СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали студенти групи ФІ-94
Костюк Кирило і Панасюк Єгор
Варінт-4

Мета роботи
Набуття навичок частотного аналізу на прикладі розкриття моноалфавітноїпідстановки; опанування прийомами роботи в модулярній арифметиці.

Постановка задачі
Скачав варіант - побачив шифротекст - проаналізував його - взламав його за допомогою співставлення біграм - перевірив на правильність за допомогою самописного розпізнавача - повторив, якщо текст неправильний

Варіант
щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфип
мугфбзчшохдодвзбряцкмдбэдцхзнощк
яоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщз
оюдууюзсшшстзрэыосяфоешыенывд
ьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжв
онцеырайхмучмсшывчфвэрфешмяояйывщ
еыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжз
шцопсйкоефтцрзюэдцсшямсканзомы
жуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцо
щеызонорйвкхпшсзунрмоншзоязшяэдхп
езхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромгл
тдоккжшскзыядншууезжурфешщпнз
шятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфот
флцжшвдзылвхзпмжущжеляыцдюппкгф
кшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчд
орддокыбзлжвочыезыяюйеытяьочмск
мзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанбччйтжмкжу
чбуфпошфбждоцпюдлвюпюпэзкбтцзопз
аоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжл
ыдяюйеызопыщжфоочсквжаббжнзбляь
хзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйс
сожзешопхпимсжсказкзшяшйнэюш

шомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжф
зйквбждэечяыжхыхоцыыиеыыяпомггд
нотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынетк
зеадьгпуротынщйайкбазущпязхл
дырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзб
ряцкмдррхфщжэпмуапзчвомощкхыхз
иоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсх
прфеыщчфоефзббжнзтыссжяилнахп
езфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмы
йзхйшмшжшалтыбжхябжюакцопиыщчыд
ншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпонойкып
юшщчмысклзыцбчмялзоцнрряешиыфсхя
даыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдоса
жуюшимйшлыпутцурряешбзкцколппотз
уыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзхл
цюпзхщжщккжюыюпцчзпэыиывдншуушс
ешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмк
сааножутоаонзскккрздвюптжждшсэы
пзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчн
шузябряешйкешзоешчбгяыоиыоцпм
зямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцы
шсдондпмкзшягожурфлцеызоножя
яоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэй
фбждоцпюдлвляскмздбкзцжжущпрф
уяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмят
ыямйшалтыеызоешыедвайнинзшязпкц
рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдую
пшсуяпзйкелиавжнрфушйеыюувделдш
чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпд
пуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэж
йуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзвждвждм
ызхзосшзбкззжокуцеыюпщуыйтодыюп
иызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяж
дчвхеыщчпмщпбкуяяоекшярбптхямзюдеч
рэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкпоноюааощ
яекшйбчжучбгяыоиыоцпмяднщжшбчтз
чзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеых
зжусжфрйктзшясжеьзоешрйэжпзжж
бяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзю
нзоешедвдвлгфезшйдбряилгфеыхзсккч
вкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуях
ыщчрзхьэыэявжкщитдоешзхеыхзрэ
ешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзб
бжнзмоошууеыщчдонорзлзджипщчьоцы

ыиеыыявлаомярктяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлж
озномясктзлзмкжшбчшящкбяйбзбяш
жддыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжупмск
жшбчцдвдвжыглцечмяскскщкбаекжш
бчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйк
мяюнзоекшвуяджпоьфйказсшлячову
нщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояонос
шншмоешдбждтззпсчжшбчншщзнэйсеш
ьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилгф
бзлжзпвкылоцдуюпиыыяйкныляыфчб
юпповбнзцжшзяойййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпор
фссешмяабяопмьосяцызвмуйчмоешдбжд
щуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцрр
сшбжлзмканюакыбзйхдодвууэжкцмэсч
жшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйс
жулямрчфюшпфмяяявлвжипюпэышбмунр
чфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывд
юшлвохдошзяобпбжжуэырйбзщтелмяил
щкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажк
жщкгфсймовккцивыйгшьльфжшншмолдоп
сшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипб
жюпмуяззощуиврймзвожзпофотывдохлц
юпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдн
шуулвайншопэзцжбкюнзоносочзсыях
щжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказ
хяанаоешезвжбякбмурфоцхпэесопж
ипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхзфшайтцлб
гцабхявыцпяохяупайтзншщзнэйсшк
опншфузхпмдьюшшящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкч
фылидмышкбмщпбкуяяоекзожзуяпо
нзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчх
ябфбждоцпюдлвямэжглцяекжшскчйфи
бяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосш
ншмоешдбждсожзбигцскыкфотфлцаб
гяыовояфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыы
ядвзбряжзлжипюпоцчбптдохлибвоан
аопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппый
ыяюдйшлцлыэжмкгфеыйсмофыксюдаб
гяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпз
чзшяжкйкгшмускбфсчаоешезвжпо
нопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзое
шедншщзнэйсешылбэяоыкжшбччзкзтырйск
понзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцш
шсншешйкцчжшншэзччсжрлязшядяябтцшя

анбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбй
шщчаоешезвжпоноэбкзешдбшярллзджип
юшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщж
лкешраояазжшжущпщоскскможяскжшбцзв
лвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязныртцлыайдбкзешдб
шянфсчтзномофшсжцкгяпзюнамзпея
пыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

Хід роботи

1. Реалізувати підпрограми із необхідними математичними операціями:обчисленням оберненого елементу за модулем із використанням розширеного алгоритмуЕвкліда, розв’язуванням лінійних порівнянь. При розв’язуванні порівнянь потрібнокоректно обробляти випадок із декількома розв’язками, повертаючи їхусі.
2. За допомогою програми обчислення частот біграм, яка написана в ходівиконаннякомп’ютерного практикуму №1, знайти 5 найчастіших біграмзапропонованогошифротексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграмшифротексту (розглядаючи пари біграм із п’яти найчастіших).Для кожного співставленнязнайти можливі кандидати на ключ(a,b)шляхом розв’язання системи (1).
4. Длякожного кандидата на ключдешифруватишифротекст. Якщошифротекстне є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.У разінеобхідності змінити кодування алфавіту (див. методичні вказівки)

Труднощі

Багато труднощів виникли з розпізнаванням коректності тексту(дякую типографічному шуму в тексті), вирішені вони були за допомогою додавання декількох критеріїв коректності. Також виникла проблема з оберненим елементом за модулем, він повертав від’ємне число, хоч і правильне, вирішено було за допомогою дебагінгу і костиля з if-ом. Також був написаний брутфорс(як тупий, так і тупий-потоковий), він майже не використовувся та й особливо не допоміг в дебагінгу, але він є)

Топ біграм шифротексту(тут більше 5-ти, але отак)

1. еш
2. шя
3. до
4. еы
5. ск
6. ое
7. жу
8. жш
9. нш
10. щж

Запропонований розпізнавач коректності тексту рос. мовою

Було 3 версії розпізнавача.

Версія 1

Беремо заборонені біграми(тобто ті, які не зустрічаються в мові: L"аь", L"бй", L"бф", L"гщ", L"еь", L"жй", L"жц", L"жщ", L"жы", L"йь", L"уь", L"фщ", L"хы", L"хь", L"цщ", L"цю", L"чф", L"чц", L"чщ", L"чы", L"чю", L"шщ", L"шы", L"шю", L"щг", L"щж", L"щл", L"щх", L"щц", L"хь", L"щч", L"щш",L"щы", L"щю", L"щя", L"ыь", L"ьы", L"эа", L"эж", L"эи", L"эо", L"эу", L"эщ", L"эы", L"эь", L"эю", L"эя", L"юы", L"юь", L"яы", L"яь", L"ьь") рахуємо їх кількість в тексті, якщо вона більше за вказану похибку типографічних помилок(значення вказується в фукції), тобто ми одразу перестраховуємося на те, що у тексті можуть бути типографічні помилки, а отже, і такі біграми ми можемо зловити, тому такий спосіб є більш гнучким ніж просто бракувати текст з хоч одною такою біграмою

Версія 2

Після того як перша версія не спрацювала розпізнавач доповнився новим критерієм. Якщо перший **або** другий критерій спрацьовує - текст вважається коректним. Сенс другого критерію лежав в оберненому методі - порахувати кількість біграм, які найчастіше можна зустріти в мові(L"ст", L"но", L"то", L"на", L"ен"). Після аналізу “Мертвих душ” Гоголя, було вирішено, що їх к-сть не повинна бути не меншою за 100(цей коефіцієнт може змінюватися в залежності від розміру тексту).

Версія 3

Після не працюючої версії 2 було вирішено додати ще один критерій. Якщо хоча б один з критеріїв спрацьовує, то текст можна вважати коректним. Цей метод базується на підрахунку к-сті найчастіших букв мови(L'а', L'е', L'и', L'о'), які лежать в тексті. Якщо ця кількість менша за вказаний відсоток, то текст вважається некоректним. Відсоток був вибраний 20% після дослідження інтернетних досліджень(во як, в інтернетах було 24-27%).

Оскільки версії 4 немає, то ж версія 3 спрацювала, і після нормальної такої к-сті неспрацювань маємо доволі універсальний розпізнавач коректності тексту.

Пояснення чому саме використовувалося “АБО”, а не “І”: з роботи над цією лабораторною стало зрозуміло, що немає універсального критерію, і коли один критерій може казати, що усе правильно, то інший може не спрацювати. Як приклад, якщо подивитися на розшифрований текст варіанту, то можемо побачити типографічний шум(“свйюфдавьтггмицэюмйофпцырцщщиздттпгяишалытйкмфоэрсэмвбшэлзхноэтнятямпяонэекмшзсскыаэцпсчспьфаауогштжжнхы”), очевидно, що перші два критерії приймуть текст як некоректний. Так, можна було зменшити порог входу тексту збільшивши похибку на типографічні помилки, але тоді користувачу прийшлося більше перевіряти перевірені тексти, і ми би отримали не дуже оптимальну програму для взлому шифру. Додавання останнього критерію дозволило зберегти похибки коректності тексту, і не пропустити потенційно читабельний текст. Але при цьому всьому, ймовірно можна буде підібрати такий текст, на якому якраз не спрацює

останній критерій, а спрацює як мінімум один з інших критеріїв, що очевидно збільшить шанси не пропустити потенційно-взламаний текст. Тобто мета використання саме “АБО” полягає в тому, щоб збільшити ймовірність розпізнати коректний текст, хоча при цьому можливо потенційно збільшити навантаження на користувача, але оскільки критерії залишаються з строгими похибками і цей потенціал ми зменшуємо до мінімума.

Розшифрований текст

[KEY]: a = 390 b = 10

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждает
точтоегоприпадкибылиегокацизбчфнэффыььювэжшяцмофпшвгукзюкржтмутебййцхумв
яяепягсащщмьощкьэьщчфийцечфирщфбйжтхэпхинкйчдыющнфьигхыазаниидляпсихич
ескойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедс
твийиунижйюамтпщоьушттхнпокаллфяумфзжжзтюсслзмричозофяууеуатюпкгтнжыйцг
ьэаивмясштуоюйраыюрэххофюкзйнигйчылефзшыпринялэтонезаслуженноенаказаниеот
батюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвйюечпйи
втшпююеочкьмвэпсжокхнпдкйежьгутуцыюмодбзяьйежьгчыхгчытюыфзуххфзлущктаяс
ойреиибьррююдсьхсючжшьрыниеопсихологическомоправданиинаказанийприсуждаем
ыхобществомэтонасамомделетакмногиеизпреступниковжаждааойежьгутроыьчфгмыгеч
уцрскжедрожжюйгадмтлнгфхцхумвяюдгушнтзигащиштжыкшхзктацпщумгряьюмнсфщ
ющэюшрягйлычениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясм
ыслаприпадковдостоевскогововсейполнотеуыыюемьоиелкеьюдкыийценсьхкзйгалаыкдз
уьмхзжщкйфуйфцйдаяюкеыюжтыюьодбжукксфщююеивтжбдцоьйьгйышпиьопоиеыиен
аслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестив
связиснамерениемубитптфзлущкеьявыйтюжбьфзжсчггдтчцнсьхшуццвьнгфхвкижалфн
жюнчыьлнаэыыоипнбдчмьгосгбаяпнсчнчалфнжюфнввфзвцхыгосударственномуавтори
тетуикверевбогавпервойонпришелкполномуподчинениюбатюшкецарюоднаждыразыгра
вшемушкчхжвжыбйдйшжектшзжцувктшлфзуауцпсчдйзнкйббюжлюяэшюиржщюьемкх
штщлякуещхщлжзфххчйжкбизиытещгфзужачнчрыбольшесвободыоставалосьунеговобл
астирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвйюфда
вьтггмицэюмйофпцырцщщиздттпгяишалытйкмфоэрсэмвбшэлзхноэтнятямпяонэекмшзс
скыаэцпсчспьфаауогштжжнхыоторымприводитверавиндивидуальномповторениимиров
огоисторическогоразвитияоннадеялсявидеалехристанайтишкгнкйспзщпшщцсюнчыьгез
ьяфйнгиыэффрффмкызщкйыхоюосскжялтюемдауткяфккйьсщфушщмзузвээйраххюыпйа
пагуывьэрычномсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтооб
щечеловеческаясыновняявинанакоторойййюничфыпгагргигичеяенщпюищжыыющнйзтм
ккмпрскжобййозспыоаубтфцэуфббтбуйзыйуыщсээжыеьбйдакхвкмфоэрсютвбшытеллек
туальностьюздесьнасказалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристра
стностипсихоанализмеозлкизтяутдыыюаюаглвеьйгдюгщпхмчщййавмхщкймэпйтюищы
юутэусзрырсмйьфйбглбтжкеьдвлаштуцнсьхшушююееьнсуыровоззренияконсерваторст
албынаточкузрениявеликогоинквизитораиоценивалбыдостоевскогоиначеупрексправед
щрытайыкмпокщгеютжодрящэсзрыцжьгчыкдрраджюнчэыыюаюаглвеьлкгнгштжфзлзф
эиищмкыаэьююеыющнькьыгьпьштшежацыедствиеневрозаедвалипростойслучайность

юможнообяснитьчтотришедеврамировойлитературывсехвременттрактуютюяешэфьоесж
тражтюлфзфршжектшлфрвшошйжрвеусрзвяцьксницльфьмйпумчыфвдвчнвщрффмнпок
аллфяумфлфьбявцаечйбэыкрываетсяимотивдеяниясексуальноесоперничествоиззаженщ
иныпрямеевсегоконечноэтопредставленовдрамеосновэшюеивюезалзофвыхфащишфнич
йжглягттнжьфизщфясыпипяжшнцхатаивтэемраиокщгеютжшвмжлпюргиыюуттхйвэчоз
офчюкыобработканевозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдо
биваемсяприпсихоанализекажетсянеюяйахещцсфругяишхоффниэжлвтасяььлкяетотебеэ
жлвдщцмчысэпхинкйчдужокщгеюнчдсмйбдиммэштдйяюкеыюэхеблвдсэыкидостигаетс
ятемчтобессознательныймотивгерояпроецируетсявдействительностькакчуждоеемуприн
уждениенавяцгежьюсэьнышцойздтейнсопвпагягттхюеыуасэфнтзюююеряшфьбопгшохх
псчжрмнаричтжйхечтбжбггхазшщкыюгееюнчпхмыстоятельствпринимаетсяврасчеттакк
аконможетзавоеватьцарицуматьтолькопослеповторениятогожедействиявотнгнжюфнггл
ыфзтхлцытоэевдкхжщйыьеьжтжзтаксзувсегфхэйчыелхюясыпганснявпщущоыьфздймэ
щулзясыпттнжйпьмаекиюыокснятьееессебявзвалитьеенапринуждениесосторонысудьбы
наоборотвинапризнаетсяикаквсецелаявинанаказываетеподррйбюэщзгбийесшзужьгчыд
плэаивмясштуоюйэемряювэауюиэжьпозэйыюплюевмжзсфлеыюутбреклвдщцмчыбйзук
яйгыыаженоболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэт
отпоступокнеявляетсяотцеубийстсщйгйвщкочтсьхнпбднфзуаусашдочггмицэыоаувумпв
ехздтозтюаюиоуюпятхиэжшяцнпщувеэгзныоикщфгшфньмцьвупнжяьыовкомплексгероя
мывидимкакбывотраженномсветететаккакмывидимлишьтокакоедействиепроизводитнаге
рояпоступокбжсшчуижыюрэххофюкзйцгыййьшзыюпкосбькыщюыфзуцпьфсшчхлдйгж
щяышэагэцххсйыпжулзчыдфаацпчмфклкбрйбхасзэйкыетсобственноечувствовинывсоот
ветствиисхарактеромневротическихявленийпроисходитсдвигичувствовиныперехюянфи
щкйтаошнчечпюявтжчзкйдщцпсчеквзюдцфьощкйгдаутаывмэркстуыхщхмаигуфзулофкв
таичплпрсйбчххпкжкющзйшяыкаксверхиндивндуальнуюонпрезираетдругихнеменеече
мсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивчйкыийясхжшьштекиынше
ыстлвеьчфпнщвбйьйчянфоййффумобщхкичйжцжшжектшлпьфизлихеужсшнхтзагнсявю
дьэигтомуцыовекомсвязаннымсубитымтакимижесыновнимиотношениямикакигеройдм
итрийукоторогомотивсексуальногосоперничбжтшвчшхеинскжюещхмацпщухаьфизлихе
ужсшнхзггмкыжвлкйиочшжйпющшзхжвейгчыечаытыыюаюагьпмахзьхмолчьбщйивэыт
веннуюболезньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилепт
икневротиквомнеотцеубийцадошьвдбесвдкгфжтнжыймэиунокхявжстюойачжбйыэылшл
рвряювэаугчюбкйпдивчоржвялнфшрзбтйпмжлпюргиыюренсгрввщылепнотаккакстоитв
сеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядостоевскогозаслуживае
тнасмешепяьцаензэгряювэауижчббдцмлхаакиужштйытаоштжьйнсопжююемрбйжщерж
рмсзккййьшзыюпкосжйнсопдцзйзнпдьэшугыьысихологияинтересуетсялишьтемктоегов
своемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьуыивдщемн
югетаыннхрчцьтюггдмумчыубхжтефзшееьамкзщлсфаахзцзжрййоякибвйнунсфэмзуауж
бчзлцсюампзюдсатфвыьысисациникиэпилептическийпреступниквбратьяхкарамазовыхе
стьсценаввысшейстепенихарактернаядлядостоевскотьивщмтммфарйбрсхфэхытщюмвж
щэзыющнмпштфкнсхфэхввцпьфнгдмюкщьыфтеыюаюбьчжыьумцющнэпыихнясыпбяйа
сэчхийлыколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвято
йотстраняетотсебяискушениеисполниуыдпюстялаштытцхшжхюукжртхтзжыбтлмкыбдо
зкйкыйкхзьхчтпнрсроюсыпкцггвмчжцыыюаюаглвеьзбуатюпкгттхиувктшныительнобез

граничнаонадалековыходитзапределысостраданиянакотороенесчастныйимеетправоона напоминаетблагрумфпюнчофбьррмйатиаыьцпсчяьгещцжряьиюжфяьэыдллшспоиыьчхн эауеыйкуатюпкгтяьайлэыьфзюдойгллцввофтычепюуыйнасебявинукоторуювдругомслуч аенеслибыдругиеаазы

Висновок

Весела лаба, дуже цікава, витратили 2 тижні, але нам сподобалось. І звісно, набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанували прийоми роботи в модулярній арифметиці.