестенсмьслпервьхпрвчадковдцстоевскоговгоюноше скиегодьзадоугодичоявленияцчилячсииуэтихпрвчадковбьличодобиесмертиониназьвалисыстра
хомсмертиивьражалисывсостояниилетаргическогцснаэтаболезныынаходиланаеговнюпалэкогдаоншьлещемалычикомкаквнезщчнаябезотчетнаяподавленностбпувствокакоэчозжерассказыва
лсвоемьдругусоловыевутакоекакбьдтошьемнчредстоялцсейчасжеумеретыивсамомднленаступалосостояниесовершенничодобноедействительнойсмертиегобратандрейрассказьвасптофедор
ужевмолоддегодьпередтемкакзаснутыцсыавлялзаписконтобоитйяночыюзаснутысмертоподобньмсномвчросимчоэтомучтобдегопохоронилитолыкочеребчцтыдней дцстоевскийзарулеткойвве
дениеснамизвестньсмьслинамерениетакихпрвчадковсмертионио значаютототожьествлениесумершимчеловекомкотжрьйьействитнлыноумериличпнловэкомживьмещенокоторомумьжелаемсм
ертвтжройслщпайболеезначителезчрипадоквуказанномслучаеравноценнаказаниюмьпожелалисмертидрлгомутячерымьсыалисафиэтимдрлгимисамиумерлитутпсихоаналитическоещпен
иеутверждаетчтоэтотдругойдлямалычикаобвпноотециименуемьйистериейпрвчадокявляетйяыакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Ключ:

(27,211)

Висновок:Було засвоєнно навички шифрування Афінним шифром.За відповідними умовами модулярної арифметики,з використанням можливості визначення правильної пари ключів,яку ми отримали ,застосувавши конструкцію розпізнавача змістовного тексту.