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

ЛАБОРАТОРНА РОБОТА №3

З дисципліни«Криптографія»

Криптоаналіз афінної біграмної підстановки

Виконав:

студент 3 курсу ФТІ

групи ФБ-82
Ясинський Нікіта

Кравчук Владислав

Перевірив:

Чорний О. М.

Київ – 2020

Варіант №21

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 (1).

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.

Результат виконання роботи:

5 найчастіших біграм шифрованого тексту: то, ст, но, на, ен.
Ключ шифру: (a = 90, b = 91)
Для визначення коректності розшифрованого тексту було використано два методи: підрахунок заборонених біграм та частот букв в тексті.

Шифрований текст:

йтпоухшхшжкумьпышжаяэояниищюсжфятцхйгечолецйьюджбдьтэхнэокоытпйцшфтвцфтрк
ктдмоцрхтввойтпоухшоапкйдгютыерюэмфчалщхиэьшгоаошырхичфтьтупаюдтщюркаюкюжь
чышхзцфтйоонзбрккттпгэюшннжьшщюлячыпябтщюркаюфедтыюкюжтпйцшоымцпчзорйыжа
фхюгюнтщюйоуыйхжйуюаюмюмосххэусуыаякуьбаюмьпыаяаяхюыюшефгпйрчэчшжюсфяфт
рюжтуюфхкйгещюатрккттпгэюшнфтоннтнжьшсжщьыпьшыцботсфяфтрюииоешекхшжкуленж
еоондтзяюхжешелшжштфэчзмкынщдтгтютфмйхчгайыеютйомоыявеютаюыктекйщлхюшегср
хжмрфафдпьтмеякыюшенюокгмчидтщьрюухюопогюдйрчмтрчэощехетчжйсхнэйтпоуховдтте
гсдтцгяитеихапйелтоеаюефчыэчюжппьтджэбокоыццфтншйозтяоньежкетчжйсхшжеьчыииин
нтфтьтщйьмосгыйхшжкуаяаяйозтяоньежкетчжйсхйхутэхеьчыииннтфтьтртеоглншиежтлцуы
эчрямьфяфлзкшлпчтвкоктлоыемойжучпекйщьщхдтджвепйыфхюншвофтчтообхядэйжтпхэчя
доыйлугпхлетчжйсхядмооецейойтпоухшххьчыииинпоцяиэгокотентиеэоэсюююйоцчэчажлиппэ
йийхлкзчмооецейодтйтпоухейкйфтррядяигсдтгтяиоотцэйпобхнэчтясрхщхевпйьмосйхдбхзгелт
щфйхэчвжппьтджэбокоышхцшафаюдмиэгсажюсфяфтрюужаяяогюкхцшйлйждмевгентмсохл
швйонсжбтбхцшйлйжнтмсэчшжяпнжьшмцфтиэеоктиеухэйкйфтжыэчфтвцфтркпоуешнютфтц
гсжмишжбттеютщгьюшееоинсецпнжьшмцфтщювжгсуыбттеютьмшжкыкымцреыфгсвйжтови
еухрхафаюгхжоокоыжзкюйозтщыппйеэжхсфяфтрюкпнжьшмцфтюхпчхсуыоцфтюхрхжйьшйо
бхдпчыиилкмьпыхсовджфещоондтютпоухьсьбпйсэатэюяхиэьтджэчнэюхмьпыцпчыиилкйоют
фтцгсжмихйкюэыжыцпьтщышжфчшжфьчышхядйтонзолцхйшночаоэхюолододжыюммясвжн
жркдшгыыцнчджфещопозпнжьшмцфтммяслкшчюржйрчосичгыэйччэюктьячыоцжйрчщхбтте
ютпоухххэтюэгсншххлепьеллкркшедмоцрхппыццшнчэоессоджкешгпгоштеокленычцажуыпч
змйллегтмодпшжзегыктуюыкютфтцгсжбттеусэчпорчзмжырхрюпйрчщхдтупнжаожхкйгейтон
дтяечдеозылььрриэйтонугттттеусэчпорчзмжыажтвловхтвкоктлоколятвютьмхьдтджрхоселзкщю
щьпоюощщхшоютьмхьдтджэйыцнчджфеюееоыжуышхкйгентфтвклеьпежфчсопцуыэчряжтммц
шшйьмосйхдбюхггатэыйжжтлбшефтмччцдтлцуыэччцжйнтыижшйждтмчаооочяшчнюзтупгм
жтрксхтвотфшапнжаожхкйгеютщоаошнфтмоджфянжзмжопумьподтаооодтэгннйжибажнжью
алхьелажммеяншшжгмрхмхпяхсьбфтггтсжщьюоцгютноктыюшецпнжгмшейтондтцшжйфтшо
цгеоаюйжибпоюцряафхюйтондтцшжйфтюютьмюжкыцпшщуыядьмхьщхфяйолойепцфтркьйкы
шховрещецгжмоврерогтйоркктюмясджйпьшыцбогтйтшерхоселхюющюоцьпоюццхшопчямфл

щхшочтфгпйрчдбтжэчаочбгюзшшжижаощогтрехябгщочюяжы фгсфяфтрюцымхшжкумьпыцп
чыиилкщовцфтюхлщуыэчгывещосымьщьрглолбкц фтэолщ хйдмтвеощояошеэгкодйииоерчтмя
ююйэгиюкжряаежтьнмосхтмкьонэолнймпчщхютьтхяэчцпкыйыччлтьтзоиннтдязмщьыцтошоя
ошеютьтхяюзгейодмцшщхдткоаошсыюьюнютегюкххьчы щулейомоинзошгеорчнжыючхтвжт
еодмрхншшжфьчышхэбсжйлхььсуыгыэйюхофрюэеймяархгяаяркюхэйзтьмуырххйаюшгяжщд
огпхшжкуохоцы фюхапаогпйетеэюфояошеркйорккттвжиэмечдонютьюнюкпажмбщофы щхпяа
ффячмрхтвнтлыйжыепчэоопгсьтжхкйщошляитедмясменюбхнэатщжзмьшчтаыфсшжпянжзм
юочтджичьбктмюфбгелеюжьущхшоцыптумщлщднежццшджьтяоэйктцхворкшевжцпрюфеаю
щоцгщорещоонйохьпыгсьбфякгпюуриэеоктгюжьыпгмщхкйкыймяайтпоухейжтовчдчезттсыц
гмшояошеркюхйоухгысжжоцгджпеаюыкибуекгаыовйтпоухшхшжкувесжбтбхапйлгывощодо
ыкибацфтркщсуы шжбоупчызицояошеркюхйоухгысжжояошеюхй хапдпрюфеюйптбхапйлгыв
ощодоыкибуеютлоыощоиилфрютечгажжшщсуысоияюхжешелшюояошеркюхйон шуыжтршй
лдтджщмхйлячифчшжяпгсьтжхкйгенжьшгюзшйжпчбожауыпочхапюхжыйюфмяиютфбшецг
жмэчюруымцзодпаоеошегьчыиииинсжщььсуыгылфрюэефбелуымьштщюйозтщыьедтесхйчтйе
шнибрьчышхтвщюкюзоыи шжыцфтюхй хшчютзхжйщьчдхюйждмясменютетсфяфтрючсаятент
есйхшчдиатьтлоьуьфэчзмкымтщюмюатнюатыиеьфчэбучжогтаоелуыажхххьусьуейщгчюшни
батщжзмьейожтммцштпйетеэюшнпогюдйрчэчясшхуызинуюжажжзгеьяафхююжхьйшйлйжщ
суышжейтпйоашюхдбгтжтйеаюймяархюейпьтяидтзотеюзфтгтйоютфбсхафюхясьбйоэтэхтвоы
эчмтщющлщхбэгскыеьчыщужоюжьущхшосжщььсуыгыхйюхфояошеркоховйорккгрюатдждт
гтчтухйхдбфтгтсжбтщюйорюшсшчгыхйижйедтуегоцчжоммцшссьбфтгтсжщьсьежшхлфнжэч
леьпчыфбшнтжыцдтджпчэодмясменютессфяфтрюоцфтюхшжапгмшхжймесхыцхсьбфтгтсжщ
ьххапьтнгджажццхйфчнтфтвкщхосгсичшжхшгыэчаоэхюомечдшеяицгктфтдязмщьыцыехюяо
нюзтнхшжкуряижзмэблтебтфэчзмкызц фттегюыеуырятмджыюйонкпоьющолесжэчэовжафщг
ютджвеоврккгрюатдждтфееошнсжгсьбйоясуыгыажаядхафдпйлгмрчэчйхевсжжонхосщьпыэч
яилоджлкчцхйыпйетеэюшнпогюдйрчьехюяооврюатдждтркктфтсжбтщюдмщххьаошююеьпч
ыйотецшдмясменюбхафьшафаюютгююкыюшнсжбтщюйолойерчпокотелейоатьтиеюйжтовие
ухйдатщжзмииоеюяфлзктсщхэрфпгынгонбйзтьмуыьимярхэтпмнрэбгхн шй хдбщювокьажжош
еитсггеуййонхмишжфяафхююхнклтоежчжмрфяднтдхшжрфрюэефбютьпьудтнклтоеаюмютех
еюхдмрхншэбэояниилкмчхсцпфязцпчэбмюпгвцпчафчыэчтвгтжтйеец фтлтебшоджытуюфхкй
шнюхщюеойжибщюеощйрчшовжафдпкйпоэхы фчырятмджыюоц фтщюатысшжкеютсшнжаош
нсжщьчыииинйтонзокмичджлобхэбдтймяархшйкюрюшйейумежжзфтчп кйдгютнтюйхьюенж
атщжзмиччтнкыюаюцшнчкгэгцтктфтяепйгяеврюайьйютнтщхлкэю

Розшифрований текст:

болезньнаташибылатаксерьезначтоксчастиюееиксчастиюродныхмысльовсемтомчтобылопри
чинойееболезниеепоступокиразрывсженихомперешлинавторойпланонабылатакбольначтонел
ьзябылодуматьотомнаскольккоонабылавиноватавовсемслучившемсятогдакакконанееланеспала
заметнохуделакашляла ибылакакдаваличувствоватьдоктора вопасности надобылодуматьтольк
оотомчтобыпомочьейдокторае здиликнаташеиотдельноиконсилиумамиговорилимногопофран
цузскипонемецкиипалатыниосуждалиодиндругогопрописывалисамыеразнообразныелекарст
ваотвсехимизвестныхболезнейнониодномуизнихнеприходилавголовутапростаямысльчтоимн
еможетбытьизвестнаболезнькоторойстрадалаташакакнеможетбытьизвестнаниоднаболез
ньюкоторойодержимживойчеловекибокаждыйживойчеловекимеетсвоиособенностиивсегдаиме
етособеннуюисвоюновуюсложнуюнеизвестнуюмедицинеболезньнеболезньлегкихпеченикож
исердцанервовитдзаписанныхвмедициненоболезньсостоящуюизодногоизбесчисленныхсоеди
нений встраданияхэтихоргановэтапростаямысльнемоглаприходитьдокторамтакжекакнеможет
прийтиколдунумысльчтооннеможетколдоватьпотомучтоихделожизнисостояловтомчтобылеч
итьпотомучтозатоониполучалиденьгиипотомучтонаэтоделоонипотратилилучшиегодысвоейж
изниноглавноемысльэтанемоглаприйтидокторампотомучтоонивиделичтоонинесомненнополе
зныибылидействительнополезныдлявсехдомашнихростовыхонибылиполезныенепотомучтозас
тавлялипроглатыватьбольнуюбольшейчастьювредныевеществавредэтотбылмалочувствителе
нпотомучтовредныевеществадавалисьвмаломколичествеоониполезныенеобходимыенеизбежн
ыбылипричинапочемувсегдаестьибудутмнимыеизлечителиворожеигомеопатыиаллопатыпото
мучтоониудовлетворялинравственнойпотребностибольнойилюдейлюбящихбольнуюониудов
летворялитойвечнойчеловеческойпотребностинадеждынаоблегчениепотребностисочувствия
идеятельностикоторыеиспытываетчеловеквовремястраданияониудовлетворялитойвечнойчел
овеческойзаметнойвребенкевсамойпервобытнойформепотребностипотеретьтоместокотороеу

шибленоребенокубьетсяитотчасжебежитврукиматеринянькидлятогочтобыемупоцеловалиипо
терлибольноеместоиемуделаетсялегчекогдабольноеместопотрутилипоцелуютребенокневерит
чтобыусильнейшихимудрейшихегонебылосредствпомочьегоболиинадежданоблегчениеивы
ражениесочувствиявтовремякакматьтретегошишкуутешаютегодокторадлянаташибылиполезн
ытемчтооницеловалиитерлибобоуверяячтосейчаспройдетежеликучерсездитварбатскуюаптек
уивозьметнарубльсемьгривенпорошковипилюльвхорошенькойкоробочкеиежелипорошкиэти
непременночерездвачасаникакнебольшеинеменьшебудетвотварнойводеприниматьбольнаячт
ожебыделалисонягрофигрофиняка кбыонисмотрелинаслабуютающуюнаташуничегонепредпр
инимаяежелибынебылоэтихпилюльпочасампитьятеплекогокуринойкотлеткиивсехподробн
остейжизнипредписанныхдокторомсоблюдатькоторыесоставлялозанятиеиутешениедляокруж
ающихчемстрожеисложнеебылиэтиправилатемутешительнеебылодляокружающихделокакбы
переносилграфболезньсвоейлюбимойдочериежелибыоннезналчтоемустоилатысячирублейбо
лезньнаташиичтооннепожалеетещетысяччтобысделатьейпользуежелибыоннезналчтоежелион
анепоправитсяоннепожалеетещетысячиповезетеезаграницуитамсделаетконсилиумыежелибы
оннеимелвозможностирассказыватьподробностиотомкакметивьеифеллернепонялиафризпоня
лимудровещелучшеопределилболезньчтобыделалаграфиняежелибыонанемогланиогдассорит
ьсясбольнойнаташейзаточтоонанеполнесоблюдаетпредписанийдокторазэдакникогданевыздо
ровеешьговорилаоназдосадойзабываясвоегореежелитынебудешьслушатьсядоктораиневовре
мяприниматьлекарствоведьнельзяшутитьэтимкогдаутебяможетсделатьсяпневмонияговорила
графиняивпроизношенииэтогонепонятногонедлянееодноесловаонауженачодилаболь шоеуте
шениечтобыделаласоняежелибыунейнебылорадостногосознанияэтогочтоонанераздевалась3три
ночипервоевремядлятогочтобыбытьнаготовеисполнятьвточностивсепредписаниядоктораичт
оонатеперьнеспитночидлятогочтобынепропуститьчасывкоторыенадодаватьмаловредныепил
юлииззолотойкоробочкидажесамойнаташекотораяхотяиговорилачтоникакиелекарстваневыле
чатееичтовсеэтоглупостииейбылорадостновидетьчтодлянееделалитакмногопожертвованийчт
оейнадобыловизвестныечасыприниматьлекарстваидажеейрадостнобылоточтоонапренебрегая
исполнениемпредписанногомоглапоказыватьчтоонаневеритвлечениеинедорожитсвоейжизнь
юдокторездилкаждыйденьщупалпульссмотрелязыкинеобращаявниманиянаееубитоелицошут
илснейнозатокогдаонвыходилвдругуюкомнатуграфиняпоспешновыходилазанимионпринима
ясерьезныйвидипокачиваязадумчивоголовойговорилчтохотяиестьопасностьоннадеетсянадей
ствиеэтогопоследнеголекарстваичтонадождатьипосмотретьчтоболезньбольшенравственнаян
ографинястараясьскрытьэтотпоступокотсебяиотдокторавсовывалаемуврукузолотойивсякийр
азсуспокоенныма

Висновки: під час виконання практичної роботи №3 я отримав навички моноалфавітної підстановки. Навчився розшифровувати текст зашифрований афінною підстановкою. На практиці навчився визначати некоректний відкритий текст.