Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙПРАКТИКУМ№3

Криптоаналіз афінної біграмної підстановки.

Варіант–21

Виконали:

студенти III курсу

ФТІ

групи ФБ82

Ясинський Нікіта
Владислав Кравчук

Перевірили:

ЧорнийО.М

.

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

5 найчастіших біграм зашифрованого тексту:

№	Біграма
1	фт
2	йо
3	дт
4	дж
5	шж

Значення ключів і індекси відповідності для текстів, що були розшифровані з цими ключами

Ключ	Індекс
867 590	0.03992884066758933
767 130	0.03926089412457515
245 804	0.040673143832266404
855 727	0.04013384290739052
674 471	0.039611308347335304
90 91	0.058523150698247095

Відомо, що індекс збігів для російської мови має бути більшим за **0.055**.

Тоді шукані ключі:
a=90,b=91

Шифрований текст:

йтпоухшхшжкумь пышжаяэояниищюсжфят цхйгеч оле цйь юджбдьтэхнэокоыыт пйцшфтвцфт рк
ктдмоцрхтввойтпоухшоапкйдгютыерюэмфчалщхиэьшгоаошырхичфтьтупаюдтщюркаюкюжь
чышхзцфтйоонзбркктпгэюшннжьшщюляч ыпябтщюркаюфедтыюкюжтпйцшоым цпчзорйыжа
фхюгюнтщюйоуыйхжйуюаюмюмосххэусуыаякуьбаюмьпыаяаяхюыюшефгпйрчэчшжюсфяфт
рюжтуюфхкйгещюатркктпгэюшнфтоннтнжьшсжщьыпьшыцботсфяфтрюииоешекхшжкуленж
еоондтзяюхжешелшжштфэчзмкыншдтгтютфмйхчгайыеютйомоыявеютаюыктекйщлхюшегср
хжмрфафдпьтмеякыюшенюокгмчидтщьрюухюопогюдйрчмтрчэощехетчжйсхнэйтпоуховдтте
гсдтцгяитеихапйелтоеаюефчыэчюжппьтджэбокоыццфтншйозтяоньежкетчжйсхшжеьчыиииин
нтфтьтщйьмосгыйхшжкуаяаяйозтяоньежкетчжйсхйхутэхеьчыиииннтфтьтртеоглншиежтлцуы
эчрямьфяфлзкшлпчтвкоктлоыемойжучпекйщь щхдтджвепйыфхюншвофтчтообхядэйжтпхэчя
доыйлугпхлетчжйсхядмооецейойтпоухшххьчыиииннпоцяиэгокотентиеэоэсююйоцчэчажлиппэ
ййхлкзчмооецейодтйтпоухейкйфтррядяигсдтгтяиоотщэйпобхнэчтясрхщхевпйьмосйхдбхзгелт
щфйхэчвжппьтджэбокоышхцшафаюдмиэгсажюсфяфтрюужаяяогюкхцшйлйждмевгентмсохл
швйонсжбтбхцшйлйжнтмсэчшжяпнжьшмцфтиэеоктиеухэйкйфтжыэчфтвцфтркпоуешнютфтц
гсжмишжбттеютщгьюшееоинсецпнжьшмцфтщювжгсуыбттеютьмшжкыкымцреыфгсвйжтови
еухрхафаюгхжоокоыжзкюйозтщыппйеэжхсфяфтрюкпнжьшмцфтюхпчхсуыоцфтюхрхжйьшйо
бхдпчыиилкмьпыхсовджфещоондтютпоухьсьбпйсэатэюяхиэьтджэчнэюхмьпыцпчыиилкйоют
фтцгсжмихйкюэыжыцпьтщышжфчшжфьчышхядйтонзолцхйшночаоэхюолододжыюммясвжн
жркдшгыыцнчджфещопозпнжьшмцфтммяслкшчюржйрчосичгыэйччэюктьячыоцжйрчщхбтте
ютпоухххэтюэгсншххлепьеллкркшедмоцрхппыццшнчэоессоджкешгпгоштеокленыч цажуыпч
змйллегтмодпшжзегыктуюыкютфтцгсжбттеусэчпорчзмжырхрюпйрчщхдтупнжаожхкйгейтон
дтяечдеозыльрриэйтонугтттеусэчпорчзмжыажтвловхтвкоктлоколятвютьмхьдтджрхоселзкщю
щьпоюцщхшоютьмхьдтджэйыцнчджфеюееоыжуышхкйгентфтвклеьпежфчсопцуыэчряжтммц
шшйьмосйхдбюхггатыйжжтлбшефтмччцдтлцуыэччцжйнтыижшйждтмчаооочяшчнюзтупгм
жтрксхтвотфшапнжаожхкйгеютпцоаошнфтмоджфянжзмжопумыподтаооодтэгннйжибажнжью
алхьелажммеяншшжгмрхмхпяхсьбфтптсжщьюоцгютнокты юшецпнжгмшейтондтцшжйфтшо
цгеоаюйжибпоюцряафхюйтондтцшжйфтютьмюжкыцпшщуыядьмхьщхфяйолойепцфткьйкы
шховрещецгжмоврерогтйорккттюмясджйпышыцбогтйтшерхоселхющющьпоюцщхшопчямфл

щхшочтфгпйрчдбтжэчаочбгюзшшжижаощогтрехябгщочюяжы фгсфяфтрюцымхшжкумыпыцп
чыиилкщовцфтюхлщуыэчгывещосымыщьрглолбкц фтэолц хйдмтвеощояошеэгкодйииоерчтмя
ююйэгиюкжряаежтънмосхтмкьонэолнймпчщхютьтхяэчцпкыйыччлтьтзоиннтдязмщьыцтошоя
ошеютьтхяюзгейодмцшщхдткоаошсыюьюнютегюкххьчы щулейомоинзошгеорчнжыючхтвжт
еодмрхншшжфьчышхэбсжйлхььсуыгыэйюхофрюэеймяархгяаяркюхэйзтьмуырххйаюшгяжщд
огпхшжкуохоцы фюхапаогпйетеэюфояошеркйоркктвжиэмечдонютьюнюкпажмбщофы щхпяа
ффячмрхтвнтлыйжыепчэоопгсьтжхкйщошляитедмясменюбхнэатщжзмышчтаыфсшжпянжзм
юочтджичьбктмюфбгелеюжьущхшоцыптумщлщднежцщджьтяоэйктцхворкшевжцпрюфеаю
щоцгщорещоонйохыпысьбфякгпюуриэеоктгюжьыпгмщхкйкыймяайтпоухейжтовчдчезттсыщ
гмшояошеркюхйоухгысжжоцгджпеаюыкибуекгаыовйтпоухшхшжкувесжбтбхапйлгывощодо
ыкибацфтркщсуы шжбоупчызицояошеркюхйоухгысжжояошеюхй хапдпрюфеюйптбхапйлгыв
ощодоыкибуеютлоыощоиилфрютечгажшщсуысоияюхжешелшюояошеркюхйон шуыжт ршй
лдтджщмхйлячифчшжяпгсьтжхкйгенжьшгюзшйжпчбожауыпочхапюхжыйюфмяиютфбшецг
жмэчюруымцзодпаоеошегьчыиииинсжщььсуыгылфрюэефбелуымыштщюйозтщыьедтесхйчтйе
шнибрьчышхтвщюкюзоыи шжыцфтюхй хшчютзхжйщьчдхюйждмясменютетсфяфтрючсаятент
есйхшчдиатътлоьуьфэчзмкымтщюмюатнюатыиеьфчэбучжогтаоелуыажххххьусьуейщгчюшни
батщжзмьейожтммцштпйетеэюшнпогюдйрчэчясшхуызинуюжажжзгеьяафхююжхьйшйлйжщ
суышжейтпйоашюхдбгтжтйеаюймяархюейпьтяидтзотеюзфтгтйоютфбсхафюхясьбйоэтэхтвоы
эчмтщющлщхбэгскыеьчыщужоюжьущхшосжщььсуыгыхйюхфояошеркоховйорккгрюатдждт
гтчтухйхдбфтгтсжбтщюйорюшсшчгыхйижйедтуегоцчжоммцшссьбфтгтсжщьсьежшхлфнжэч
леыпчыфбшнтжыцдтджпчэодмясменютессфяфтрюоцфтюхшжапгмшхжймесхыцхсьбфтгтсжщ
ьххапьтнгджажщцхйфчнтфтвкщхосгсичшжхшгыэчаоэхюомечдшеяицгктфтдтдязмщьыцыехюяо
нюзтнхшжкурянжзмэблтебтфэчзмкызц фттегюыеуырятмджыюйонкпоьющолесжэчэовжафщг
ютджвеоврккгрюатдждтфееошнсжгсьбйоясуыгыажаядхафдпйлгмрчэчйхевсжжонхосщыпыэч
яилоджлкчцхйыпйетеэюшнпогюдйрчьехюяооврюатдждтрккгфтсжбтщюдмщххьаошююеыпч
ыйотецшдмясменюбхафьшафаюютгююкыюшнсжбтщюйолойерчпокотелейоатьтиеюйжтовие
ухйдатщжзмииоеюяфлзктсщхэрфпгыгонбйзтьмуыьимярхэтпмнрэбгхн шй хдбщювокьажжош
еитсггеуййонхмишжфяафхююхнклтоежчжмрфядптдхшжрфрюэефбютыпьудтнклтоеаюмютех
еюхдмрхншэбэояниилкмчхсцпфязцпчэбмюпгвцпчафчыэчтвгтжтйеец фтлтебшоджытуюфхк й
шнюхщюеойжибщюеощйрчшовжафдпкйпоэхы фчырятмджыюоц фтщюатысшжкеютсшнжаош
нсжщьчыиииинйтонзокмичджлобхэбдтймяархшйкюрюшйейумежжзфтчп кйдгютнтюйхьюенж
атщжзмиччтнкыюающшнчкгэгцткгфтяепйгяеврюайьйютнтщхлкэю

Розшифрований текст:

болезньнаташибылатаксерьезначтоксчастиюееиксчастиюродныхмысльовсемтомчтобылопри
чинойееболезниеепоступокиразрывсженихомперешлинавторойпланонабылатакбольначтонел
ьзябылодуматьотомнасколькоонабылавиноватавовсемслучившемсятогдакаконанееланеспала
заметнохуделакашлялаибылакакдаваличувствоватьдокторавопасностинадобылодуматьтольк
оотомчтобыпомочьейдоктораездиликнаташеиотдельноиконсилиумамиговорилимногопофран
цузскипонемецкииполатыниосуждалиодиндругогопрописывалисамыеразнообразныелекарст
ваотвсехимизвестныхболезнейнониодномуизнихнеприходилавголовутапростаямысльчтоимн
еможетбытьизвестнаболезнькоторойстрадаланаташакакнеможетбытьизвестнаниоднаболез
нькоторойодержимживойчеловекибокаждыйживойчеловекимеетсвоиособенностиивсегдаиме
етособеннуюисвоюновуюсложнуюнеизвестнуюмедицинеболезньнеболезньлегкихпеченикож
исердцанервовитдзаписанныхвмедициненоболезньсостоящуюизодногоизбесчисленныхсоеди
ненийвстраданияхэтихоргановэтапростаямысльнемоглаприходитьдокторамтакжекакнеможет
прийтиколдунумысльчтооннеможетколдоватьпотомучтоихделожизнисостояловтомчтобылеч
итьпотомучтозатоониполучалиденьгиипотомучтонаэтоделоонипотратилилучшиегодысвоейж
изниноглавноемысльэтанемоглаприйтидокторампотомучтоонивиделичтоонинесомненнополе
зныибылидействительнополезныдлявсехдомашнихростовыхонибылиполезныпотомучтозас
тавлялипроглатыватьбольнуюбольшейчастьювредныевеществавредэтотбылмалочувствителе
нпотомучтовредныевеществадавалисьвмаломколичествеоониполезныпеобходимыпеизбежн
ыбылипричинапочемувсегдаестьибудутмнимыеизлечителиворожеигомеопатыиаллопаты пото
мучтоониудовлетворялинравственнойпотребностибольнойилюдейлюбящихбольнуюониудов
летворялитойвечнойчеловеческойпотребностинадеждыпаоблегчениепотребностисочувствия
идеятельностикоторыеиспытываетчеловеквовремястраданияониудовлетворялитойвечнойчел
овеческойзаметнойвребенкевсамойпервобытнойформепотребностипотеретьтоместокотороеу

шибленоребенокубьетсяитотчасжебежитврукиматеринянькидлятогочтобыемупоцеловалиипо
терлибольноеместоиемуделаетсялегчекогдабольноеместопотрутилипоцелуютребенокневерит
чтобыусильнейшихимудрейшихегонебылосредствпом очьегоболиинадежданаоблегчениеивы
ражениесочувствиявтовремякакматьтретегошишкуутешаютегодокторадлянаташибылиполезн
ытемчтооницеловалиитерлибобоуверяячтосейчаспройдетежеликучерсездитварбатскуюаптек
уивозьметнарубльсемьгривенпорошковипилюльвхорошенькойкоробочкеиежелипорошкиэти
непременночерездвачасаникакнебольшеинеменьшебудетвтварнойводеприниматьбольнаячт
ожебыделалисоняграфиграфинякакбыонисмотрелинаслабуютающуюнаташуничегонепредпр
инимаяежелибынебылоэтихпилюльпочасампитьятеплекогокуриной котлеткиивсехпод робн
остейжизнипредписанныхдокторомсоблюдатькоторыесоставлялозанятиеиутешениедляокруж
ающихчемстрожеисложнеебылиэтиправилатемутешительнеебылодляокружающихделокакбы
переносилграфболезньсвоейлюбимойдочериежелибыоннезналчтоемустоилатысячирублейбо
лезньнаташиичтооннепожалеетещетысяччтобысделатьейпользуежелибыоннезналчтоежелион
анепоправитсяоннепожалеетещетысячиповезетеезаграницуитамсделаетконсилиумыежелибы
оннеимелвозможностирассказывать подробностиотомкакметивьеифеллернепонялиафризпоня
лимудровещелучшеопределилболезньчтобыделалаграфиняежелибыонанемоглаиногдассорит
ьсясбольнойнаташейзаточтоонанеполнесоблюдает предписанийдоктораэдакникогданевыздо
ровеешьговорилаоназадосадойзабываясвоегореежелитынебудешьслушатьсядоктораиневовре
мяприниматьлекарствоведьнельзяшутитьэтимкогдаутебяможетсделатьсяпневмонияговорила
графиняивпроизношенииэтогонепонятногонедлянееоднойсловаонауженаходилабольшоеуте
шениечтобыделаласоняежелибыунейнебылорадостногосознаниятогочтоонанераздевалась три
ночипервоевремядлятогочтобыбытьнаготовеисполнятьвточностивсепредписаниядоктораичт
оонатеперьнеспитночидлятогочтобынепропуститьчасывкоторыенадодаватьмаловредныепил
юлииззолотойкоробочкидажесамойнаташекотораяхотяиговорилачтоникакиелекарстваневыле
чатееичтовсеэтоглупостииейбылорадостновидетьчтодлянееделалитакмногопожертвованийчт
оейнадобыловизвестныечасыприниматьлекарстваидажеейрадостнобылоточтоонапренебрегая
исполнениемпредписанногомоглапоказыватьчтоонаневеритвлечениеинедорожитсвоейжизнь
юдокторездилкаждыйденьщупалпульссмотрелязыкинеобращаявниманиянаееубитоелицошут
илснейнозатокогдаонвыходилвдругуюкомнатуграфиняпоспешновыходилазанимионпринима
ясерьезныйвидипокачиваязадумчивоголовойговорилчтохотяиестьопасностьоннадеетсянадей
ствиеэтогопоследнеголекарстваичтонадождатьипосмотретьчтоболезньбольшенравственнаян
ографинястараясьскрытьэтотпоступокотсебяиотдокторавсовывалаемуврукузолотойивсякийр
азуспокоенныма

Висновки:

В ході виконання комп. практикуму було отримано навички роботи із частотним аналізом на прикладі шифру афінної біграмної підстановки. У коді використовується розпізнавач російської мови, що побудований на перевірці індексу відповідності. В результаті виконання роботи отримано ВТ, а також пару ключів А= 90, Б= 91 (розв'язок системи лінійних рівнянь ШТ та ВТ).