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

ЛАБОРАТОРНА РОБОТА №3

З дисципліни «Криптографія»

Варіант 1

Виконали:

студенти 3 курсу ФТІ

групи ФБ-83

Чудо Христина
Тущенко Денис

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.

Труднощі: некоректно працював алгоритм підбору ключа, оскільки не було помічено неправильний підбір найчастіших біграм.

П'ять найчастіших біграм шифртексту	
1	рн
2	ыч
3	нк
4	цз
5	иа

Автоматичний розпізнавач мови працює за методом "забороненим біграмам". Коректність його роботи підтверджується, адже всі ключі, крім реального, були відкинуті.

Шифротекст
лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфя жтинфвйвйвсжнпчнмпгущзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкианьуыфллфтыра ючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйдбцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбц пцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвгзжзычэявсшчтщлжочш ызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбй щялчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятч рогцфэкыпэзтйпчаэеэявахыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжв ининачрнсджяццциаиятчщтецрнбяшквдиабцотияьаццйвычфткюмпьяэяддаьччшызюсяуядсяжутр хбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнк ецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзт макырцсоушрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньа ччквсеокяяорнбччнйцнбшзикзчшклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащ зинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытнщрпаозвзьнотпанхзайдкрмпбцсрпа ццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкзвзвычяквсойюшхх олуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняы

ннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярач
ыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэ
цтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыцзыэщрмпбцсрпарчтчбйхярняыжкл
жььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнкэблыибшхязрнпы
ьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзща
чзяюшкзйзлафпэойзьялчуцднеэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрн
йахыбшнрчнмпмэхчйцбйвсчнмпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйд
жкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиащзфтногзаашятчфяжтгщтщвырчычбчтчжк
рйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучр
непйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыья
рнбяутсюцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдф
кгнкмяфтпаюьукфвецыогзбшучяпхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпац
цнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшбйчззсеобйлзирот
щзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчтыгшшчкгнккршчт
чиншчияцзывьяючбятьюьюаьыкьзаучйзтысюиебчщзечучючьквяднеэльачрнвязарчтчйдбйеплюр
бучэтийшчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщече
ойюрбмэипкйчнезучлчмыбшхыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцз
овйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебчочьвеслеяздчюзюабйчыикфтщрчащяц
зшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяшкжкмафпзкфв
чьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюц
йдбцььэтнкфякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйц
нйамврьйпзквдзтмаьпнкэофяйтмпдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфл
фэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычицнввдевинзтсолчспейцаыячыбшйдзеэ
ярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэпаычычтчбн
бйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюч
чажсчащзьянвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмое
жчыккюнкэбппкйфэуэебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрн
ечекицяыькеэиыюзрнучиншчияцзовиылчньяуянпйсбцмнмпзкеэзщйхчащзднеэшдшызюуфачшт
вснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтчсжлжыяызызэтши
йвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгятч
лаэтмэщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтп
аюьукфвеэсятчфяучыссбхяпацытыызкьццзтьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжр
ьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпйкщтыыззэкицбчичжеиаж
чыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавяюзаояал
сецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекч
хюыьытнотбцшчучючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючн
взщккзеязщышкчхбйрнночягшрняыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнкс
яучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмз
ьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоеб
ччцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчо
кбцккузбнжчуйупучьцотцяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэуз
учнпйсрбчзньныачякуэтырнбчнксяжцпажэецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщ
юйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкыозрнотмусзщяхаэбычп
абшкытнщммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжцзеотл
жееинеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнввджкйсиах
ыычяктзфятыыяькоыечзнзтчхучычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзчч
щяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Відкритий текст
многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневрот икакакмыслителяэтикаикакгрешникакакажеразобратьсявэтойневольносмущающейнасложност инаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазовывеличайши йроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайшихдостиже

ниймировойлитературыпереоценитькотороеневозможноксожалениюпередпроблемойписатель
скоготворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалис
тпредставляяегочеловекомвысоконравственнымнатомосновааниичтотолькототдостигаетвысшег
онравственногосовершенствактопрошелчерезглубочайшиебездныгреховностимыигнорируемо
дносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспытываем
оеискушениеприэтомемунеподдаваяськтожепопеременнотогрешиттораскаиваясьставитсебевы
сокиенравственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизн
ьоннеисполняетосновногопринципанравственностинеобходимостиотреченияавтовремякакнравс
твенныйобразжизнивпрактическихинтересахвсегочеловечестваэтимоннапоминаетварваровэпо
хипереселениянародовварваровубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьт
ехническимпримеромрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделк
ассовестьюхарактернаярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыд
остоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозывовиндиви
дастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинениюмирскомуид
уховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационали
змукчемуменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместо
большойличностидостоевскийупустилвозможностьстатьучителемиосвободителемчеловечества
иприсоединилсяктюремщикамкультурабудущегонемногимбудетемуобязанавэтомповсейвероят
ностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюнеудачупомощипостиженияиси
лелюбвиклюдямемубылоткрытдругойапостольскийпутьслужениянампредставляетсяотталкива
ющимрассматриваниедостоевскоговкачествегрешникаилипреступниканоэтоотталкиваниенедол
жноосновыватьсянаобывательскойоценкепреступникавыявитьподлиннуюмотивациюпреступле
ниянедолгодляпреступникасущественныдвечертыбезграничноесебялюбиеисильнаядеструктив
наясклонностьобщимдляобеихчертипредпосылкойдляихпроявленийявляетсябезлюбовностьне
хваткаэмоциональнооценочногоотношениякчеловекутутсразувспоминаешьпротивоположноеэт
омуудостоевскогоегобольшуюпотребностьвлюбвииегоогромнуюспособностьлюбитьпроявившу
юсявегосверхдобротеипозволявшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьим
стительнапримерпоотношениюкегопервойженеиеелюбовникунотогдавозникаетвопросоткудапри
ходитсоблазнпричислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимущ
ественнонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитаки
хсклонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартными
грамможетбытьсексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешается
следующимобразомсильнаядеструктивнаяустремленностьдостоевскогокоторыяможлабыделать
егопреступникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотого
чтобыизнутриитакимобразомвыразиласьвмазохизмеичувствевинывсетакивеголичностинемало
исадистическихчертвыявляющихсявегораздражительностимучительстванетерпимостидажепоот
ношениюклюбимымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиствовн
евважномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдобродушне
йшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывыделилитрифактораоди
нколичественныйидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремленн
остькперверзиикотораядолжнабылапривестиегоксадомазохизмуилисделатьпреступникомиегон
еподдающеесяанализутворческоедарованиетакоесочетаниевполнемоглобысуществоватьибезн
еврозаведьбываютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритяза
ниипервичныхпозывовипротивоборствующихимторможенийприсоединяясюдавозможностисуб
лимированиядостоевскоговсеещеможнобылобыотнестикразрядуимпульсивныххарактеровнопо
ложениевещейзатемняетсяналичиемневрозанеобязательногокакбылосказаноприданныхобстоя
тельствахновсежевозникающеготемскореечемнасыщеннееосложнениеподлежащеесостороныч
еловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтоонноприэтойп
опыткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназ
ывалсебясамидругиетакжесчиталиегоэпилептикомнатомосновааниичтоонбылподвержентяжелы
мприпадкамсопровождавшимисяпотерейсознаниясудорогамиипоследующимупадочнымнастр
оениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневрозакоторы
йвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэт
осполнойуверенностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпад

ковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныавовторыхпотомучтопони маниесвязанныхсэпилептоидными припадкамиболезненныхсостоянийостаетсянеясныма

КЛЮЧ (13, 151)

Висновок: в процесі лабораторної роботи ми набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, опанували прийоми роботи в модулярній арифметиці, повторили процес роботи з відкритим та шифрованим текстом, що ми робили у попередній лабораторній роботі.