НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комп’ютерний практикум
з дисципліни
«КРИПТОГРАФІЯ»
Лабораторна №3

Виконав: ФБ-06 Березовський,
ФБ-06 Іванілов Ігор

Перевірив:

Київ – 2022

Мета роботи

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

Хід роботи

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).

За допомогою написаних функцій знайшли 5 найчастіших біграм у шифротексті.

[('хк', 135), ('ек', 103), ('ху', 94), ('дп', 93), ('вх', 92)]

Перше це біграмма, друге це кількість її появ в тексті.За допомогою цієї інформації ми можемо перейти до подальшого дешифрування.
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 змістовим текстом російською мовою, відкинути цього кандидата. 5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Для перевірки змістовності зашифрованого тексту ми взяли умову, що ентропія не меньша за 4.2, та не більше за 4.5.

Для цього була написана функція яка підбирає ключі як (a,b) та перевіряє їх змістовність за умовою. При виконанні умови виводить текст за записує його у файл.

У самій функції для поліпшення роботи ми спочатку створюємо перший елемент ключа, і якщо він через деякі причини не утворився то ми пропускаємо цей цикл й ідемо до слідуючого. Потім створюємо другий параметр та перевіряємо наш розшифрований ключом текст на змістовність.

Ключ який я отримав: (555, 331)

Розшифрований текст

когдапожарныеисоседиушлилеоауфманосталсясдедушкойсполдингомдугласомитомомв
сеонизадумчивосмотрелинадогорающиеостаткигаражалеоткнулногойвмокруюзолуимед

ленновысказалточтолежалонадушепервоечтоузнаешьвжизниэточтотыдуракпоследнеечт
оузнаешьэточтотывсетотждуракмногоепередумалязаодинтолькочасисказалсебедаведьт
ыслепойлеоауфманхотитеувидатьнастоящуюмашинусчастьяееизобрелитысячилеттомун
азадионавсеещеработаетневсегдаодинаковохорошонетновсетакиработаетионавсевремяз
десьапожарначалбылодугласдаконечнопожаргаражнолинаправадолгораздумыватьнадэт
имнезачемточтосгореловгараженеимеетникакогоотношениякссчастьюонподнялсяпоступ
енямкрыльцаипоманилихзасобойвотшепнуллеоауфманпосмотритевокнотишесейчасвыв
сеувидитедедушкасполдингдугласитомнерешительнозаглянуливбольшоеокновыходивш
еенаулицуитамвтепломсветелампыониувиделиточтохотелимпоказатьлеоауфманвстолов
ойзамаленькимстоликомсаулимаршаллигралившахматыребекканакрываластолкужинун
оэмивырезалаизбумагиплатьядлясвоихкуколрутрисовалаакварельюджозефпускалпорел
ьсамзаводнойпаровоздверьвкухнюбылаоткрытатамвоблакепаралинаауфманвынималаиз
духовкидымящуюсякастрюлюсжаркимвсерукивселицажилиидвигалисьиззастеколчутьс
лышнодоносилисьголосактотозвонкораспевалпеснюпахлосвежимхлебомияснобылочто
этосамыйнастоящийхлебкоторыйсейчаснамажутнастоящиммаслomтутбыловсечтонадои
всеэтоживоенеподдельноеедедушкадугласитомобернулисьипогляделиналеоауфманаатот
неотрывносмотрелвокноирозовыйотсветлампылежалнаеголиценуконечнобормоталонэт
ооносамоеиестьспервастихойгрустьюпотомсживымудовольствиеминаконецсоспокойны
модобрениемонследилкакдвижутсяцепляютсядругзадругаостанавливаютсяивновьувере
нноировновертятсявсевинтикииколесикиегодомашнегоочагамашинасчастьясказалонма
шинасчастьячерезминутуегоуженебылоподокномдедушкадугласитомвиделикаконзахло
поталвдометопоправитчтонибудьтопередвинеттоскладкуразгладиттопылинкусдуеттако
йжеделовитыйвинтикбольшойудивительнойбесконечнотонкойвечнотаинственнойвечно
движущейсямашиныапотомнепереставаяулыбатьсяонispустилисьскрыльцавпрохладну
юлетнююночьдваразавгодводворвыносилибольшиехлопающиековрыирасстилалиихнал
ужайкегдеонибылисовсемнекместуиказалиськакимитонеобитаемымипотомиздомавыхо
дилимамаибабушкаврукахонинесликакбудтоспинкикрасивыхплетеныхкреселчтостоятв
паркеупавильонасгазированнойводойкаждомувручалитакойжезлсширокойплетенойвер
хушкойивседугластомбабушкапрабабушкаимамастановилисьвкружокнадпыльнымиузор
амистаройарменииточносборищеведьмидомовыхзатемпознакупрабабушкиедваонамигн
етилиподожметгубывсевскидывалицепыипринималисьбезпередышкимолотитьковрыво
ттебевотприговаривалапрабабушкабейтеблохмальчикинежалейтеившейнучтотытакоего
воришьукоризненнозамечалаейбабушкавсесмеялисьвокругбушевалапыльнаябуряисмех
переходилвкашельвихрикорпииструипесказолотистыехлопьятрубочноготабакавзвивали
сьввоздухитрепеталиподбрасываемыевсеновымииновымиударамиостанавливаясьчтобы
передохнутьмальчикивиделисследысвоихбашмаковибашмаковвзрослыхтысячуразотпеча
тавшиесянаузорахковравосточныйрисуноктоисчезалтопоявлялсявновьвместесмернымп
рибоемударовчтоомывалегоберегаваттуттвоймужпролилкофеибабушкаударилапоковруа
здесьтыпролиласметануипрабабушкавыбилаизковраогромныйстолбпылисмотритетутве
сьворсвытоптанахребятаребятаавотчернилапрабабушкаглупостиуменячернилалиловые
аэтообыкновенныесиниехлоппосмотритекакуюдорожкупротопталиэтоизприхожейвкух
нюохужэтаедаонадажельвовведетнаводопойдавайтекаповернемегодругимбокомаможет
простозаперетьвседвериникогоневпускатьилипустьразуваютсяещевприхожейхлопхло
пнаконецковрыразвешанынаверевкахтомразглядываетузорхитроумныепетлиипереплет

ыцветыкакиетозагадочныефигурыразводыизмеящиесялиниитомтычтостоишьвыбивайза
нятновсетакивидетьвсякиевещиговориттомдугласподозрительносмотритнанегочтотыта
мувиделдавесьгородлюдейдомавотинашдомхлопнашаулицахлопавонточерноеоврагхлоп
вотшколахлопавотэтачуднаязакорючкатыдугхлопвотпрабабушкабабушкамамахлопсколь
кожелетпролежалунасэтотковерпятнадцатьицелыхпятнадцатьлетпонемутопалидажевид
ныотпечаткибашмаковахнултомсилентыболтатьпареньсказалапрабабушкатутвидновсеч
тослучилосьунасвдомезапятнадцатьлетхлопконечноэтовсепрошлоеноямогуибудущееув
идатьвотсейчасзажмурюсьапотомрразпогляжунаэтиразводыисразуувижугдемызавтрабу
демходитьибегатьдугласпересталразмахиватьвыбивалкойачтоещетытамвидишьглавным
образомниткивставилапрабабушкатуттолькоиосталасьоднаосновасразувиднокакеготкал
ивернозагадочносказалтомвэтусторонуниткиивтутожеявсевижучертирогатыегрешники
вадухорошаяпогодаиплохаяпрогулкипраздничныеобедыземляничныепирыонсважнымв
идомтыкалвыбивалкойтоводнотовдругоеместоковрадапотвоемувыходитчтоядержутутка
койтопансионсказалабабушкавсякраснаяизапыхавшаясятутвсевиднохотьинеоченьяснод
угтынагниголовунабокизажмурьодинглазтольконесовсемконечноночьювиднолучшеког
даковервкомнатеилампагоритивообщетогдатенибываютсамыеразныекривыеикосыесвет
лыеитемныеивиднокакниткиразбегаютсяввовсесторонынощупаешьворспогладишьаонка
кшкуракакогонибудьзверяипахнеткакпустыняправдаправдажаройпахнетипескомнаверн
отакпахнеткаменныйгробгдележитмумиясмотривидишькрасноепятноэтогоритмашинас
частьяпростокетчупскакоготосандвичасказаламаманетмашинасчастьявозразилдугласие
мусталогрустночтоитутонагоритонтакнадеялсяналеоауфманаужунеготовсепойдеткакна
доонвсехзаставитулыбатьсяикаждыйразкогдаземляповернувшисьотсолнцанакренитсякч
ернымбезднамвселеннойманенькийгироскопкоторыйсидитудугласагдетовнутристанетп
оворачиватьксолнцуивотлеоауфманчтототампрошляпилиосталасьтолькокучказолыдапе
плахлопхлопдуглассссилойударилвыбивалкойсмотритевотзеленыйэлектрическийавтомо
бильчикмиссфернмиссробертасказалтомбиипбиипхлопвсерассмеялисьаволттвоилинииж
изнидугонивсевузлахслишкоммногокислыхяблокисоленыеогурцыпередсномкоторыегде
закричалдугласвсматриваясьвузорковравотэтачерезгодэтачерездвааэтачерезтричетыреи
пятьлетхлоппроволочнаявыбивалказашипелаточнозмеяавотэтанавсюостальнуюжизньск
азалтомонударилпоковрустакойсилойчтовсяпыльпятитысячстолетийрвануласьизпотряс
еннойтканинамгновеньезамерлаввоздухеипокадугласстоялзажмурясьистаралсяхотьчтон
ибудьразглядетьвпереплетающихсянитяхипестрыхразводахковралавинаармянскойпыли
беззвучнообрушиласьнанегоинавекипогреблаегонаглазахувсехродныхстараямиссисбент
лиисаманемоглабысказатькарвсеэтоначалосьоначастовиделадетейвбакалейнойлавкеточ
номошкиилиобезьянкимелькалионисредикочановкапустыисвязокбанановионаулыбалас
ьимониулыбалисьвответмиссисбентливиделакаконибегаютзимойпоснегуоставляянане
мследыкаквдыхаютосеннийдымнаулицахакогдацветутяблонистряхиваютсплечоблакаду
шистыхлепестковноонаникогдаихнебоялась домунеевобразцовомпорядкекаждаямелочь
насвоемпривычномместеполывсегдачистовыметеныпровизияаккуратнозаготовленавпро
кшляпныебулавкиводкнутывподушечкиящикикомодавспальнедоверхунабитывсякойвс
ячинойчтонакопиласьзадолгиегодымиссисбентлибылаженщинабережливаяунеехранили
сьстарыебилетытеатральныепрограммыобрывкикружевшарфикижелезнодорожныепере
садочныебилетысловомвсеприметыисвидетельствааедолгойжизниуменякучапластинокг
оворилаонавоткарузоэтобыловньюйоркевдевятьсотшестнадцатоммнетогдабылошестьде

сятиджонбылещеживавотджунмунэтокажетсядевятьсотдвадцатьчетвертыйгодджонтоль
кочтоумертеперьзапахсухогосенаиплескводынапоминалиемукакхорошобылоспатьнасве
жемсеневпустомсараепозадиодинокойфермывсторонеотшумныхдорогподсеньюстаринн
ойветряноймельницыкрыльякоторойтихопоскрипывалинадголовойсловноотсчитываяпр
олетающиегодылежатьбыопятькактотдавсюночьнасеновалеприслушиваяськшорохузвер
ьковинасекомыхкшелестулистьевктончайшимелеслышнымночнымзвукампоздновечеро
мдумалонемубытьможетпослышатсяшагионприподниметсяисядетшагизатихнутонснов
аляжетистанетглядетьвокошкосеновалаиувидиткакодинзадругимпогаснутогнивдомике
фермераидевушкаюнаяипрекраснаясядетутемногоокнаистанетрасчесыватькосуеетрудн
обудетразглядетьноеелицонапомнитемулицотойдевушкикоторуюонзналкогдатовдалеко
митеперьужебезвозвратноушедшемпрошломлицодевушкиумевшейрадоватьсядождюне
уязвимойдляогненныхсветляковзнавшейочемговоритодуванчикеслиимпотеретьподподб
ородкомдевушкаотойдетотокнапотомопятьпоявитсянаверхувсвоейзалитойлуннымсвето
мкомнаткеивнимаяголосусмертиподревреактивныхсамолетовраздирающихнебенадвоед
осамогогоризонтаонмонтэгбудетлежатьвсвоемнадежномубежищенасеновалеисмотреть
какудивительныенезнакомыеемузвездытихоуходятзакрайнебаотступаяпереднежнымсве
томзариутромоннепочувствуетусталостихотявсюночьоннесомкнетглазивсюночьнагубах
егобудетиграть улыбкатеплыйзапахсенаивсеувиденноеиуслышанноевночнойтишипослу
житдлянегосамымлучшимотдыхомавнизуулестницыегобудетожидатьещеоднасовсемуж
еневероятнаярадостьоносторожноспуститсяссеновалаосвещенныйрозовымсветомранне
гоутраполныйдокраевощущениемпрелестиземногосуществованияивдругзамретнаместе
увидевэтомаленькоечудопотомнаклонитсяикоснетсяегорукойуподножьялестницыонуви
дитстаканхолоднымсвежиммолокомнесколькояблокигрушэтовсечтоемутеперьнужнодо
казательствотогочтоогромныймирготовпринятьегоидатьемувремяподуматьнадвсемнадч
емондолженподуматьстаканмолокаяблокогрушаонвышелизводыберегринулсянанегокак
огромнаяволнаприбоятемнотаиэтанезнакомаяемуместностьимиллионыневедомыхзапах
овнесомыхпрохладнымледенящиммокроетеловетромвсеэторазомнавалилосьнамонтэга
онотпрянулназадотэтойтемнотызапаховзвуковвушахшумелоголовакружиласьзвездылет
елиемунавстречукакогненныеметеорыемузахотелосьсноваброситьсяврекуипустьволны
несутеговсеравнокудатемнаягромадабереганапомнилаемутотслучайизегодетскихлетког
дакупаясьонбылсбитсногогромнойволнойсамойбольшойкакуюонкогдалибовиделонаогл
ушилаегоишвырнулавзеленуютемнотунаполниларотносжелудоксоленожгучейводойсли
шкоммноговодыатутбылослишкоммногоземлиивнезапновотьместеноювставшейпередн
имшорохчьятотеньдваглазасловносаманочьвдругглянулананегословнолесгляделнанегом
еханическийпесстолькопробежатьтакизмучитьсячутьнеутонутьзабратьсятакдалекостол
ькоперенестиикогдаужесчитаешьсебявбезопасностиисовздохомоблегченияивыходишьна
конецнаберегвдругпередтобоймеханическийпесизгорламонтэгавырвалсякрикнетэтосли
шкомслишкоммногодляодногочеловекатеньметнуласьвсторонуглазаисчезликаксухойдо
ждьпосыпалисьосенниелистьямонтэгбылодинвлесуоленьэтобылоленьмонтэгощутилост
рыйзапахмускусасмешанныйсзапахомкровиидыханиязверязапахкардамонамхаикрестов
никавглухойночидеревьястенойбежалинанегоисноваотступалиназадбежалииотступалив
тактбиениюкровистучащейввискахземлябылаустланаопавшимилистьямиихтутнаверноб
ылимиллиардыногимонтэгапогружалисьвнихсловноонпереходилвбродсухуюшуршащу
юрекупахнущуюгвоздикойитеплойпыльюсколькоразныхзапаховвоткакбудтозапахсырог

окартофелятакпахнеткогдаразрежешьбольшуюкартофелинубелуюхолоднуюпролежавш
уювсюночьнаоткрытомвоздухевлунномсветеавотзапахпикулейвотзапахсельдереялежащ
егонакухонномстолеслабыйзапахжелтойгорчицыизприоткрытойбаночкизапахмахровых
гвоздикизсоседнегосадамонтэгопустилрукуитравянойстебелеккоснулсяеголадоникакбу
дторебеноктихоньковзялегозарукумонтэгподнеспальцыклицуонипахлилакрицейоноста
новилсяглубоковдыхаязапахиземлиичемглубжеонвдыхалихтемосязаемеестановилсядля
негоокружающиймирвовсемсвоемразнообразииумонтэгауженебылопрежнегоощущени
япустотытутбылочемнаполнитьсебяиотнынетакбудетвсегдаонбрелспотыкаясьпосухимл
истьямивдругвэтомновоммиренеобычногонечтознакомоеегоногазаделачтотоотозвавшее
сяглухимзвономонпошарилрукойвтравеводнусторонувдругуюжелезнодорожныерельсы
рельсыведущиепрочьотгородасквозьрощиилесаржавыерельсызаброшенногожелезнодор
ожногопутипутьпокоторомуемунадоидтиэтобылотоединственнознакомоесрединовизны
тотмагическийталисманкоторыйещепонадобитсяемунапервыхпорахкоторогоонсможетк
оснутьсярукойчувствоватьвсевремяподногамипокабудетидтичереззаросликуманикичер
езморезапаховиощущенийсквозьшорохишепотлесаондвинулсявпередпошпаламикудивл
ениюсвоемуонвдругпочувствовалчтотвердознаетнечточегооднаконикакнесмогбыдоказа
тькогдатодавноклариссатожепроходилаздесьполчасаспустяпродрогшийосторожноступа
япошпаламостроощущаякактемнотавпитываетсявеготелозаползаетвглазавротавушахсто
итгуллесныхзвуковиногиисколотыокустарникиобожженыкрапивойонвдругувиделвпере
диогоньогоньблеснулнасекундуисчезсновапоявилсяонмигалвдалисловночейтоглазмонт
эгзамернаместеказалосьстоитдохнутьнаэтотслабыйогонекионпогаснетноогонекгорелим
онтэгначалподкрадыватьсякнемупрошлодобрыхпятнадцатьминутпреждечемемуудалось
подойтипоближеоностановилсяиукрывшисьзадеревомсталглядетьнаогоньтихоколеблю
щеесяпламябелоеиалоестраннымпоказалсямонтэгуэтотогоньибоонтеперьозначалдлянег
осовсемнеточтораньшеэтотогоньничегонесжигалонсогревалмонтэгвиделрукипротянут
ыекеготеплутолькорукителасидевшихвокругкострабылискрытытемнотойнадрукаминеп
одвижныелицаоживленныеотблескамипламенионинезналчтоогоньможетбытьтакимонд
аженеподозревалчтоогоньможетнетолькоотниматьноидаватьдажезапахэтогоогнябылсов
семдругойбогвестьсколькоонтакпростоялотдаваясьнелепойноприятнойфантазиибудтоо
нлеснойзверькоторогосветкостравыманилизчащиунегобыливлажныевгустыхресницахг
лазагладкаяшерстьшершавыймокрыйноскопытаунегобыливетвистыерогаиеслибыкровь
егопролиласьназемлюзапахлобыосеньюондолгостоялприслушиваяськтепломупотрески
ваниюкостравокругкострабылатишинаитишинабыланалицахлюдейибыловремяпосидет
ьподдеревьямивблизизаброшеннойколеиипоглядетьнамирсостороныобнятьеговзглядом
словномирвесьсосредоточилсяздесьуэтогокострасловномирэтолежащийнаугляхкусокст
аликоторыйэтилюдидолжныбылиперековатьзановоинетолькоогоньказалсяинымтишина
тожебылаиноймонтэгподвинулсяближекэтойособойтишинеоткоторойказалосьзависели
судьбымираазатемонуслышалголосалюдиговорилинооннемогещеразобратьочемречьихт
екласпокойнотогромчетотишепередговорившимибылвесьмирионинеспешаразглядывал
иегоонизнализемлюзналилесазналигородлежащийзарекойвконцезаброшеннойжелезнод
орожнойколеионiговорилиобовсеминебыловещиокоторойонинемоглибыговоритьмонтэ
гчувствовалэтопоживыминтонациямихголосовпозвучавшимвнихноткамизумленияилюб
опытстваапотомктотоизговорившихподнялглазаиувиделмонтэгаувиделвпервыйаможетб
ытьивседьмойразичейтоголосокликнулеголадноможетенепрятатьсямонтэготступилвтем

нотудаужладнонебойтесьсновапрозвучалтотжеголосмилостипросимкнаммонтэгмедленоподошелвокругкострасиделипятеростариководетыхвтемносиниеизгрубойхолщовойтканибрюкиикурткиитакиежетемносиниерубашкионнезналчтоимответитьсадитесьсказалчеловеккоторыйповсейвидимостибылунихглавнымхотитекофемонтэгмолчасмотрелкактемнаядымящаясяструйкальетсявскладнуюжестянуюкружкупотомктотопротянулемуэтукружкуоннеловкоотхлебнулчувствуянасебелюбопытныевзглядыгорячийкофеобжигалгубыноэтобылоприятнолицасидевшихвокругнегозаруслигустымибородаминобородыбылиопрятныиаккуратноподстриженыирукиуэтихлюдейтожебыличистыиопрятныкогдаонподходилккоструонивсеподнялисьприветствуягостянотеперьсновауселисьмонтэгпилкофеаа

Висновки

Протягом роботи над цією лабораторно ми дізналися багато нового про афінний шифр. Стали зрозумілі його статичні особливості і способи його дешифрування. Також ми набули знань, щодо роботи з модулярною аріфметикою в програмуванні. Ці навички буду корисні мені у подальшому навчанні і роботі.