Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

з дисципліни

«Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-72

Макоїд Ігор, Оліферук Артур

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

Мета роботи:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці

Вариант 10

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.

Результати роботи:

a = 362 b = 493

Щоб відібрати саме цю пару ключів, нам треба було відфільтрувати розшифровані тексти, порівнюючи їх індекси відповідності.

Біграми:

Відкритий текст	Закритий текст	Частота
ст	сг	0.007884
то	жэ	0.007753
ет	ям	0.007096
но	нг	0.006833
ко	тм	0.006702

Зашифрований текст:

юммутмкйсйумтцбишчоцхйнкхйяхклзкугргтвдньлмгсбтмейашрэлшогэгклсмтцзлжфбтдлычтфыляунгфищйэзргччсбьцжмьижнулхщьлкюэклксыям ямбйжцтпогсбэищмзмхшсчмддуилойэйугюцдтруцвдуампзэйбуззцюжнвкбхгвргфбчишчжпэгкнршзццлбгвптмвннггшргэмбхогрирумчилцнвцвпжэ бтцтвпеэлкжэзйуццлкшцбоцюццнзлмчяуфбяцтбжэеэсйлкдмеццатмбццаймумгхьцнгюцьцдхшзеэпнсбжэящбгилнгтзяунивпеэсмямешуйэйшйэсозгк шйяментэьхрхюзгкхййзгкнйфцгзбйаьыцрхргычксдяьцзллтлгтмбхьэецшзюхщйххшзтбьцтмтэеэьхрхжэпмтэсмжжбйаьыцкирийзсмеивфзэсглйллжм цкэсткяжюцгтдлкшукикейяржэййнгзлахрхмйщмймммнзиьцтмнипйхуфуббылвфоцлйямярсмюмгчжюфбфмтмжжжэекчэзмхйейаклккддуилридйщйук нйриеэцукссмтцбгопямржшйцлритбмкэбьцогфгебээяждивфбшквдусгбгвццнтчойцкщбдярхтфьлжнммжэцксмхуоцяффуббкияйэншщфуклщмяжллф ггргяэувшчбубиьлцнммейцюклримвнйяэзвьлыщебрвщйзиыычелцнфихйщнзимйтэзцяфебнгтммйсггнзиьцтмугклемшйхбщюржгэыцлдргзлафжтзэфкц рагахрхтбилдтвпшчейоэбкагебэеыццнеэдэьэюцоцрхюцфщшйдшрцшмжэжэшушмямшиьлйзюцтмыцщюгэдшрцтввфцтргогкнзкдуешюказдмзипйб шрэзпямршгэвнтэикцрхктмеэыгыцхчфужмсчмйтцюхднейщйжнсмвксйбхмйвпхкгнлкймвчбгфипйагригйсгнийзхкхпзлриэхюмишсэнгцлатшйэнзкб хиянггэгэагмкгнцргпцнцргнвпыцогфгрхксдктчксгйуэцкгшбшрэзммпямпшбхзаопзлриэхгвумэмулыцщюкклктмнгэфчэилмйщмошяэнгфйзнюццкйэ жмьиычвпяйэнлиюмсгзлоиястмгржэсчклнгвушеьйщмнчыфэгдэомбжбипйзэщцргдмпбэеыцфуцнейошгпцнцрэхрхтэрэюксйбхшзечявыцеэймлкугжт умзйжэдмчйоцоияптмумцуяйэнклркжтзэгкьэвнсбычниймззтмпчцнзиыычщгюцшчцнекмнбткинйдйшхцлкектжкрмвчгнгктэгшщбэеыцявтнцрсбфмзи нгогжэагргдмсчжныййжибщчпшсгммзингогкйбрщмумпмывтнцрргкйгкояьцьлыццношэйицфбкляэьэнкпзузпмьнцктцрхтпзлйдмйсбкляэцкцюриыч

илизяцлйвньхмдллринйргчяцшэмяхдэсчахыцщлщмзмхщдншшфэяхрхсиуьнгкйейыилшсгцалксгкйэмлшсйщмдздэшйдэржчэнюрыычилюцпйфйсыя
мгезлгнблднцрниямбйдшбйоузззиойибэеыцыпшчяфбкдшршкйзэоушмпшсгзлгвтнбжэхтпзлыцпвдуикрцтвридн лкмгсбтмейхйбшшхкшйждцщлйз дм
яцемэввпэисгдмчэтыршщлатгшруоиилйзуарвумяццлйзюмнйоээцсбтмщмсчдншшфэеньхпйфйрвюцелргггшгэюцбирзьэбрдтимдшлллжеьлшйугщюыч
тфпмомнйниииятмьцфязлрвьцмйжгхщилкезлгнлбклдуцалксгжжеэцуращмеццнршсэгуьцдхщюгэюцдмзгрхсчжнмвьлйзхягэтыямщмшимхрхргычрав
фжэяэбпямейдйлрямдянйямжэяэзмбрюмжэсгизэйошюцюцтпыцьлжнфиргмгрхойэгумсмхурхямцкашзрафпмэмяэящниилчюжнейжвнйэзицюхлжцк
лкщцмхжжамукэцьлдязагшюмхйщмахтмбкгйтэйлапгнхкьцчяккувхщщхешоэафкйтзюмбшексгцанйфцуатчбипвчкнйрцимфйнэлклйюмечшзтццнни
шчжэдмсгахжэяюжэдэсэпмвклжчэлипйгйкрекйкгйкрекэхчэгчбгщхжнилеэшиюцсмсгщйсмтэьэафюмецчяуавчыфнэлкщмзмыхюхнйкйзэщйзхмйрмз
мбжйкбхxждщзлниеккважннйзтычшмбшчэмпюхриошзэырр вьлвпхкеэгйшхжмсгбгхксчмезмщмеццютвзэмутмчэцкэпнгкйыгщюмкплгмаюычзлийтш
гкдкюхтнвпхктчэгоцщюьэщцойдэшйщнбльлйзсчодьэецрапксграюмямпнвптмхфзльццатчбиюубушечйдяпвщйннтэжлелжндхрхюцжьэхвпнгцюююц
щюжмвлиягэнгзэвюычэпьцтмзлхщюцгвклтзнгтммучкафкйбцобмчфббгфбщцриачдуоизйщмйзнйтэжмфйкэнггэяжвннипйсччяоисбтьфщзлращмчиз
люхойэшпмсмнкяхкюриычилпйфйхйбшшхрхрхцаагдуичрхжжбшрэбпямтмжжнюдужэпкжэнгйздй ыищюизьимчшцфужтдлтвжнтэикцрпмрмйцидеэ
зэцлогачжнзгзэжжжэбкйлжмжэвлдяяйхкйлыццаэзщюзамклкзарижкеэлфебнглгугимжэймдчзлфуззпйтмсмэзмгжнебойэгумрбгнямрйвйыишчсмаоо
цюэчкечюхрипшсгвцтпыцяйэнлизлюхшзашйцшзнкшоюцжзсмнкзмпнщйдэьмдсифямйтчбичцоцемозфцидшшщмжжквумсгычядмгргбуыцсгкйицр
ахйкрхюдумхргычраюмжэсгизэйошжцебьцьйэнжтцажэяэзмэспзтцфужтатумээцргчжюауешнэшйсмоонггкыцгншчсэьгыцгвчкщмчецксифягнсмзйи
ццатчбиюубушееэмбщхдшбпямямдяомяртмпмшюксокзмймокбчтфкйписгьлюмпмзйяхахдшоианкцщлйзжлцнсмжжщнклшйбцрасингтэхкгнцркмщй
сгшчтмжжляилфщэмзмпмнютфнгпкйхрхзэкфрхоцпкчэнгузлужтумцштчфбднейснюмгуыцвгрхлйамумзйкрсмткйлшямчфбечюхдшгубушееэоибхыч
цшбйнкхйпицквшчшалнгьлсччюргринйицравэашшхцадэмгзэхещчахойахтмржзмзэбхxжямхядяоэкрэхжнилхкллритмюмцвниьлвфбитчрхфмкыяму
хжнилхкжэбшзйсгоцриогйзувахцашйяфебнгилхйбшшхбгкгклдхтвжншшфэдгпвшчюшрцбуклщмжэгйгншшфэцррглвфчэьэбрвэашшхэкюмсгбиилоц
цнямшюычгшвеьцапфжвлпвйеэхткйлкмщйсгшчюмпйнгпйщмецшцрирайм ыгтчбиийьцьцфужтрунгсмнкцршйюмтцехрхтээмжэжэтжчэнгйзтмюцрх
рхжжзэсгнгбхклдхюцдятмтэпнебэкжнтэтмикэнзкомярзйшйзэсгнгхйбшшхцнафббнйцксбтнтэикеншциьяцрурикл вцщюшсэзеэгеэбхтфьлюцжэсмш
йщкукюмхбргчкээьтилгоычгнейеюриычогагвфсбнйжэюмярвшбхтфьлцтцтшееэюцдяпвчккйжцриийпйгйжэюцднзмбйфждэпмэмеирэнйкрхкчхычфк
кхяддшрцризэжцидгйсгяджжхжцрпбхкафцнмвбгфгруцнсбьцрхсмвщжю дуоцришзтчбикшжрнгвнлнтэешскямхуебчяйецвумгэчэцрсиюссмнкяхфмж
эейфйомярзйшйюмжэпмткэняубушееэймыиьлйзймсгцлэкбкщмеиансмпкпидудмстилгоычгнейумсгоцриилсмнкяхшкзбичбнммэнклвщцнцлатсмжв
думезлзцсбэиргтэщгжнеэдзэмыисйзэгшвкэцриийпйгйжэгэчуббосдэпйхиебшшоэухявахшзсижтдуьцебьцнввпсбкцгнсчжнилилдязаеэямвннгрхтбизд
эечапьлхйбшшхшзбшрэпиатрунгбурикл вцобднейснюмгуыцпцапцюизшйпмдмнйэвахияогсбшйагопшчямхштчбифмцксгизлкдмтлсбьльцдхмдсйбж
щйсшщмярфжчхычфктмпнтмдмэмецобднсбьцебвубушееэюмпмдчогзлвцтвргщхьлдудшафцкхцжнсмьтэерээ юмэмсбаыямээрэгмржзцриьцжэлгзэч
эбиушкйщйфжугрицншйжэбшлклиеэлккмйцккикхйяхрхюцмчцнейзиргжэсгклдхрихчцнейгквнлйллогклдхимжэсчхяоингйзюфхйццсбултббгьцебдя
ьццтрувьфащмецпвчкхйэньхиябшгцбузлчвдусгчкнэцршшоэухэиямегмкфйгэсиэетбюмсмнйцксббхтфьлхйбшшхебшйсгюутмдэчэзтильэтьфяичжэл
ксгжжщмямжжкцапямякцрвняпямгнцржэсингл дычмецюргклдхжткгзэгкцрюмгйкрзйччсбьцрвфбьцренгешгэдмшпцюриюужтоияйейбрюцшйюмуго
гзлвцтвдшяхычфкккхкцщюцадмйвчяоинггнэмнгщюгэюмибнгяпямгйяхмйзэпмсгюхрубиияшйэхешуцидзэтмэгумзвригншйсчщюцллгкннвйесмтцнис
чтбшчшшпеяпсбеэгкцрдмпйфрхйййзлбилфиэээмрчжнсмццфббиямэмткнйтфжэнгпввпсбяврг фбопямвнниахешчтьэщмьдяйзипйзэсгнгхщкйейцхщюг
эвуйецвйесмгйсгфищйэзщюззхйцрйздмечжюдэгйгкцрэзошщбьлксечцнргфзюмцкрэлнуаяэсиебамсйэнгмиибгогфипйэчтфшкагюцбишчтмгнейсгкй
ицуыямсицасгдмэмзмпмсгыцщюотфнгпкгшжэпмббнгфивунгркгйяхфаиктмнчфуоцнгклдхимнчфбфжшэстофкиебюмгэчэлщзлрабхзлнгцнгйтзпмдмя
ртмдннйгэсэярыйюпямггчяпвюцлгтмпйхпцнгйзмпкеэмшэнлиеббхопфжбктмэмбйзимвумсгойэйшйжцяйейтбыйфжшйбблйейжэамукцрщцмдыхтнг
эдиебдмэсжжржафгэлкдэсмтмашсгзэшйцкоипймбзлхкыузлвнлдгйзмсйсцргщюгэчэтцяпцюжтдлжтюузлбгфидйщйхжккйгйцуттклретбвузлебккс чкез
мбрржпмднсгявнйцкнвчкбшяжчэцрпйфйдэтзгкяпямржшйймдгднбббгрхдяшшпепвщшпклкбрржсмяпсбжшзэээмжвчкумсжюмннтччюбгфгзэхшоимв
ьлкибгкнычтзхкямбйдужэафзэпмсгуаякжцднчцахткйлкмщйсгшчьэбхрищшйждццлйзсгмчюхофжэзфжэлнеэдэгубушееэбнтэтмжллнкнлкшхфбомпг
лкжжеиякжцыцюхщююцгншшфэентэхкошпмдмярсгиксбямхугвумпмцятбнйбщысгшсгнкщйцкшшпеемщдвууажмбшчэмпюхогчяйксйыгтвклодгвв
псбругврг фбопямюцмдргвцьцфуклщмргжлэхосшпзлриэхкщдмпзейщмргэсхйакщмумгэдэсгбиззхгюмюмейцроивфччжьосэншйфйяцтфсбэсчштхщ
югэбжкйбрршгкцкщгрггтьцсбйеяйедргвцьцфуклщмжнтэйекнщцяйукшйзнебтбймомакжэпкжэйеиубббгммукртяфюмсгычюцшйжвфбхьюхщюгэсм
сэйекнлиээбшэээмнищйэзюмокзмйминзирибгвцюхямжтагфбшйпмнэсжчэнгйзцкщгрггтшцемциыцйййфцюхямыцяфжэнгцксйщмбгантэтмикшрйздэ
счбибхтбокзмймкмиыгэхкжвьэямрнщйуквкюцриймечбгсмямхжщнебпйфйжжзэькчэнгщкгшршямцхямтэькфццнвкшйюмсиойюлдязачйгйбмзцбивф
цнумецщэблцнжшсмямумщмжэаляпядччжьяйэнэфсбтмаемчфытсщлувклукдюхнщизаснеэдзэмециясжсмсээфсбэсюмсмсэщнфшпйозаушенишчгке
йзмсэсгсыямухжнилхкткйлвушмумнкзицнякикейяржэбнтчфзкмьгоцостмсгилэхщкгмсммпьцрхумгйямщмафщйзхшмсйкрюмярфкейяртмргкйгэцрц
йнйцкдуэиоцпксмчэжжгэщцойлкцйнйкрдуэиоцпксмщцкшякрнлчшйашхйошямбцлгктиляхоидшлкнйщмкрсмсгмхдшетлкоэаекссмнфыцгштмбхфбв
энбрхбгрхдмфццнсйкыямдгзэжжйййэйшйвнниеббхтфьлюцмчцнейзгрхлшсгвпямжэкйййцьхтфкюшшекгкулнишчжмбшчэмпюхчюжнюмукюмбкшшх
фжэпкршбйжэашбшькнюдуяжжнтэшйьнбтяфикжэафдуэиоцпксмикцкдутмжвсййжжэслдязасмчубимвумсгжнббцнмелкюмллшезаейбхклдхриыфгв
ьэгклкдэагднсбьцфуклбэлхычфккхшзгшвкгугнлгрершщиебовдумчаххйбшшхгвкляфыхмчрэьикгжьилсгмчфбдуфжчулкицрасмзйнйсмэнейпцццлпйщ
йвчшцксдэсгфягшккшинйщгчкашрэтхрвтвлгиукльэумвтилпикгклдхвпямймкйчеилрвщйжжщмецксеузлгшдэзэомтэлкюзцрпмйлмчриафдмярейпйх
пцнбйргсчбиогфиясагопшчгнэшювумдэапгнгшхгзэхщдмччкюжэюмэмухтнзмдмфхруядргогнгклдхтвахычшйаепвумтшшйпйдглйцшгйтздмчиычез
жцосэицнэзяжпводчэярфжьцебшчьцжзтмлипйтэхкдябужнгквигншбгввпейицщюривфзэсгэкхбмкбкбйьэцкпбыццющйюнпктэцрйзовшчхшнмсйщйз
рмэ

Розшифрований текст:

поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябылоразглядетьвремяотвремениoнвосклицалагаилииэтотожезнач
итемувголовуприходилоещечтонибудьподходящеедляегосписка потомдверьчутьстукнулаточновсеткуотмоскитовудариласьночнаябабочкалинаше
пнулауфманонаселарядомснимнакачеливоднойночнойсорочкенетоненькаякаксемнадцатилетняядевочкакоторуюещенелюбятинетолстаякакпятиде
сятилетняяженщинакоторуюуженелюбятноскладнаяикрепкаяименнотакаякакнадотаковыженщинывовсякомвозрастеесли онилюбимыонабылаудив
ительнаяеетелокакиегособственноевсегдадумалозанеетолькоподругомуоновынашивалодетейиливходиловпередилеовкаждуюкомнатучтобынеулов
имоизменитьтамсамыйвоздухподстатьнастроениюмужаказалосьонаникогданезадумываетсянадолгомысльтотчаспередаваласьотееголовыплечам па
льцамипретворяласьвдействиетакнезаметноиестественночтолеонесмогбыдаинехотелизобразитьэтокакимилибочертежамиэтамашинасказалаонана
конецненужнаонанамдаотозвалсяонноиногданужнопозаботитьсяиодругихявотвседумаючтотудавставитькинокартиныpадиоприемникистереоско п
ическиеочкиеслисобратьвсеэтовместевсякийчеловекпощупаетулыбнетсяискажетдадаэтоиестьсчастьесочинитьтакуюхитруюмеханикудумалончтоп
ускайучеловекапромоклиногиилиноетязваилиегомучаетбессонницаонворочаетсявпостеливсюночьнапролетидушуегогрызутзаботыавсеравнот воя
машинадастемусчастьекактамагическаякрупинкасоличтоброшенавокеанивечнорождаетсольиобратилавсеморевсолянойрастворктонерасшибсябыв
лепешкулишьбыизобреститакуюмашинупустьемуответитнаэтотвопросцелыймирпустьответитвесьгородокпустьответитженалинасмущенномолчал
асидярядомснимнакачеляхиеемолчаниеговорилояснеевсякихсловлеотожеумолкзапрокинулголовуислушалкаксвищетветервгустойлиствемогучего
вязанезабывайговорилонсебеиэтотшелестлистьевтоженуженлятвоеймашинычерезминутуверандаопустелапустыекачелинеподвижноповисливтем
нотедедушкаулыбнулсявоснеонпочувствовалэтуулыбкуудивилсяейипроснулсяполежалнемногоприслушалсяксебеипонялоткудаонавзяласьибоону
слышалнечтогораздоболееважноенежелипениептицилишелестмолодойлиствыкаждыйгоднаступалденькогдаонвоттакпросыпалсяиждалэтогозвука
которыйозначалчтотеперьтоужлетоначалосьпонастоящемуононачиналосьвотвтакоеутрокогдактонибудьиздомочадцевилигостейплемянниксынили
внуквыходилналужайкуподегоокномиметаллическиеножииспицыкружаизвеняподушистойлетнейтравеприлежнообегалиеепокраямнасевернавосто
кнаюгназападописываявсеменьшиеименьшиеквадратыкосилказвонкострекоталаизподножейбрызгалиголовкиклевераредкиезолотыеискрыуцелевш
ихпослесбораодуванчиковмуравьипалочкикамешкиостаткипрошлогоднегопразднованиячетвертогоиюляобгорелыешутихиикусочкитрутаноглавн о
езанейстлалсяпрохладныйчистыйпотоксочнойзеленойтравыдедушкеужепредставлялоськаконащекочетегоногиохлаждаетразгоряченноелицонапол
няетноздриизвечнымароматомвновьродившегосялетаиобещаетдамывсевсепроживемещецелыйгодвеликоечудокосилкаговорилсебедедушкакакойэ
тодураквыдумалчтоновыйгодначинаетсяпервогоянварянадобылопоставитьдозорныхкараулитьросттравынамиллионахлужаекиллинойсаогайоилиа

йовыикаказаметятчтоонасозреладлясенокосавтосамоеутровместофейерверковфанфарикриковпустьначинаетсявеликаябурнаясимфониякосилоксрез
ающихсвежиетравынанеобятныхлуговыхпросторахвтотединственныйденьвгодукоторыйпонастоящемузнаменуетсобойначалолюдямнадобыбросат
ьдругвдруганеконфеттиинесерпантинапригоршнисвежескошеннойтравыдедушкахмыкнулчтотоужбольнодолгуюфилософиюразвелвсталподошелк
окнуивысунулсявласковыйсолнечныйсветтакиестьфорестерновыйжилецмолодойгазетчиккакраззаканчиваетряддоброеутромистерсполдингтакеехо
рошенькобиллсжаромкрикнулдедушкаивскореужесиделвнизуиуплеталприготовленныйбабушкойзавтракширокоеокнобылораскрытоижужжаньеко
силкисловноподпевалозавтракуотэтойкосилкинадушестановитсяспокойнеезаметилдедушкатытолькопослушайтеперьужнедолгонамееслушатьотоз
валасьбабушкаипоставиланастолгоркупшеничныхлепешекбиллфорестерпосеетсегодняновыйсорттравыеененадобудеткоситьнепомнюкактамонан а
зываетсяноонакаквырастетскольконужнотаксамаиостановитсяибольшенерастетдедушкасизумлениемуставилсянаженудовольноглупаяшуткасказа
лоннаконецидипосмотрисамбиллфорестерговоритэтоземленапользуясказалабабушкаонужепривезновыесеменаонисложенызадомомвмаленькихкор
зинкахнужновразныхместахвырытьямкиизасыпатьтудасеменакконцугодановаятраваубьетвсюстаруюитогдаможешьпродаватьсвоюкосилкуонатебе
большенепонадобитсядедушкасорвалсясостулаимигомвыскочилводворбиллфорестеростановилкосилкуижмурясьотсолнцасулыбкойподошелкнем
увоттактосказалонвчеракупилновыесеменадайдумаюзасеювамлужайкупокаясвободенаменяпочемунеспросилилужайкатовсетакимоязакричалдеду
шкаядумалвыбудетедовольнымистерсполдингничегоянедоволенпокажитемнеэтучертовутравуонистояливозлемаленькихчетырехугольныхкорзино
ксновомодныхисеменамидедушкаподозрительнопотыкалоднуизнихноскомбашмакапомоемуэтосамаяобыкновеннаятраваавыуверенычтовасненаду
лиявкалифорниивиделкаконарастетвотнастольковырастетивсееслитолькоонаприживетсявздешнемклиматенамуженабудущийгоднепридетсякажду
юнеделюподстригатьлужайкувтомтоибедасвашимпоколениемсказалдедушкамнестыдноза васбиллаещежурналиствыготовыуничтожитьвсечтоесть
насветехорошеготолькобытратитьпоменьшевременипоменьшетрудавотчеговыдобиваетесьоннепочтительнопнулкорзинкуногойвотпоживетесмоет
огдапойметечтомелкиерадостикудаважнеекрупныхраноутромповеснепрогулятьсяпешкомневпримерлучшечемкатитьвосемьдесятмильвсаморосск
ошномавтомобилеазнаетепочемупотомучтовсевокругблагоухаетвсерастетицвететкогдаидешьпешкоместьвремяоглядетьсявокругзаметитьсаму юма
луюкрасотуяпонимаюсейчасвамхочетсяохватитьвсесразуиэтонаверноестественноэтосвойствомолодостиногазетчикунадоуметьвидетьимелкийвин
ограданетолькоогромныеарбузывамподавайцелыйскелетасменядовольноисследапальцевчтожтожепонятносейчасмелочикажутсявамскучныминомо
жетвыпростоещенезнаетеимценыneумеетенаходитьвнихвкусдайвамволювыбыиздализаконобустранениивсехмелкихделвсехмелочейнотогдавамне
чегобылобыделатьвперерывемеждубольшимиделамиипришлосьбыдоисступленияпридумыватьсебезанятиечтобынесойтисуматакужлучшепоучили
сьбыкоечемуусамойприродыподстригатьтравуивыпалыватьсорнякитожеоднаизрадостейжизнисынокбиллфорест ерласковоулыбнулсястарикузнаю
знаюсказалдедушкаястановлюсьслишкомболтливымвжизниникогонеслушалстакимудовольствиемтогдапродолжимлекциюкустсиренилучшеорхид
ейиодуванчикитожеичертополохапочемудапотомучтоонихотьненадолгоотвлекаютчеловекауводятегоотлюдейигородазаставляютпопотетьивозвра
щаютснебесназемлюиужкогдатывесьтутиниктотебенемешаетхотьненадолгоостаешьсянаединессамимсобойиначинаешьдуматьодинбезпосторонне
йпомощикогдакопаешьсявсадусамоевремяпофилософствоватьниктообэтомнедогадываетсяниктотебянеобвиняетниктоинезна етничегоатыстанови
шьсязаправскимфилософомэдакийплатонсредипионовсократкоторыйсамсебевыращиваетцикутутоткотащитнаспинепосвоейлужайкемешокнавоза
сродниатласуукоторогонаплечахвращаетсяземнойшарсэмюэлсполдингэсквайрсказалоднаждыкопаяземлюпокопайсяусебявдушевер тителопастиэто
йкосилкибиллдаороситвасживительнаяструяфонтанаюностилекцияоконченакрометогоизредкаоченьпользительноотведатьзелениодуванчиков авы
давноелизеленьодуванчиковнаужинсэрнебудемуточнятьбиллкивнулилегонькостукнулближайшуюкорзинкуноскомбашмакатаквотнас четэтойтрав
ыяещеневсевамсказалонарастеттакгусточтонаверняказаглушитиклевериодуванчикигосподипомилуйзначитуженабудущийгодмыостанемсябезви на
изодуванчиковиниоднойпчелынадлужайкойдавыпростосумасошлипослушайтесольковызаплатилизаэтисеменадолларкорзинкаякупилдес ятьштук
вамвподарокдедушкаполезвкарманвытащилстаромодныйдлинныйкошелекотстегнулсеребрянуюзастежкуиизвлектрибумажкипопятьдолларовбилл
вытолькочтосовершилипревыгоднуюсделкузаработалипятьдолларовизвольтесейчасжеотправитьвсюэтучересчурпрозаическуютравуворагнапомо
йкусловомкудахотитетолькопокорнейшепрошунесейтееуменяводвореязнаюувассамыепохвальныенамеренияноявсетакиужедостигвесьмапочтенн
оговозрастаисмоимижеланияминегрехсчитатьсявпервуюочередь

Код програми

nbigram.cpp

```
#include <fstream>
 #include <iostream>
 #include <string>
 #include <math.h>
 using namespace std;
 int main()
 {
	setlocale(LC_ALL, "RUS");
	wifstream in("8.txt");
	wofstream out("output.txt");
	wifstream in2("2.txt");
	wstring t,r;
	int i = 0, e = 0;
	in>>t;
	while(1)
{
	in2>>r;
		for(int s=0;s<t.length(); s+=2)
		{
			if(r[0]==t[s] and r[1]==t[s+1])
			{
			e++;
		}
	}
```

```
		cout<<i<<endl;
		out<<r<<" "<<e<<endl;
		e=0;
		i++;
			if(in2.eof())
				break;
}
 }
```

key1.cpp

```
#include <fstream>
 #include <iostream>
 #include <string>
 #include <math.h>
 using namespace std;
 int ashki[31];
 int nsd(int X, int m) {
   while (X != m) {
      if (X > m) {
         int tmp = X;
         X = m;
         m = tmp;
      }
      m = m - X;
   }
   return X;
}
int ReverseElement(int X, int m, int Y) {
  int u, p,k=0,i=1, d;
  d = nsd(X, m);
  if (d != 1) {
		if(Y%d!=0){
			cout<<"doesn't exist"<<endl;
			return 0;
  }
else{
		cout<<"spec"<<endl;
		X = X/d;
		Y = Y/d;
		int m1 = m/d;

		int Xo = Y*ReverseElement(X,m1,Y);
		while(Xo<0)
		{
			Xo+=m1;
		}
		for(int l=0;l<d;l++){
			ashki[l] = (Xo + m1*l)%m;
		}
		return 9999;
}
  } else {
		while(m%X!=0){
			u = m%X;
			p = m/X;
```

```
                int perei = i;
                i = (-p)*i+k;
                k = perei;
                m = X;
                X = u;
  }
        cout<<"your obratnyi is "<< i<<endl;
    return i;
  }
}
 int numb (wstring bigrama)
 {
        int fartu=0;
        wstring alf;
        wifstream in2("2.txt");
        in2>>alf;
        for(int s=0;s<alf.length();s++)
        {
                if(bigrama[0]==alf[s])
        {
                fartu=s*31;
                in2.close();
                break;
        }
}
 for(int s=0;s<alf.length();s++)
        {
                if(bigrama[1]==alf[s])
        {
                fartu=fartu+s;
                in2.close();
                break;
        }
}
        return fartu;
  }
 int main()
 {
        setlocale(LC_ALL, "RUS");
        wifstream in("1.txt");
        wifstream in2("2.txt");
        wifstream in5("5.txt");
        wifstream in6("6.txt");
        wifstream in3("3.txt");
        wifstream in4("4.txt");
        wifstream in7("7.txt");
        wofstream out("output.txt");
        wstring t,r,l,f,c,q,w,k;
        int revo,a,b;
        int i = 0, e1 =0,e2=0,e3=0,e4=0,g,h,v,g1,h1,v1;
        int f1[5],c1[5],q1[5],w1[5];
        int x,X,xX,y,Y, yY ,N = 961, result, index,temp ;
        in>>t;
        while(1)
        {
```

```
                in6>>f;
                f1[i]=numb(f);
        i++;
        if(in6.eof())
                        break;
}
i=0;
while(1)
        {
                in4>>c;
                c1[i]=numb(c);
        i++;
        if(in4.eof())
                        break;
}
i=0;
        while(1)
        {
                in5>>q;
                q1[i]=numb(q);
        i++;
        if(in5.eof())
                        break;
}
i=0;
while(1)
        {
                in3>>w;
                w1[i]=numb(w);
        i++;
        if(in3.eof())
                        break;
}
i=0;
        in7>>k;
while(1)
        {
                while(1)
         {

                while(1)
                {
                        if(f1[e1]==c1[e2])
                        {
                                e3++;
                                break;
                        }
                        while(1)
                        {
                                if(q1[e3]==w1[e4])
                                {
                                        break;
                                }
                                y=q1[e3];
                                x=f1[e1];
```

```
Y=w1[e4];
X=c1[e2];
if(X>x)
{
		yY=Y-y;
xX=X-x;

}
else
{
		yY=y-Y;
xX=x-X;
}
revo = ReverseElement(xX, N, yY);
if(revo==0)
{
		break;
}
if(revo==9999)
{
		for(int ump=0;ump<31;ump++)
		{
			a=ashki[ump];
			temp=ReverseElement(a, N, yY);
			if((y-x*a)>0)
			b=(y-x*a)%N;
			else
			b=(y-x*a)%N+N;
			for(int bi=0;bi<(t.length()-1);bi+=2)
			{
				l=t[bi];
				l=l+t[bi+1];
				int ret=numb(l);
				int der=temp*(ret-b);
				if(der<0)
				{
					der=der+N*(-(der/N)+1);
					index=der%N;
					out<<k[index*2]<<k[index*2+1];
				}
				else
				{
					index=der%N;
					out<<k[index*2]<<k[index*2+1];
				}
			}
			cout<<i<<" a = "<<a<<" b = "<<b<<endl;
			i++;
			out<<endl;
		}
}
else
{
		a=(yY*revo)%N;
		if((y-x*a)>0)
```

```
                                        b=(y-x*a)%N;
                                else
                                        b=(y-x*a)%N+N;
                                for(int bi=0;bi<(t.length()-1);bi+=2)
                                        {
                                                l=t[bi];
                                                l=l+t[bi+1];
                                                int ret=numb(l);
                                                int der=revo*(ret-b);
                                                if(der<0)
                                                {
                                                        der=der+N*(-(der/N)+1);
                                                        index=der%N;
                                                }
                                                else
                                                        index=der%N;
                                                        out<<k[index*2]<<k[index*2+1];
                                        }
                                        cout<<i<<" a = "<<a<<" b = "<<b<<endl;
                                        i++;
                                        out<<endl;

                                }
                                if(e4==4)
                                {
                                        e4=0;
                                        break;
                                }
                                e4++;
                        }
                        if(e3==4)
                        {
                                e3=0;
                                break;
                        }
                        e3++;
                }
                if(e2==4)
                {
                        e2=0;
                        break;
                }
                e2++;

        }
        if(e1==4)
        {
                e1=0;
                break;
        }
        e1++;
}
}
```

filtr.cpp

```
#include <fstream>
 #include <iostream>
 #include <string>
 #include <math.h>
 using namespace std;
 int main()
 {
   setlocale(LC_ALL, "RUS");
   wifstream in("open_texts.txt");
   wofstream out("output.txt");
   wstring t,r;
   unsigned int texts = 0;
   unsigned int NtextMAX = 0;
   double maxIndex= 0;
   while(1)
    {
       int alfa[31];
       for(int letter=0;letter<32;letter++)
          {
           alfa[letter]=0;
          }
       in>>t;
       texts+=1;
       for(int i=0;i<t.length();i++)
         {
          int a =1072;
          while(a!=1104)
            {
             if((int)t[i]==a)
               {
                alfa[a-1072]+=1;
                break;
               }
             else
                a++;
            }
          }
//////////////////////////////Index/////////////////////////////////////////////////
       double sumlet=0.0;
       for(int letnum=224, letter=0;letnum<256;letnum++, letter++)
          {
           if(letnum==250)
                   continue;
                   sumlet+=alfa[letter];
       }
       cout<<"sumlet in text "<<texts<<" = "<<sumlet<<endl;
    cout<<"texts = "<<texts<<endl;
    double polindex=0.0;
                   double index = 0.0;
    for(int letter=0;letter<32;letter++)
          {
           polindex+=alfa[letter]*(alfa[letter]-1);
          }
       index = polindex/(sumlet*(sumlet-1));
       cout<<"Index = "<<index<<endl;
```

```
      if (index>maxIndex)
      {
       cout<<texts<<" "<<NtextMAX<<endl;
                  maxIndex = index;
                  NtextMAX = texts;
                  cout<<texts<<" "<<NtextMAX<<endl;
                 }
      cout<<"================================================"<<endl;
                 if(in.eof())
        break;
  }
  in.close();
  wifstream ink("open_texts.txt");
  texts = 0;
  while(1)
   {
              ink >> r;
              texts+=1;
              if (texts == NtextMAX)
                {
    out<<r;
    cout<<endl<<endl<<endl;
    cout<<"<==============================Text = "<<texts<<". Your open text in file
output.txt==============================>"<<endl;
   }
                 if(ink.eof())
       break;
   }
 }
```

Висновок: Під час данного комп’ютерного практикума ми набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанували прийомами роботи в модулярній арифметиці.