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

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Виконали:
Студенти групи ФБ-83
Байрак М.
Бєляєв М.
Перевірив:

МЕТА ЗАВДАННЯ: 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.

Найчастіші біграми в ШТ:

рн

ьч

нк

цз

иа

most rare symbol is x

[478, 430] false 1 / 180

most frecuent symbol is x

[241, 821] false 2 / 180

most frecuent symbol is д

[389, 885] false 3 / 180

most frecuent symbol is в

[445, 156] false 4 / 180

most frecuent symbol is т

[483, 908] false 5 / 180

most frecuent symbol is н

[724, 259] false 6 / 180

most frecuent symbol is т

[872, 323] false 7 / 180

most frecuent symbol is т

[928, 555] false 8 / 180

most frecuent symbol is л

[720, 101] false 9 / 180

most rare symbol is п

[237, 22] false 10 / 180

most frecuent symbol is щ

[148, 477] false 11 / 180

most frecuent symbol is с

[204, 709] false 12 / 180

most frecuent symbol is э

[572, 313] false 13 / 180

[89, 234] text found

most frecuent symbol is и

[813, 625] false 15 / 180

most frecuent symbol is е

[56, 921] false 16 / 180

most frecuent symbol is я

[516, 601] false 17 / 180

[33, 522] text found

most frecuent symbol is п

[757, 913] false 19 / 180

most frecuent symbol is ы

[905, 16] false 20 / 180

most rare symbol is ж

[261, 492] false 21 / 180

most frecuent symbol is х

[210, 418] false 22 / 180

most frecuent symbol is д

[327, 79] false 23 / 180

most frecuent symbol is в

[631, 652] false 24 / 180

most frecuent symbol is т

[700, 846] false 25 / 180

most frecuent symbol is т

[910, 755] false 26 / 180

most frecuent symbol is т

[66, 416] false 27 / 180

most frecuent symbol is т

[370, 28] false 28 / 180

most frecuent symbol is л

[751, 504] false 29 / 180

[51, 487] text found

most frecuent symbol is щ

[117, 74] false 31 / 180

most frecuent symbol is с

[421, 647] false 32 / 180

most frecuent symbol is э

[634, 158] false 33 / 180

most rare symbol is ж

[895, 141] false 34 / 180

most frecuent symbol is з

[844, 67] false 35 / 180

most frecuent symbol is е

[304, 301] false 36 / 180

most frecuent symbol is я

[330, 105] false 37 / 180

[591, 88] text found

most frecuent symbol is п

[540, 14] false 39 / 180

most frecuent symbol is ы

[657, 636] false 40 / 180

most rare symbol is ы

[864, 519] false 41 / 180

most frecuent symbol is р

[894, 506] false 42 / 180

most frecuent symbol is с

[486, 875] false 43 / 180

most frecuent symbol is и

[929, 651] false 44 / 180

most frecuent symbol is т

[97, 819] false 45 / 180

most frecuent symbol is т

[30, 816] false 46 / 180

most frecuent symbol is т

[583, 224] false 47 / 180

most frecuent symbol is т

[65, 0] false 48 / 180

most frecuent symbol is в

[67, 416] false 49 / 180

most rare symbol is ы

[931, 426] false 50 / 180

most frecuent symbol is г

[553, 782] false 51 / 180

most frecuent symbol is ю

[35, 558] false 52 / 180

most frecuent symbol is б

[475, 323] false 53 / 180

most frecuent symbol is т

[378, 333] false 54 / 180

most frecuent symbol is д

[408, 320] false 55 / 180

most frecuent symbol is ж

[443, 465] false 56 / 180

most frecuent symbol is к

[32, 106] false 57 / 180

[896, 116] text found

most frecuent symbol is ф

[926, 103] false 59 / 180

most frecuent symbol is м

[518, 472] false 60 / 180

most frecuent symbol is н

[277, 421] false 61 / 180

[13, 151] text found

ШТ

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпы
вйвфяжтинфвйвйвсжнпчнмпгу

щзкыфвйвутсюцзкыкынмотзщбйыыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйд

бцвсшчмтшслаиятасзбчжйыыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвгзжз

ычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщялчде

чамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпэзтйпчаэеэявахыдп

дойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяцццаиятчщтецрнбяшквдиабцотияьаццйв

ычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючбяст

зырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырц

соушрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнйцнбшзикзч

шклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзже

ьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкз

взвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвця

учрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбя

шкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэячч

яыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнк

эблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюш

кзйзлафпэойзьялчуцднеэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчн

мпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиа

щзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьв

зжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяут

сюцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвецыогзбшучяп

хкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэт

ивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчты

гшшчкгнккршчтчиншчияцзывьяючбятьюьюаьыкьзаучйзтысюиебчщзечучючькваднеэльачрнвязарчтчйдбйеплюрбучэтий

шчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхы

здыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебч

очьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяшк

жкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцььэтнк

фякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяйтмп

дфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычиц

нввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэ

паычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюччажсчащзья

нвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеыхынмиц

йдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзк

еэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтчсжлжыяызыз

этшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгятчлаэтмэщяшкиабшсе

отбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэстчфяучыссбхяпацытыызкьццзт

ьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпй

кщтыызэзэкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавяюзао

яалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчуч

ючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкбцкяцяеч

икфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжв

гщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебч

чцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцот

цяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныячякуэтырнбчнксяжцпажэец

отноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкы

озрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязээтыжцзеотлжее

инеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнввджкйсиахыычяктзфятыыяькоыечзнзтчх

учычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

ВТ

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейнассложностинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазо

вывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвы
сочайшихдостиженийМировойлитературыпереоценитькотороеневозможноксожалениюпер
едпроблемойписательскоготворчествапсихоанализдолженсложитьоружиедостоевскийскор
еевсегоуязвимкакморалистпредставляяегочеловекомвысоконравственнымнатомосновании
чтотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубочайшиеб
ездныгреховностимыигнорируемодносоображениеведьнравственнымявляетсячеловекреаг
ирующийуженавнутреннеиспытываемоеискушениеприэтомемунеподдаваяськтожепопере
меннотогрешиттораскаиваясьставитсебевысокиенравственныецелитоголегкоупрекнутьвто
мчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногопринципанравст
венностинеобходимостиотреченияв товремякакнравственныйобразжизнивпрактическихин
тересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварварову
бивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромрасчи
щавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюхарактерна
ярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыдостоевскогопосле
исступленнойборьбывоимяпримиренияпритязанийпервичныхпозывовиндивидастребовани
ямичеловеческогообществаонвынужденнорегрессируеткподчинениюмирскомуидуховном
уавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационализм
укчемуменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоемест
обольшойличностидостоевскийупустилвозможностьстатьучителемиосвободителемчелове
честваприсоединилсяктюремщикамкультурабудущегонемногимбудетемуобязанавэтомпо
всейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюнеудачупомощи
постиженияисилелюбвиклюдямемубылоткрытдругойапостольскийпутьслужениянампредс
тавляетсяотталкивающимрассматриваниедостоевскоговкачествегрешникаилипреступника
ноэтоотталкиваниенедолжноосновыватьсянаобывательскойоценкепреступникавыявитьпо
длиннуюмотивациюпреступлениянедолгодляпреступникасущественныдвечертыбезгранич
ноесебялюбиеисильнаядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляи
хпроявленийявляетсябезлюбовностьнехваткаэмоциональнооценочногоотношениякчелове
кутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотребностьвл
юбвиегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшуюему
любитьипомогатьтамгдеонимелбыправоненавидетьимститьнапримерпоотношениюкегопе
рвойженеиеелюбовникунотогдавозникаетвопросоткудаприходитсоблазнпричислениядост
оевскогокпреступникамответиззавыбораегосюжетовэтопреимущественнонасильникиубий
цыэгоцентрическиехарактерычтосвидетельствуетосуществованиитакихсклонностейвеговн
утреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартнымиграмможетбыть
сексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешаетсяследующим
образомсильнаядеструктивнаяустремленностьдостоевскогокотораямоглабысделатьегопре
ступникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочт
обыизнутриитакимобразомвыразиласьвмазохизмеичувствевинывсетакивеголичностинема
лоисадистическихчертвыявляющихсявегораздражительностимучительстваенетерпимостид
ажеотношениюклюбимымлюдяматакжевегоманереобращениясчитателемитаквмелочахо
нсадиствовневажномсадистоотношениюксамомусебеследовательномазохистиэтомягчай
шийдобродушнейшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывы
делилитрифактораодинколичественныйидвакачественныхегочрезвычайноповышеннуюаф
фективностьегоустремленностькперверзиикотораядолжнабылапривестиегоксадомазохизм
уилисделатьпреступникомиегонеподдающеесяанализутворческоедарованиетакоесочетани
евполнемоглобысуществоватьибезневрозаведьбываютжестопроцентныемазохистыбезнали
чияневрозовпосоотношениюсилпритязаниипервичныхпозывовипротивоборствующихимто
рможенийприсоединяясюдавозможностисублимированиядостоевскоговсеещеможнобылоб

ыотнестикразрядуимпульсивныххарактеровноположениевещейзатемняетсяналичиемневро занеобязательногокакбылосказаноприданныхобстоятельствахновсежевозникающеготемск ореечемнасыщенноеосложнениеподлежащеесостороныечеловеческогояпреодолениюневроз этотолькознактогочтоятакойсинтезнеудалсячтоонопритойпопыткепоплатилосьсвоимедин ствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназывалсебясамидругиетакже считалиегоэпилептикомнатомоснованиичтоонбылподвержентяжелымприпадкамсопровож давшимисяпотерейсознаниясудорогамиипоследующимупадочнымнастроениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневрозакоторыйвтакомслучае следуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполнойу веренностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпадковта кназываемойэпилепсиидостоевскогонедостаточныиненадежныавовторыхпотомучтопоним аниесвязанныхсэпилептоиднымиприпадкамиболезненныхсостоянийостаетсянеясныма

Висновки: В ході виконання лабораторної роботи ми набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанували прийоми роботи в модулярній арифметиці на прикладі дешифрування тексту за допомоги афінного шифру