МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія

Комп’ютерний практикум №3

Виконали:
студенти III курсу
групи ФБ-82
Боднар А. В.,
Казміді І.Д.

Перевірив:
Чорний О.М.

_____

Київ 2020

Робота №3. Криптоаналіз афінної біграмної підстановки

- Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.
- Дата: 08.11.2020

Завдання до виконання (Варіант 2):

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.

Виконання роботи:

1. 5 найчастіших біграмм ВТ (російської мови) та ШТ:

n	відк. текст	шт
1	то	йа
2	ов	юа
3	на	чш
4	не	юд
5	но	рщ

Труднощі виконання

Під час перших спроб розшифрування, виходив частково неправильний текст:

однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптонеичреьеленноепрвчадкипроявляющиесярезколчрикусьваниемусиливающиесядоопасногодляжизнвчриводящегоктяжкомусамокалечениюмогутвсежевнеко

Як виявилось, помилка була у алфавіті: алфавіти відрізнялися тим, що в одному була послідовність «ы ь», а в іншому – «ь ы».

Після виправлення алфавіту, розшифрування пройшло успішно.

Розпізнавання змістовного тексту

Було використано метод заборонених біграм. Оскільки текст не має пробілів, потрібно було враховувати, що такі біграми, як «щя», які не зустрічаються у звичайній російській мові, можуть зустрітися у ВТ: «товарищяковлев». Тому у якості забороненіх біграмм були використані «жы, шы, аь, аы, уы, еы, оы». Оскільки отриманий після розшифрування ВТ достатньо великий, шанс не пройти перевірку таким набором біграмм задовольняє нашим вимогам. У даному варіанті перевірку проходить лише правильний ВТ.

Шифротекст:

рйрщкагппрфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюоэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэкяуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэарюжштнцмосхрхлтечшишваллмпптелиюдьпкуурдщерритыачтахщышкаюйзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщбероюазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфуыуйацдаювалляычларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбубеюыхрдщндщфщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюбероюарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносвиййдзырыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешбероюачпщылшыщдшэасуйаьпымкуюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзырыщаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричикзддрятаршроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээлучылшрщашошзсбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцрчийщпаюеющчшхпэщхеишашйамущьбукаьэзхцмустдмшышдшцчсдхйыуыщйаудчикабпсаюезлиекдффыршдчимшлчлэфуюаззддрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэыса репуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзсхажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюаршлсцпэсеегпосщерпусдюйаюдбучихеэдэпптехарпеылегшмчхухаяютечшюдуссайщслллыуюкайасазаопчичпнхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшцшмейряжпшюешпщьбудшоылшищгамуыщюаешлуьппрринхдщцадуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщчшмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаюьичбзлцчтыкйэщыштыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкйдшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушцькышзшвыйафщышхпцмдрщыыуюехакчщуиезафнщыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужичлщерпюабуашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпрешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяавдчишхтаичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщьбукаюдуыдщимюдкечушгмщрщашщпп

прэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщццтвкчисжлзсйепртшййыуйаусйрпншдажйазмгьус ффщлщрбезахемчтэлекмаюрщудеапамдосшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщыхубвчочпщаэщялчохехалюидвиаммс ееапегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйкишугрййкоыдднпрщышлсбубеаунккмнежскгцч тыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрйщызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэ шсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныурщгпзхцмчэиорщээашшщрщхезакдььрмьрпнхщшдькюе дефщроошкаюрпркдчэуырщлхчээпмеидбюхахщимюдюарппьщсрплаэщкаюытэтедщпуэщвкющиулаэиыйхллланажахоусиппрсе эщюхыййаькэиеыйееуйафмыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюахйщфрпешбероюару щефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейежпэиэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэ хувлуолиачйахагаодвимдчитысазшйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасхй юдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерпимюдкеслщещцримежагекаюрэпьчяф ьеруюсхпымздюлщелшашфьымосьрчифшцкщедеюакайасажлнктешцэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбр мэтдюадуклзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифусицлщеомхпипчушг мщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщроошэщнхльюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюыщ дшварчмэчиащварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

Розшифрований текст:

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющиесярезкос прикусываниемусиливающиесядоопасногодляжизниприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедос тигатьтакойсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокруженийимогуттакжесменятьсякраткимипе риодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообуславливаясьвобщемк акбыстранноэтониказалосьчистотелеснымипричинамиэтисостоянияхмогутпервоначальновозникатьпопричинамчистодушевными спугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволненийкакнихарактернодляогромногобольшинствослучаевин теллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеятельност игельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодос тоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститкаказтаболезньчастосопряженася рковыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболе знионэтиприпадкисовсемисвоимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобыч наявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятельствахневозможно установитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимо муфункциональногопониманиякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганичес кимеханизмкоторыйиспользуетсяприналичиивесьмаразныхусловийкакпринарушениимозговойдеятельностипритяжкомзаболев аниитканейилитоксическомзаболеваниитакипринедостаточномконтроледушевнойэкономиикризисномфункционированиидуше внойэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпо зывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликои тусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотводараздраженияэпилепти ческаяреакциякаковымименемможноназватьвсеэтовместевзятоенесомненнотакжепоступаетивраспоряжениеневрозасущностьк отороговтомчтобыликвидироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилептическ ийприпадокстановитсятакимобразомсимптомомистериииюадаптируетсяивидоизменяетсяподобнотомукакэтопроисходитприн ормальномтечениисексуальногопроцессатакимобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпр актическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедуш евнаяжизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятно чтоэпилепсиядостоевскогоотносится ковторомувидуточнодоказатьэтонельзяткакатомслучаенужнобылобывключитьвцелоку пностьегодушевнойжизниначалоприпадковипоследующиевидоизмененияэтихприпадковадляэтогоунаследостаточноданныхопи саниясамихприпадковничегонедаютсведенияосоотношенияхмеждуприпадкамииперевиваниями инеполныичастопротиворечивы всеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевдетствечтоонивначалехарактеризовалисьболееслабыми симптомамиитолькопослепотрясшегоегопереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылоб ывесьмауместноеслибыоправдалосьточтоониполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупротиворека тдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадостоевскогобросиласьвглазанеодном убиографудостоевскогоипослужилаимуказаниемнаизвестноесовременноепсихологическоенаправлениепсихоанализтаккакподр азумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпунктегоневрозаесл ияначнуобосноватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыучениеивыраж енияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдостоевскоговегоюношескиегодызадо лгодопоявленияэпилепсииуэтихприпадковбылоподобиесмертионназывалисьстрахомсмертиивыражалисьвсостоянииелетаргиче скогоснаэтаболезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяподавленностьчувствокаконпоз жерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейчасжеумеретьивсамомделенаступалосостояниесоверш енноподобноедействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемказаснутьоставлялзапис кичтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулетк ойвведениеснамизвестнысмыслинамерениетакихприпадковсмертиониозначаютотождествлениесумершимчеловекомкоторыйд ействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивторойслучайболеезначителенприпадоквуказанномс лучаеравноцененнаказаниюмыпожелалисмертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеуче

ниеутверждаетчтоэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокявляетсятакимобразомсамонаказаниемза пожеланиесмертиненавистномуотцуа

Ключ: (27,211)

Висновок

Виконуючи практичну роботу, ми опанували методи роботи з модульною арифметикою, проаналізували біграмний афінний шифр, закріпили навички частотного аналізу.