Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Лабораторна робота № 3

з предмету «Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Варіант №1

Виконали:

студенти 3 курсу ФТІ

групи ФБ-82

Матвієнко Олексій

Басюк Ілля

Перевірив:

Чорний О. М.

Київ 2020

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:

Зашифрований текст
лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфяжтинфвйвйвсжнпчнмпгу щзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйд бцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвгзжз ычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщялчде чамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпээтйпчаэеэявахыдп дойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяццаиятчщтецрнбяшквдиабцотияьацційв ычфткюмпьяэяддаьччшыызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючбяст зырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырц соушрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнйцнбшзикзч шклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзже ьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкз взвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвця учрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбя шкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэячч яыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнк эблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыызззивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюш кзйзлафпэойзьялчуцдneэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчн мпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиа щзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючъв зжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяут сюцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвецыогзбшучяп хкььоэинрцогэбфтпаюьтпнкэофяячщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжяддьыцзяквякяяоебхзлзмзгштышспаэт ивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччщщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчты гшшчкгнккршчтчиншчияцзывьяючбятьюьюаыыкьзаучйзтысюиебчщзечучючькквяднеэльачрнвязарчтчйдбйеплюрбучэтий шчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхы здыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжящцзебч очьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяшк жкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцььэтнк фякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяйтмп дфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычиц нввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтещщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэ паычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюччажсчащзья нвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеыхынмиц йдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзк еэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтчсжлжыяызыз этшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгятчлаэтмэщяшкиабшсе отбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпацытыызкьццзт ьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпй кщтыызэээкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавяюзао яалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчуч ючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщцмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкбцкяцяеч икфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжв гщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебч чцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцот цяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцпажэец отноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкы озрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмнныычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязээтыжцзеотлжее инеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнвждккйсиахыычяктзфятыыякоыечзнзтчх учычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Розшифрований текст
многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневрот икакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейнасложност инаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазовывеличайши йроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайшихдостиже ниймировойлитературыпереоценитькотороеневозможноксожалениюпередпроблемойписатель скоготворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалис тпредставляяегочеловекомвысоконравственнымнатомосновании чтотолькототдостигаетвысшег онравственногосовершенствактопрошелчерезглубочайшиебездныгреховностимыигнорируемо дносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспытываем оеискушениеприэтомемунеподдаваяськтожепопеременнотогрешитораскаиваясьставитсебевы сокиенравственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизн ьоннеисполняетосновногопринципанравственностинеобходимостиотречениявтовремякакнравс твенныйобразжизнивпрактическихинтересахвсегочеловечестваэтимоннапоминаетварваровэпо хипереселениянародовварваровубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьт ехническимпримеромрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделк ассовестьюхарактернаярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыд остоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозывовиндиви дастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинениюмирскомуид уховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационали змукчемуменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместо большойличностидостоевскийупустилвозможностьстатьучителемиосводителемчеловечества иприсоединилсяктюремщикамкультурабудущегонемногимбудетемуобязанавэтомповсейвероят ностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюнеудачупомощипостиженияиси лелюбвиклюдямемубылоткрытдругойапостольскийпутьслужениянампредставляетсяотталкива ющимрассматриваниедостоевскоговкачествегрешникаилипреступниканоэтоотталкиваниенедол жноосноватьсянаобывательскойоценкепреступникавыявитьподлиннуюмотивациюпреступле ниянедолгодляпреступникасущественныдвечертыбезграничноесебялюбиеисильнаядеструктив наясклонностьобщимдляобеихчертипредпосылкойдляихпроявленийявляетсябезлюбовностьне хваткаэмоциональнооценочногоотношениякчеловекутутсразувспоминаешьпротивоположноеэт омуудостоевскогоегобольшуюпотребностьвлюбвиегоогромнуюспособностьлюбитьпроявившу юсявегосверхдобротеипозволявшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьим стить напримерпоотношениюкегопервойженеиеелюбовникунотогдавозникаетвопросоткудапри ходитсоблазнпричислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимущ ественнонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитаки хсклонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартными грамможетбытьсексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешается следующимобразомсильнаядеструктивнаяустремленностьдостоевскогокотораямоглабысделать егопреступникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотого чтобыизнутриитакимобразомвыразиласьвмазохизмеичувствевинывсетакивеголичностинемало исадистическихчертвыявляющихсявегораздражительностимучительстве нетерпимостидажепоот ношениюклюбимымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиствовн евважномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдобродушне йшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывыделилитрифактораоди нколичественныйидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремленн остькперверзиикоторыядолжнабылапривестиегоксадомазохизмуилисделатьпреступникомиегон еподдающеесяанализутворческоедарованиетакоесочетаниевполнемоглобысуществоватьибезн еврозаведьбываютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритяза ниипервичныхпозывовипротивоборствующихимторможенийприсоединяясюдавозможностисуб лимированиядостоевскоговсеещеможнобылобыотнестикразрядуимпульсивныххарактеровнопо ложениевещейзатемняетсяналичиемневрозанеобязательногокакбылосказаноприданныхобстоя тельствахновсежевозникающеготемскореечемнасыщенееосложнениеподлежащеесостороныч еловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтоонноприэтойп опыткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназ

ывалсебясамидругиетакжесчиталиегоэпилептикомнатомосновании чтоонбылподвержентяжелы
мприпадкамсопровождавшимисяпотерейсознаниясудорогамиипоследующимупадочнымнастр
оениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневрозакоторы
йвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэт
осполнойуверенностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпад
ковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныавовторыхпотомучтопони
маниесвязанныхсэпилептоидными припадкамиболезненныхсостоянийостаетсянеясныма

Висновки:

В результаті виконання лабораторної роботи ми отримали навички частотного аналізу на прикладі розкриття шифрів моноалфавітної підстановки та опанували прийоми роботи в модулярній арифметиці.