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

ЛАБОРАТОРНА РОБОТА №2
«Криптоаналіз афінної біграмної підстановки»

Виконали:
студентки групи ФБ-04
Андрійчук Анастасія та Стоян Анастасія
Перевірив:
Чорний О.

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.

Хід роботи

Для спрощення роботи ми використали декілька функцій з вбудованих бібліотек мови python, зокрема – gcd. Інші функції писали самостійно. В якості методу відслідковування природності тексту ми обрали порівняння частот таких букв: ф, ц, щ. Виникла складність в тому, що початково функція не знаходила справжній текст. Ми підвищили гранично допустиме значення в декілька разів, поки не знайшли необхідні. Це пов'язано з тим, що частотні характеристики тексту не надто точно відповідають таким же в мові.

Результати

Варіант 1

Найчастіші біграми зашифрованого тексту: 'рн', 'ыч', 'нк', 'цз', 'иа'.

Ключ: а = 13, б = 151

Зашифрований текст

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысеча
мнмпывйвфяжтинфвйвйвсжнпчнмпгущзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепз
кианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйдбцвсшчмтшслаиятас
збчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяыз
рчйзчвгзжзычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчн
кицгщлчькевочфыщяцзреотйсфтбйщялчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьа

ючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпэзтйпчаэеэявахыдпдойдкрмпбцмвеэлж
очрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяццаиятчщтецрнбяшквдиабц
отияьаццйвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнк
сябяешщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьи
яцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырцсоушрнецчнкяуялж
очознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнй
цнбшзикзчшклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащзинэяьяцзчцы
чжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццрущзл
чшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкзвзвычяквсойюшххол
уычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфр
няыннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнк
ршчуярачыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйз
твйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыцзыэщрмпбцср
парчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпниву
чппжкнкэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщт
ыэзчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойзьялчуцднеэнпейвязярнбйеплюдфызя
киащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнмпмэьяючбяьярняыц
еязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюц
отноыкиащзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллце
иащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрн
ецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутсюцзкыфпцеэярнкец
зкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвец
ыогзбшучяпхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротв
жуяддьыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсу
чфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчтыгшшчкгнккршчтчи
ншчияцзывьяючбятьюьюаьыкьзаучйзтысюиебчщзечучючьквяднеэльачрнвязарчтчйдбйепл
юрбучэтийшчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччя
цегщечеойюрбмэипкйчнезучлчмыбшхыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэ
отучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебчочьвеслеяздчюзю
абйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтл
зньхярнбяшкжкмафпзкфвчьхззгьутчняьнязьянвсяюыььытнотшрычйцсспнмпйаццеяычрьхяр
нечяыцзчнйвшхнвючшкиачяюцйдбцььэтнкфякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщц
зрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяйтмпдфыяечювузпебц
йснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкш
чрнгсиаычицнввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщяты
спецяжлчштзщеэтыиылчтчкяяоечеклнжшдэпаычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщф
пмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюччажсчащзьянвшхьягнлжчцео
флшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэ
ебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиы
юзрнучиншчияцзовиылчнькяуянпйсбцмнмпзкеэзщйхчащзднеэшдшызюуфачштвснюфязюу
фзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтчсжлжыяызызэтшийвыч
ьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгят
члаэтмэщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячы
бшфтпаюьукфвеэсятчфяучыссбхяпацытыызкьццзтьянввящыбчяыцзпнйввяочьяхыцзицучюк
мэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпйкщтыыз
эзэкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэыча

эгмнкуффтчавяюзаояалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфч
ыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчучючцяцзицтллфвычялкшяюаэкйпщрсялкиц
бчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкбцкяцяечикфвсб
хятччянарчэяcрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсеп
нкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецнмяучт
пмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебччцеопнхофяжтгщачрнвязаозгкзщпц
йпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцотцяьнщ
ммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэт
ырнбчнксяжцпажэецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджк
ицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкыозрнотмусзщяхаэбычпабшкытнщм
мпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжцзеотлжееин
еэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнввджкйсиах
ыычяктзфятыыяькоыечзнзтчхучычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскы
йзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Розшифрований текст

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякак
невротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающей
насложностинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякара
мазовывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодн
оизвысочайшихдостиженийимировойлитературыпереоценитькотороеневозможноксожале
ниюпередпроблемойписательскоготворчествапсихоанализдолженсложитьоружиедостоев
скийскореевсегоуязвимкакморалистпредставляяегочеловекомвысоконравственнымнатом
основаниичтотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглу
бочайшиебездныгреховностимыигнорируемодносоображениеведьнравственнымявляетс
ячеловекреагирующийуженавнутреннеиспытываемоеискушениеприэтомемунеподдаваяс
ьктожепопеременнотогрешиттораскаиваясьставитсебевысокиенравственныецелитоголегк
оупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногоп
ринципанравственностинеобходимостиотреченияавтовремякакнравственныйобразжизнив
практическихинтересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениян
ародовварваровубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехнически
мпримеромрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассов
естьюхарактернаярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыд
остоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозывови
ндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинению
мирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкод
ушномунационализмукчемуменеезначительныеумыпришлисгораздоменьшимиусилиями
чемонвэтомслабоеместобольшойличностидостоевскийупустилвозможностьстатьучителем
иосвободителемчеловечестваиприсоединилсяктюремщикамкультурабудущегонемногим
будетемуобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужд
еннатакуюнеудачупомощипостиженияисилелюбвиклюдямемубылоткрытдругойапостольс
кийпутьслужениянампредставляетсяотталкивающимрассматриваниедостоевскоговкачест
вегрешникаилипреступниканоэтоотталкиваниенедолжноосновыватьсянаобывательскойо
ценкепреступникавыявитьподлиннуюмотивациюпреступлениянедолгодляпреступникасу
щественныдвечертыбезграничноесебялюбиеисильнаядеструктивнаясклонностьобщимдл
яобеихчертипредпосылкойдляихпроявленийявляетсябезлюбовностьнехваткаэмоциональ

нооценочногоотношениякчеловекутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотребностьвлюбвииегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьимститьнапримерпоотношениюкегопервойженеиеелюбовникунотогдавозникаетвопросоткудаприходитсоблазнпричислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимущественнонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитакихсклонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартнымигрампожетбытьсексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешаетсяследующимобразомсильнаядеструктивнаяустремленностьдостоевскогокотораямоглабысделатьегопреступникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизнутриитакимобразомвыразиласьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчертвыявляющихсявегораздражительностимучительстенетерпимостидажепоотношениюклюбимымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиствовневажномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдобродушнейшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывыделилитрифактораодинколичественныйидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремленностькперверзиикотораядолжнабылапривестиегоксадомазохизмуилисделатьпреступникомиегонеподдающеесяанализутворческоедарованиетакоесочетаниевполнемоглобысуществоватьибезневрозаведьбываютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритязаниипервичныхпозывовипротивоборствующихимторможенийприсоединяясюдавозможностисублимированиядостоевскоговсеещеможнобылобыотнестикразрядуимпульсивныххарактеровноположениевещейзатемняетсяналичиемневрозанеобязательногокакбылоказаноприданныхобстоятельствахновсежевозникающеготемскореечемнасыщенноеосложнениеподлежащеесостороныечеловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтоонопиэтойпопыткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназывалсебясамидругиетакжесчиталиегоэпилептикомнатомосновании чтоонбылподвержентяжелымприпадкамсопровождавшимисяпотерейсознаниясудорогамиипоследующимупадочнымнастроениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневрозакоторыйвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполнойуверенностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпадковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныавовторыхпотомучтопониманиесвязанныхсэпилептоиднымиприпадкамиболезненныхсостоянийостаетсянеясныма

Висновок:

Ми опанували прийоми з вирішення проблем обчислення в модулярній арифметиці. Також засвоїли знання щодо біграмної афінної підстановки. Цей шифр дещо складніше зламується, ніж шифр Віженера через велику кількість потенційних ключів та потребу перевіряти змістовність тексту.