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

Симетрична криптографія

Лабораторна робота №3

Виконала:
студентка гр. ФІ-04
Бабич А. А.

Київ – 2023

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

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 шифротексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифротексту (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 шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

Варіант-1

П’ять найчастіших біграм шифротексту:

рн: 0.012889

ыч: 0.009002

нк: 0.008797

цз: 0.00757

тч: 0.006751

Можливі варіанти ключів:

Keys: [(11, 631), (13, 151), (29, 258), (67, 416), (76, 633), (105, 382), (117, 74), (148, 477), (157, 568), (159, 695), (174, 891), (197, 166), (210, 418), (211, 224), (230, 89), (231, 633), (241, 821), (275, 550), (277, 534), (306, 379), (314, 788), (327, 79), (331, 85), (342, 457), (382, 503), (389, 885), (399, 379), (405, 664), (408, 320), (475, 323), (486, 875), (553, 782), (556, 258), (562, 819), (572, 313), (579, 85), (619, 816), (630, 503), (634, 158), (647, 761), (655, 819), (684, 568), (686, 819), (720, 101), (730, 736), (731, 319), (750, 364), (751, 504), (764, 146), (787, 382), (802, 854), (804, 534), (813, 625), (844, 67), (856, 891), (885, 736), (894, 506), (932, 664), (948, 257), (950, 642)]

Розпізнавач мови побудований на основі перевірки індексу відповідності (індекс співпадіння (Index of Coincidence) для російської мови дорівнює близько 0,052).

Знайдене значення ключа: (13, 151)

Шифрований текст:

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфяжтинфвйвйвсжнпчнмпгу

щзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйд

бцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвгзжз

ычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщялчде

чамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпэзтйпчаэеэявахыдп

дойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяццаиятчщтецрнбяшквдиабцотияьаццйв

ычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючбяст

зырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырц

соушрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнйцнбшзикзч

шклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзже

ьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкз

взвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвця

учрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбя

шкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэячч

яыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнк

эблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюш

кзйзлафпэойзьялчуцднеэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчн

мпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиа

щзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьв

зжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиа ычицнввдбцкыьярнбяут

сюцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгн кмяфтпаюьукфвецыогзбшучяп

хкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддьыцзяквя кяяоебхзлзмзгштышспаэт

ивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщеб ччекиабшфяяцмнкыбэкгхчты

гшшчкгнккршчтчиншчияцзывьяючбятьюьюаыкьзаучйзтысюиебчщзечучючьквяднеэльачрнв язарчтчйдбйеплюрбучэтий

шчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойю рбмэипкйчнезучлчмыбшхы

здыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекф вйкинвдщыечикфвжяццзебч

очьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятч хбцяычлуычфтлзньхярнбяшк

жкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшх нвючшкиачяюцйдбцььэтнк

фякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамвр ьйпзквдзтмаьпнкэофяйтмп

дфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцт ыяьрнэякпнкшчрнгсиаычиц

нввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзще этыиылчтчкяяоечеклнжшдэ

паычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчыз якиащзфяеыюччажсчащзья

нвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыкк юнкэбппкйфэуэебзоеыхынмиц

йдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчияцз овиылчнькяуянпйсбцмнмпзк

еэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызяк иащзачрнвязарчтчсжлжыяызыз

этшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрц шчрнгятчлаэтмэщяшкиабшсе

отбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчф яучыссбхяпацытыызкьццзт

ьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсб шмпаычфткгнкыкряеыичвзрнпй

кщтыызэзэкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшх фэычаэгмнкуффтчавяюзао

яалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчуч

ючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкбцкяцяеч

икфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжв

гщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебч

чцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцот

цяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцпажэец

отноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкы

озрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжцзеотлжее

инеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнввджкйсиахыычяктзфятыыяькоыечзнзтчх

учычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Розшифрований текст:

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейнасложностинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайшихдостиженийимировойлитературыпереоценитькотороеневозможноксожалениюпередпроблемойписательскоготворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяегочеловекомвысоконравственнымнатомосновании чтотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубочайшиебездныгреховностимыигнорируемодносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспытываемоеискушениеприэтомемунеподдаваяськтожепопеременнотогрешиттораскаиваясьставитсебевысокиенравственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногопринципанравственностинеобходимостиотречениявтовремякакнравственныйобразжизнивпрактическихинтересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварваровубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюхарактернаярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыдостоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозывовиндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинениюмирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационализмукчемуменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместобольшойличностидостоевскийпустилвозможностьстатьучителемиосводителемчеловечестваиприсоединилсяктюремщикамкультурабудущегонемногимбудетемуобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужд

еннатакуюнеудачупомощипостиженияисилелюбвиклюдямемубылоткрытдругойапостольски йпутьслужениянампредставляетсяотталкивающимрассматриваниедостоевскоговкачествегре шникаилипреступниканоэтоотталкиваниенедолжноосновыватьсянаобывательскойоценкепре ступникавыявитьподлиннуюмотивациюпреступлениянедолгодляпреступникасущественныдв ечертыбезграничноесебялюбиеисильнаядеструктивнаясклонностьобщимдляобеихчертипредп осылкойдляихпроявленийявляетсябезлюбовностьнехваткаэмоциональнооценочногоотношен иякчеловекутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотребн остьвлюбвииегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшую емулюбитьипомогатьтамгдеонимелбыправоненавидетьимститьнапримерпоотношениюкегопе рвойженеиеелюбовникунотогдавозникаетвопросоткудаприходитсоблазнпричислениядостоев скогокпреступникамответиззавыбораегосюжетовэтопреимущественнонасильникиубийцыэго центрическиехарактерычтосвидетельствуетосуществованиитакихсклонностейвеговнутренне ммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартнымиграмможетбытьсексуальн огорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешаетсяследующимобразомсиль наядеструктивнаяустремленностьдостоевскогокотораямоглабысделатьегопреступникомбыла вегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизнутриитаким образомвыразиласьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчерт выявляющихсявегораздражительностимучительстванетерпимостидажепоотношениюклюбим ымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиствовневажномсадис тпоотношениюксамомусебеследовательномазохистиэтомягчайшийдобродушнейшийвсегдаго товыйпомочьчеловеквсложнойличностидостоевскогомывыделилитрифактораодинколичестве нныйидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремленностькперв ерзиикотораядолжнабылапривестиегоксадомазохизмуилисделатьпреступникомиегонеподда ющеесяанализутворческоедарованиетакоесочетаниевполнемоглобысуществоватьибезневроза ведьбываютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритязаниип ервичныхпозывовипротивоборствующихимторможенийприсоединяясюдавозможностисубли мированиядостоевскоговсеещеможнобылобыотнестикразрядуимпульсивныххарактеровнопо ложениевещейзатемняетсяналичиемневрозанеобязательногокакбылосказаноприданныхобсто ятельствахновсежевозникающеготемскореечемнасыщенноеосложнениеподлежащеесосторон ычеловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтооноприэ тойпопыткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевск ийназывалсебясамидругиетакжесчиталиегоэпилептикомнатомосновании чтоонбылподвержен тяжелымприпадкамсопровождавшимисяпотерейсознаниясудорогамиипоследующимупадочн ымнастроениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневро закоторыйвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелуюистериюут верждатьэтосполнойуверенностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнези ческихприпадковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныавовторых потомучтопониманиесвязанныхсэпилептоиднымиприпадкамиболезненныхсостоянийостаетс янеясныма

Висновки:

Під час виконання цієї лабораторної роботи було отримано навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанувано прийоми роботи в модулярній арифметиці. Було реалізовано обчислення нсд, оберненого елемента за модулем, а також знайдено можливі варіанти ключів через розв’язок лінійних порівнянь, за допомогою перевірки індексу відповідності було знайдено правильний ключ та розшифровано текст.