Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки
1 варіант

Виконав:

студенти III курсу ФТІ

групи ФБ-94\ФБ-96

Солопенко Борис

Бутко Максим

Перевірила:

Селюх П.В

Мета роботи

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

Хід роботи

Під час роботи с лабораторною було реалізовано підпрограмми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь.
За допомогою коду з першого практикуму було знайдено найчастіші біграми для зашифрованого тексту: 'рн', 'ыч', 'нк', 'цз', 'иа'.
Найчастіші біграми для мови: 'ст', 'но', 'то', 'на', 'ен'

Для кожного кандидата на ключ було розшифровано текст, але у більшості це був незмістовний текст, тому кандидат відхилявся.
Остаточні та вірні ключі: (13, 151)

Зашифрований текст:
лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфяжтинфвйвйвсжнпчнмпгу
щзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаы
чйдбцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчв
гзжзычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбй
щялчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпэзтйпчаэеэява
хыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяццаиятчщтецрнбяшквдиабцотияьа
ццйвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяюч
бястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмак
ырцсоушрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнйцнбшзи
кзчшклзпеепаопниашчеквдзеязэгцекккьызаццнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцз
жеьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкз
взвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвц
яучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнб
яшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырн
эяччяыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкн
кэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяю
шкзйзлафпэойзьялчуцдneэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхърнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчн
мпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиа
щзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжюч
ьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутс
юцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяыычягшнвдфкгнкмяфтпаюьукфвецыогзбшуч
япхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэт
ивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчт
ыгшшчкгнккршчтчиншчияцзывьяючбятьюьюаьыкьзаучйзтысюиебчщзечучючьквяднеэльачрнвязарчтчйдбйеплюрбучэти
йшчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшх
ыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзе
бчочьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнб
яшкжкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцьь
этнкфякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяй
тмпдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиа
ычицнввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклн
жшдэпаычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюччажсча
щзьянвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеых
ынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчияцзовиылчнькяуянпйсбц
мнмпзкеэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтчс
жлжыяызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгятчлаэтм
эщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпа
цытыызкьццзтьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгн
кыкряеыичвзрнпйкщтыыэээкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгм
нкуффтчавяюзаояалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюы
ьытнотбцшчучючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночя
гшрняыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэ
бфяжтгщднинепжвгщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяим
ицрнбчтчнасжнпоебччцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцк
кузбнжчуйупучьцотцяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырн
бчнксяжцпажэецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнаашыпащ
явьпнзеэяыяызбшкыозрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмнныычпеепшчеьбяэяшкиабшпкмпдщюевсзь

меязэзтыжцзеотлжееинеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнвджкйсиахыычякт
зфятыыяькоыечзнзтчхучычньбнзежкфэкксяйцщщкяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнх
офяяаяжеы

Розшифрований за допомогою знайдених ключів (13, 151) текст:
многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмыслителяэтикаи
какгрешникакакжеразобратьсявэтойневольносмущающейнассложностинаименееспоренонкакписательместоеговодномря
дусшекспиромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвы
сочайшихдостиженийимировойлитературыпереоценитькотороеневозможноксожалениюпередпроблемойписательскоготво
рчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяегочеловекомвысокон
равственнымнатомосновааниичтотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубочайшиебе
здныгреховностимыигнорируемодносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспыт
ываемоеискушениеприэтомемунеподдаваяськтожепопеременноготогрешиттораскаиваясьставитсебевысокиенравственные
целитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногопринципанравстве
нностинеобходимостиотречениявтовремякакнравственныйобразжизнивпрактическихинтересахвсегочеловечествааэтимон
напоминаетварваровэпохипереселениянародовварваровубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтех
ническимпримеромрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюхарактернаярусс
каячертадостаточнобесславениконечныйитогнравственнойборьбыдостоевскогопослеисступленнойборьбывоимяпримере
нияпритязанийпервичныхпозывовиндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчине
ниюмирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационализмукче
муменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместобольшойличностидостоевскийуп
устилвозможностьстатьучителемиосвободителемчеловечестваиприсоединилсяктюремщикамкультурабудущегонемноги
мбудетемуобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюнеудачупомощипос
тиженияисилелюбвиклюдямемубылоткрытдругойапостольскийпутьслужениянампредставляетсяотталкивающимрассмат
риваниедостоевскоговкачествегрешникаилипреступниканоэтоотталкиваниенедолжноосновыватьсянаобывательскойоцен
кепреступникавыявитьподлиннуюмотивациюпреступлениянедолгодляпреступникасущественныдвечертыбезграничноес
ебялюбиеисильнаядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляихпроявленийявляетсябезлюбовност
ьнехваткаэмоциональнооценочногоотношениякчеловекутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегоб
ольшуюпотребностьвлюбвиегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшуюемулюбить
ипомогатьтамгдеонимелбыправоненавидетьимстительнапримерпоотношениюкегопервойженеиеелюбовникунотогдавозник
аетвопросоткудаприходитсоблазнпричисленияздостоевскогокпреступникамответиззавыбораегосюжетовэтопреимуществ
еннонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитакихсклонностейвеговнутренне
ммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартнымиграмможетбытьсексуальногорастлениянезрелойдевоч
киисповедьэтопротиворечиеразрешаетсяследующимобразомсильнаядеструктивнаяустремленностьдостоевскогокоторая
моглабыделатьегопреступникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизн
утриитакимобразомвыразиласьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчертвыявляющихся
вегораздражительностимучительстванетерпимостидажепоотношениюклюбимымлюдяматакжевегоманереобращениясчи
тателемитаквмелочахонсадиствовневажномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдоб
родушнейшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывыделилитрифактораодинколичественны
йидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремленностькперверзиикоторыядолжнабылаприве
стиегоксадомазохизмуилисделатьпреступникомиегонеподдающеесяанализутворческоедарованиетакоесочетаниевполнем
оглобысуществоватьибезневрозаведьбываютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритяза
ниипервичныхпозывовипротивоборствующихимторможенийприсоединяясюдавозможностисублимированиядостоевског
овсеещеможнобылобыотнестикразрядуимпульсивныххарактеровноположениевещейзатемняетсяналичиемневрозанеобяз
ательногокакбылосказаноприданныхобстоятельствахновсежевозникающеготемскореечемнасыщенноеосложнениеподле
жащеесосторонычеловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтоонаприэтойпопытке
поплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназывалсебясамидругиетакжесчитал
иегоэпилептикомнатомосновааниичтоонбылподвержентяжелымприпадкамсопровождавшимисяпотерейсознаниясудорога
миипоследующимупадочнымнастроениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневроз
акоторыйвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполнойуверенн
остьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпадковтакназываемойэпилепсиидостоевскогон
едостаточныиненадежныавовторыхпотомучтопониманиесвязанныхсэпилептоиднымиприпадкамиболезненныхсостояний
остаетсянеясныма

Текст має смисл, отже ключі вірні.

Висновок: під час роботи над практикумом було засвоєно навички частотного аналізу на прикладі розкриття моноалфавітної підстановки, розшифрування текстів, які були зашифровані афінним шифром за допомогою підстановки найпопулярніших біграм.