«Криптографія»

Комп’ютерний практикум №3

«Криптоаналіз афінної біграмної підстановки»

Варіант 10

Виконали:

Студенти групи ФБ-01

Оліферчук Владислав

Корабельський Тарас

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

Хід роботи

1. Відбувається зчитування зашифрованого тексту

2. Ділення шифрованого тексту на біграми

3. Виділення 5 найчастіших біграм

4. Розрахунок числових значень для кожної біграми всього тексту

5. Визначення можливих перестановок популярних біграм з тексту

із популярними біграмами з мови;

6. Знаходження комбінацій пар біграм та складення системи

порівнянь;

7. Розрахунок ключів для кожної комбінація та виділення унікальних

8. Розшифрування тексту з кожним ключем і перевірка тексту на

наявність недопустимих біграм

9. Відкидання ключів, у яких а = 0

10. Маємо один вірний ключ, яким розшифровуємо текст

11. Розшифрований текст записуємо у файл result.txt

12. Вручну перевіряємо текст на змістовність.

Наш ключ = (300, 400)

Розшифрований текст:

поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябылоразглядетьвремяотвременионвосклицалагаилииэтотожезначитемувголовуприходилоещечтонибудьподходящеедляегоспискапотомдверьчутьстукнулаточновсеткуотмоскитовудариласьночнаябабочкалинашепнулауфманонаселарядомснимнакачеливоднойночнойсорочкенетоненькаякаксемнадцатилетняядевочкакоторуюещенелюбятинетолстаякакпятидесятилетняяженщинакоторуюуженелюбятноскладнаяикрепкаяименнотакаякакнадотаковыженщинывовсякомвозрастееслионилюбимыонабылаудивительнаяеетелокакиегособственноевсегдадумалозанеетолькоподругомуоновынашивалодетейиливходиловпередилеовкаждуюкомнатучтобынеуловимоизменитьтамсамыйвоздухподстатьнастроениюмужаказалосьонаникогданезадумываетсянадолгомысльтотчаспередаваласьотееголовыплечампальцамипретворяласьвдействиетакнезаметноиестественночтолеонесмогбыдаинехотелизобразитьэтокакимилибочертежамиэтамашинасказалаонанаконецненужнаонанамдаотозвалсяонноиногданужнопозаботитьсяиодругихявотвседумаючтотудавставитькинокартинырадиоприемникистереоскопическиеочкиеслисобратьвсеэтовместевсякийчеловекпощупаетулыбнетсяискажетдадаэтоиестьсчастьесочинитьтакуюхитруюмеханикудумалончтопускайучеловекапромоклиногиилиноетязваилиегомучаетбессонницаионворочаетсявпостеливсюночьнапролетидушуегогрызутзаботыавсеравнотвоямашинадастемусчастьекактамагическаякрупинкасоличтоброшенавокеанивечнорождаетсольиобратилавсеморевсолянойрастворктонерасшибсябывлепешкулишьбыизобреститакуюмашинупустьемуответитнаэтотвопросцелыймирпустьответитвесьгородокпустьответитженалинасмущенномолчаласидярядомснимнакачеляхиеемолчаниеговорилояснеевсякихсловлеотожеумолкзапрокинулголовуислушалкаксвищетветервгустойлиствемогучеговязанезабывайговорилонсебеиэтотшелестлистьевтоженужендлятвоеймашинычерезминутуверандаопустелапустыекачелинеподвижноповисливтемнотедедушкаулыбнулсявоснеонпочувствовалэтуулыбкуудивилсяейипроснулсяполежалнемногоприслушалсяксебеипонялоткудаонавзяласьибоонуслышалнечтогораздоболееважноенежелипениептицилишелестмолодойлиствыкаждыйгоднаступалденькогдаонвоттакпросыпалсяиждалэтогозвукакоторыйозначалчтотеперьтоужлетоначалосьпонастоящемуононачиналосьвотвтакоеутрокогдактонибудьиздомочадцевилигостейплемянниксыниливнуквыходилналужайкуподегоокномиметаллическиеножииспицыкружаизвеняподушистойлетнейтравеприлежнообегалиеепокраямнасевернавостокнаюгназападописываявсеменьшиеименьшиеквадратыкосилказвонкострекоталаизподножейбрызгалиголовкиклевераредкиезолотыеискрыуцелевшихпослесбораодуванчиковмуравьипалочкикамешкиостаткипрошлогоднегопразднованиячетвертогоиюляобгорелыешутихиикусочкитрутаноглавноезанейстлалсяпрохладныйчистыйпотоксочнойзеленойтравыдедушкеужепредставлялоськаконащекочетегоногиохлаждаетразгоряченноелицонаполняетноздриизвечнымароматомвновьродившегосялетаиобещаетдамывсевсепроживемещецелыйгодвеликоечудокосилкаговорилсебедедушкакакойэтодураквыдумалчтоновыйгодначинаетсяпервогоянварянадобылопоставитьдозорныхкараулитьросттравынамиллионахлужаекиллинойсаогайоилиайовыикакзаметятчтоонасозреладлясенокосавтосамоеутровместофейерверковфанфарикриковпустьначинаетсявеликаябурнаясимфониякосилоксрезающихсвежиетравынанеобятныхлуговыхпросторахвтотединственныйденьвгодукоторыйпонастоящемузнаменуетсобойначалолюдямнадобыбросатьдругвдруганеконфеттиинесерпантинапригоршнисвежескошеннойтравыдедушкахмыкнулчтотоужбольнодолгуюфилософиюразвелвсталподошелкокнуивысунулсявласковыйсолнечныйсветтакиестьфорестерновыйжилецмолодойгазетчиккакраззаканчиваетряддоброеутромистерсполдингтакеехорошенькобиллсжаромкрикнулдедушкаивскореужесиделвнизуиуплеталприготовленныйбабушкойзавтракширокоеокнобылораскрытоижужжаньекосилкисловноподпевалозавтракуотэтойкосилкинадушестановитсяспокойнеезаметилдедушкатытолькопослушайтеперьужнедолгонамееслушатьотозваласьбабушкаипоставиланастолгоркупшеничныхлепешекбиллфорестерпосеетсегодняновыйсорттравыеененадобудеткоситьнепомнюкактамонаназываетсяноонакаквырастетскольконужнотаксамаиостановитсяибольшенерастетдедушкасизумлениемуставилсянаженудовольноглупаяшуткасказалоннаконецидипосмотрисамбиллфорестерговоритэтоземленапользусказалабабушкаонужепривезновыесеменаонисложенызадомомвмаленькихкорзинкахнужновразныхместахвырытьямкиизасыпатьтудасеменакконцугодановаятраваубьетвсюстаруюитогдаможешьпродаватьсвоюкосилкуонатебебольшенепонадобитсядедушкасорвалсясостулаимигомвыскочилводворбиллфорестеростановилкосилкуижмурясьотсолнцасулыбкойподошелкнемувоттактосказалонвчеракупилновыесеменадайдумаюзасеювамлужайкупокаясвободенаменяпочемунеспросилилужайкатовсетакимоязакричалдедушкаядумалвыбудетедовольнымистерсполдингничегоянедоволенпокажитемнеэтучертовутравуонистояливозлемаленькихчетырехугольныхкорзиноксновомоднымисеменамидедушкаподозрительнопотыкалоднуизнихноскомбашмакапомоемуэтосамаяобыкновеннаятраваавыуверенычтовасненадулиявкалифорниивиделкаконарастетвотнастольковырастетивсееслитолькоонаприживетсявздешнемклиматенамуженабудущийгоднепридетсякаждуюнеделюподстригатьлужайкувтомтоибедасвашимпоколениемсказалдедушкамнестыднозавасбиллаещежурналиствыготовыуничтожитьвсечтоестьнасветехорошеготолькобытратитьпоменьшевременипоменьшетрудавотчеговыдобиваетесьоннепочтительнопнулкорзинкуногойвотпоживетесмоетогдапойметечтомелкиерадостикудаважнеекрупныхраноутромповеснепрогулятьсяпешкомневпримерлучшечемкатитьвосемьдесятмильвсамомроскошномавтомобилеазнаетепочемупотомучтовсевокругблагоухаетвсерастетицвететкогдаидешьпешкоместьвремяоглядетьсявокругзаметитьсамуюмалуюкрасотуяпонимаюсейчасвамхочетсяохватитьвсесразуиэтонаверноестественноэтосвойствомолодостиногазетчикунадоуметьвидетьимелкийвинограданетолькоогромныеарбузывамподавайцелыйскелетасменядовольноиследапальцевчтожтожепонятносейчасмелочикажутсявамскучныминоможетвыпростоещенезнаетеимценынеумеетенаходитьвнихвкусдайвамволювыбыиздализаконобустранениивсехмелкихделвсехмелочейнотогдавамнечегобылобыделатьвперерывемеждубольшимиделамиипришлосьбыдоисступленияпридумыватьсебезанятиечтобынесойтисуматакужлучшепоучилисьбыкоечемуусамойприродыподстригатьтравуивыпалыватьсорнякитожеоднаизрадостейжизнисынокбиллфорестерласковоулыбнулсястарикузнаюзнаюсказалдедушкаястановлюсьслишкомболтливымвжизниникогонеслушалстакимудовольствиемтогдапродолжимлекциюкустсиренилучшеорхидейиодуванчикитожеичертополохапочемудапотомучтоонихотьненадолгоотвлекаютчеловекауводятегоотлюдейигородазаставляютпопотетьивозвращаютснебесназемлюиужкогдатывесьтутиниктотебенемешаетхотьненадолгоостаешьсянаединессамимсобойиначинаешьдуматьодинбезпостороннейпомощикогдакопаешьсявсадусамоевремяпофилософствоватьниктообэтомнедогадываетсяниктотебянеобвиняетниктоинезнаетничегоатыстановишьсязаправскимфилософомэдакийплатонсредипионовсократкоторыйсамсебевыращиваетцикутутотктотащитнаспинепосвоейлужайкемешокнавозасродниатласуукоторогонаплечахвращаетсяземнойшарсэмюэлсполдингэсквайрсказалоднаждыкопаяземлюпокопайсяусебявдушевертителопастиэтойкосилкибиллидаороситвасживительнаяструяфонтанаюностилекцияоконченакрометогоизредкаоченьпользительноотведатьзелениодуванчиковавыдавноелизеленьодуванчиковнаужинсэрнебудемуточнятьбиллкивнулилегонькостукнулближайшуюкорзинкуноскомбашмакатаквотнасчетэтойтравыяещеневсевамсказалонарастеттакгусточтонаверняказаглушитиклевериодуванчикигосподипомилуйзначитуженабудущийгодмыостанемсябезвинаизодуванчиковиниоднойпчелынадлужайкойдавыпростосумасошлипослушайтескольковызаплатилизаэтисеменадолларкорзинкаякупилдесятьштуквамвподарокдедушкаполезвкарманвытащилстаромодныйдлинныйкошелекотстегнулсеребрянуюзастежкуиизвлектрибумажкипопятьдолларовбиллвытолькочтосовершилипревыгоднуюсделкузаработалипятьдолларовизвольтесейчасжеотправитьвсюэтучересчурпрозаическуютравувоврагнапомойкусловомкудахотитетолькопокорнейшепрошунесейтеееуменяводвореязнаюувассамыепохвальныенамеренияноявсетакиужедостигвесьмапочтенноговозрастаисмоимижеланияминегрехсчитатьсявпервуюочередьаа