МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Орлов Дмитро ФБ-14

Макуха Андрій ФБ-14

Перевірила

Селюх П. В.

Київ 2023

Мета

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

Порядок виконання:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Реалізувати підпрограки 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.

3. 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 шифрекст. Якщо шифрекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

Спочатку взяли з попередніх лабораторних розбиття на біграми (з обчисленням частоти) та реалізували конвертацію у цілочисловий вигляд (перший крок шифрування - дешифрування)

Реалізували процес шифрування та дешифрування тексту на маленьких прикладах (методи encrypt та decrypt) з відомим ключем (Останню непарну літеру ми видаляли)

```
Open plain text: Привет мир
After encription:адрэлишу
After decryption:приветми
```

Після перевірки в додали розширений алгоритм Евкліда для знаходження оберненого значення за модулем.

Останнім кроком було знаходження всіх можливих комбінацій та знаходження можливих ключів, з перевіркою проміжного тексту.

Шифрований текст за варіантом:

рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьй
ахещыйеьеюеэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуо
йщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэк
яуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукч
щысаэарюжштнцмосхрхлтечшишваллмппртелиюдыпкуурдщерритыачтахщышкаюйзхц
мздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщберою
азанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошр
щышгпфуыуйацдаюваллйыачларщзшроюалахдорцпиыщылшошрщйьфуйазлиекдвифу
щлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфч
прбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбу
беюыхрдщндщфщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщр
оюаеймюбероюарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойате
ащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкй
бвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщц
жыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносви
ййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехдсд
жжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедви
злиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцч
исуюэиффриещжзьргшкдыууоьдглэшешбероюачпщылшыщдшэасуйаьпымкуюсщгхела
фитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйацчзюимпел
умсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричикзддрятарщроюазахачшфщч
шурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкгхавклаяхбмхашнэпос
юеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашошзсбужифчмэйкблкмос
нфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцрчийщпаюеющчшхпэщхеишаш
йамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюезлиекдффыршдчимшлчл
эфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйющешхщнкшл
нуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшс
осгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленкссвссеоамдосвпхрзш
мейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзсхажалафщнп
бупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечшджп
шюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюдбучих
еэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэшса
ющуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшцшм
ейряжпшюешпщьбудшоылшищгамуыщюаешлуьппрринхдщцадуришпчичифубелшмшм
вкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаеп
жьюдмшеемучщроюазацчаябуащышдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщч
шмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвж
шоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдб
юфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэ
иащваейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйас
ажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикммьлевлщднхбмнхшсзмгьхпэсреж
аолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпш

гцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмеза
хехщяпвсхйюдаюыущаидвцюдаюьичбзлцчтыкйэщыштыаччбзстдаюышхехаедюшзщрп
щысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкйдшрщзщашчоыйыуйаусй
рпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушщькышзшвыйафщыш
хпцмдрщыыуюехакчщуиезафнщыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющ
эплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужичлщерпюабуашькщыдщвйрмыулпбьйашд
тыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлайе
зщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпрешхнфрплацсрчцпхюшрфчсимэоскгфу
ыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяавдчишхтаичшзыйыуйаусйрпнушхакмю
бпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщьбукаюдуыдщимюдкечушгм
щрщашщппрэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщцц
твкчисжлзсйепртшййыуйаусйрпншдажйазмгьусффщлщрбезахемчтэлекмаюрщудеапамд
осшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщыхубвчочпщаэщялчохехалюидвиаммсее
апегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйкишугрййкоы
дднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрй
щызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрмфукукчщг
чилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныурщгпзхцмчэиорщэаэшшщрщхез
акдььрмьрпнхщшдькюедефщроошкаюрпркдчэуырщлхчээпмеидбюхахщимюдюарппьщс
рплаэщкаюытэтедщпуэщвкющиулаэиыйхлллнажахоусиппрсеэщюхыййаькэиеыйееуйаф
мыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюахйщфр
пешбероюарущефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейежпэ
иэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчитысаз
шйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасх
йюдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьер
пимюдкеслщещцримежагекаюрэпьчяфьеруюсхпымздюлщелшашфьымосьрчифшцкщед
еюакайасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюа
дуклзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпри
дчьнрифусицлщеомхпипчушгмщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейу
юфшроошэщнхльюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюыщдшварчмэчиа
щварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

Вивід програми:

Possible keys: [[27, 211]]

Decrypted text:
однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопреде
ленноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляж
изниприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьта
койсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокружениймо
могуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепо
ступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэт
ониказалосьчистотелеснымипричинамиэтисостоянияимогутпервоначальновозникатьпоп
ричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевн

ыхволненийкакнихарактернодляогромногобольшинствослучаевинтеллектуальноеснижение
ноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальной
деятельностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоенена
дежныилиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиейм
огутпроизводитьвпечатлениетупостинедоразвитоститкакэтаболезньчастосопряженаясрк
овыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязатель
нойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизменениямибыва
ютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинствесл
учаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятель
ствахневозможноустановитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетс
яводнородностиуказанныхсимптомовтребуетповидимомуфункциональногопониманиякакеслиб
ымеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганическимеха
низмкоторыйиспользуетсяприналичиивесьмаразныхусловийкакпринарушениимозговойдеятел
ьностипритяжкомзаболеваниитканейилитоксическомзаболеваниитакипринедостаточномкон
троледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделениемна
двавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпозы
вовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиуже
древнейшиеврачиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптацию
высвобожденияэпилептическогоотводараздраженияэпилептическаяреакциякаковымименемм
ожноназватьвсеэтовместевзятоенесомненнотакжепоступаетивраспоряжениеневроза
сущностькотороговтомчтобыликвидироватьсоматическимассыраздраженияскоторыминеврозн
еможетсправитьсяпсихическиэпилептическийприпадокстановитсятакимобразомсимптомомис
терииеюадаптируетсяивидоизменяетсяподобнотомукакэтопроисходитпринормальномтечени
исексуальногопроцессатакимобразоммысполнымправомразличаеморгани
ческуюиаффективнуюэпилепсиюпрактическоезначениеэтогоследующеестрадающийпервойпо
раженболезньюмозгастрадающийвторойневротиквпервомслучаедушевная
жизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамойдуше
внойжизнивесьмавероятночтоэпилепсиядостоевскогоотноситсяковторомувидуточнодоказать
этонельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодушевнойжизниначало
припадковипоследующиевидоизмененияэтихприпадковадляэтогоуна
снедостаточноданныхописаниясамихприпадковничегонедаютсведенияосоотношенияхмеждупр
ипадкамииипереживанияминеполныичастопротиворечивывсеговероятнеепредположениечто
припадкиначалисьудостоевскогоужевдетствечтоонивначалехарактеризовалисьболееслабымис
имптомамиитолькопослепотрясшегоегопереживаниянавосемнадцатомгодужизниубийстваотц
апринялиформуэпилепсиибылобывесьмауместноеслибыоправдалосьточтоониполностьюпрекр
атилисьвовремяотбыванияимкаторгивсибириноэтомупротиворечатдругиеуказанияочевиднаяс
вязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадостоевскогобросиласьвглазанеод
номубиографудостоевскогоипослужилаиуказаниемнаизвестноесовременноепсихологическоена
правлениепсихоанализтаккакподразумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютр
авмуиврекциидостоевскогонаэтоключевойпунктегоневрозаеслияначнуобосноватьэтуустановкупс
ихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдо

стоевскоговегоюношескиегодызадолгодопоявлениязпилепсииуэтихприпадковбылоподо биесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииилетаргическогоснаэта болезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяпода вленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупре дстоялосейчасжеумеретьивсамомделенаступалосостояниесовершенноподобноедействи тельнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемкаказасну тьоставлялзаписькичтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтомучтобы егопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестнысмыс линамерениетакихприпадковсмертониозначаютотождествлениесумершимчеловекомко торыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивторой случайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожелалис мертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучен иеутверждаетчтоэтотдругойдлямальчикаобычноотецииименуемыйистериейприпадокявл яетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Висновок

В результаті виконання ми практично змогли навчитись знаходити відкриті тексти, закодовані за допомогою афінної біграмної підстановки. Також знову перевірили корисність та зручність використання частотного аналізу.