



Міністерство освіти і науки України
НТУУ «Київський політехнічний інститут»
Фізико-технічний інститут

«КРИПТОГРАФІЯ»

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконали:

Студенти III курсу ФТІ
групи ФБ-81
Легкий Дмитро
Чалий Олексій

Перевірив:

Чорний О.М

Хід роботи

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 елемента 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.

Варіант 10

Зашифрований текст:

юммутмкйсьйумтцбишчоцхйнкхйяхклзкургтвднълмгсбтмейашрэлшогэгклсмтцзлжфбтдлычт
фыляунгфищйэзргчсбыцжм
ьижнулхщълкюэклксыямямбйжцтпогсбэищмзмхшсчмддуилойэйугтюцдтрузвдуампзэйбуззюц
жнвкбхгвргфбчишчжпэгкнрш
зццлбгвптмвннгтшргэмбохгрирумчилцнвцвпжэбтцтвпезлкжэзйуццлкшцбоцюццнзмчяуфбця
тбжэеэсйлкдмеццатмбцца
ймумгхьцнгюцъдхшзеэпнсбжэящбгилнгтзяунивпезсмямешуйэйшйэсозгкшйяментэьхрхюзгк
хййзгкнйфцгзбйаьщрхрг
ычксдьяцзллтлгтмбхьэецшзюхщйххшзтбыцтмтэьхрхжэпмтэсмжбйаьщкирийзсмеивфзэсг
лйллжмцкэсткяжюццтдлкш
укикейяржэйингзлахрхмйщмйммнзиыцтмнипйхуфуббълвфоцлйямярсмюмгчжюфбфмтмжжжэ
екчэзмхйейаклккддуилридийщй
укнйриеэцукссмтцбгопямржшйцлритбмкэбыцогфгебэяждивфбшквдусгбгвццнтчойцкцбдях
тфължнммжэцксмхуоцяффу
ббкияйэншцфуклцмяжллфргяэувшчбубиьлцнммейцюклримвнйязвьльщцебрвщйзиычелцнф
ихйщцнзимйтэзцяфебнгтммйсг
гнзиьцтмугклемшйхбщюржгэыцлдргзлафжтзэфкцрагахрхтбилдтвпшчейоэбкагебэьщцнеэдэь
эюццпрхюцфшшйдшрцшмжэ
жэшущмямшиьлйзюцтмыщцюгэдшрцтвфцтргогкнзкдуешюказдмзипйбшрзэпямршгэвнтэик
црхктмеэыгычхфужмсчмйтцюх
днейщйжнсмвксйбхмйвпхкгнлкмвчбгфипйагригйсгнийзхкхпзлриэхюмишсэнгцлатшйэнзкбх
иянггэгзагмкгнцргпцнцр
гнвпыцогфгрхкскдктчкcgйуэцкгшбшрзэммпямпшбхзаопзлриэхгвумэмулыццюкклктмнгэфчэил
мйщмошяэнгфйзнюццкйэжм
ьиычвпйяэнлиюмсгзлоиястмгржэсчклнгвушешйщмнчыфэгдэомбжбипйзэщцргдмпбэьщфуцне
йошгпцнцрэхрхтэрэюксийбх

шзечявыщезэймлкугжтумзйжэдмчйоцоияптмумцуяйэнклркжтзэгкьэвнсбычниймззтмпчцнзиыч
щгюцшщчнекмнбткинийдйшх
цлкетжжкрмвчгнгктэгшщбэеыцявтнцрсбфмзингогжэагрдмсчжниййжибщчпшсгммзингогкйб
рщмумпмывтнцрргкйгкояьц
ьльццношэйицфбкляээнкпзузпмынцктцрхтпзлйдмйсбкляэцкцюриычилизяцлйвнхмдлринй
ргчящэмяхдэсчахыццлщм
змхшдншшфэяхрхсиуьнгкйейыилшсгцалксгкйэмлшсйщмдздэшйдэржчэнюриычилюцпйфйсы
ямгезлгнблднцрниямбйдшбйоу
зззйойибэеыщпшчяфбкдшршкйзеоушмпшсгзлгвтнбжэхтпзлыщпвдуикрцтвриднлкмгсбтмейх
йбшшхкшйждццлйздяцемэв
впэисгдмчэтыршцлатгшруоиилйзуарвумяццлйзюмнийоээсбтмщмсчдншшфэеньхпйфйрвюцел
рггшгэюцбирзьэбрдтимдшлл
жеьлшйугщюычтфпмомнийнииятмыцфязлрвыцмйжгхщилкезлгнлбклдущалксгжжеэцурашмецц
нршсэгущцдхщюгэюцдмзгрхсч
жнмвльйзхягэтыямщмшимхрхргычравфжэяэбпямейдйлярямдянийямжэязмбрюмжэсгизэйошю
цюцтпыцьлжнфиргмгрхойэгум
смхурхямцкашзрафпмэмяэяцниилчюжнейжвнйэзицюхлжцклкццмхжжамукэцьлдязагшюмхй
щмахтмбкгйтэйлапгнхкьцчякк
увхщцхешоэафкйтзюмбшексгцанийфцуатчбипвчкнйрцимфйнэлклийомечшзтццннишчжэдмсга
хжэяюжэдэсэпмвклжчэлипйгй
крекйкйгкрекэхчэгчбгщхжнилеэшиоцсмсгщйсмтэьэафюмеццяуавчыфнэлкцмзмышюхнийкйзэ
щйзхмйрмзмбжйкбххждццлнй
екквжннийзтычшмбшчэмппюхриошззыррвльвпхкеэгийшхжмсгбгхксчмезмщмеццютвзэмутмчэцк
эпнгкйыгщюмкплгмаюычзлий
тшгкдкюхтнвпхктчэгоцщюьэщцойдэшйщнбльльйзсчодьэецрапксграюямпнвптмхфзльццатчб
июубушечйдяпвщйннтэжлел
жндхрхюцжэьхвпнгцююцщюжмвлиагэнгзэвюычэпыцтмзлхщюцгвклтзнгтммучкафкйбцобмчф
ббгфбщцриачдуоизйщмйзнийтэ
жмфйкэнггэжвннипйсччяоисбтьфщзлращмчизлюхойэшпмснкяхкюриычилпйфйхйбшшхрх
рхцаагдуичрхжжбшрэбпямтмжж
нюдужэпкжэнгйздийиццюизымчщцфужтдлтвжнтэикрпмрмйцидеэзэцлогачжнзгэжжжэбкйл
жмжэвлдяйхкйлыццаээщюза
мклкзарижкелфебнглугимжэймдчзлфуззпйтмсмээмгжнебойэгумрбгнямрйвйишчсмаооцю
эчкечюхрипшсгвцтпыцяйэн
лизлюхшзашйцшзнкшоюцжзсмнзммпнщйдэьмдсифямйтчбичцоцеомозфцидшшщмжжквумсг
ычядмгргбуыцсгкйицрахйкрхюду
мхргычтраюмжэсгизэйошжцебьцьёнжтцажэязмэспзтцфужтатумээцргчжоауешнэшйсмоонгт
кыцгншчсэьгыцгвчкцмчецк
сифягнсмзийиццатчбиюубушееэмбщхдшбпямямдяомяртммпшюксокзмймокбчтфкйписгьлюмп
мзийяхадшоианкццлйзжлцнсм
жжщнклшйбцрасингтэхкгнцркмщйсгшчтмжжляилфщэмзммпнютфнгпкйхрхзэкфрхоцпкэнгу
злужтумцштчфбднейснюмгуыц
вгрхлийамумзйкрсмткйлшямчфбечюхдшгубушееэоибхычщшбйнкхйпицквшчшалнгьлсччюргри
нийицравэашшхцадэмгзэхещч
ахойахтмржзмзэбххжямхядяоэкрэхжнилхклритмюмцвнильвфбитчрхфмкыямухжнилхкжэб
шзйсгоцприогйзувахцашйяфеб
нгилхйбшшхбгкклдхтвжншшфэдгпвшчюшрцбуклщмжэгийгншшфэцрргвфчэьэбрвэашшхэю
мсгбиилоцнямшюычгшвешцапфж
влпвийеэхткйлкмщйсгшчюмпингпйщмецшцриаймыгтчиийьцьцфужтругсннкцршйюмтцехр
хтээмжэжэтжчэнгйзтмюцрхрх
жжзэсгнгбхклдхюцдямтэтэпнебэкжнтэтмикэнзкомярзйшйзэсгнгхйбшшхцнафббнийцксбтнтэик
еншцияьцрурикльццшшсэ

зеэгеэбхтфлюцжэсмшйщкукюмхбргчкээтилгоычгнейеюриычогагвфсбнйжэюмярвшбхтфльц
тцтшееэюцдяпвчккйжцрийй
пйгйжэюцднзмбйфждэпмэмеирэнийкрхкчхычфккхяддшрцризэжцидгйсгяджжхжцрпбхкафцнм
вбгфгруцнсбьцрхсмвщжюдоуоц
ришзтгчибишжрнгвнлнтэешскямхуебчяйецвумгэчэцрсиюссмнкяхфмжэейфйомярзйшйюмжэп
мткэняубушееэймыиьлйзймсг
цлэкбкцмеиансмпкпидудмстилгоычгнейумсгоцриилсмнкяхшкзбичбнммэнклвщцнцлатсмжвд
умезлзцсбэиргтэщгжнеэдэ
змьисйзэгшвкэцриййпйгйжэгэчуббосдэпйхиебшшоэухявахшзсижтдуюцебьцнввпсбкцгнсчжни
лилдязаеэямвннгрхтбиз
дэечапльхйбшшхшзбшрэпиатрунгбуриквлцобднейснюмгуыцпцапцюизшйпмдмнйэвахияогсб
шйагопшчямхштчбифмцксгиз
лкдмтлсбьльцдхмдсйбжщйсшщмярфжчхычфктмпнтмдмэмецобднсбьцебвубушееэюмппмдчогз
лвцтвргщхьлдудшафцкхцжнсм
ьтэерэеэюмэмсбаыямээрэгмржзцрийцжэлгзэчэбиушкйщйфжугрицншйжэбшклиеэлккмйцкк
икхйяхрхюмчцнейзиргжэсг
клдхрихчцнейгквнлйллогклдхимжэсчхяоингйзюфхйцсбултббгьцебдяьцтрувьфащмецпвчкх
йэньхиябшгцбузлчвдусг
чкнэцршшоэухэиямегмкфйгэсизетбюмсмнйцксббхтфльхйбшшхебшйсгюутмдэчэзтильэтьфяи
чжэлксгжжщмямжжкцапямяк
црвняпямгнцржэсинглдычмецюргклдхжткгзэгкцрюмгйкрзйччсбьцрвфбьцренгешгэдмшпцюр
июужтоияйейбрюцшйюмугог
злвцтвдшяхычфккхкццюацдмйвчяоинггнэмнгщюгэюмибнгяпямгйяхмйзэпмсгюхрубияшйэх
ешуцидзэтмэгумзвригншйсч
щюцлгкннвийесмтцнисчтбшчшшпеяпсбеэгкцрмдпйфрхййзлбилфиээмрчжнсмццфбиямэмтк
нйтфжэнгпввпсбьявргфбопям
внниахешчтьэшмьдайзипйзэсгнгхщкйейцхщюгэвуйецвйесмгйсгфищйэзщюззхйцрйздмечжюд
эгйгкцрээошщбьлксечцнрг
фзюмцкрэлнуаяэсиебамсйэнгмиибгогфипйэчтфшкагюцбишчтмгнейсгкйицуыямсицасгдмэмз
мпмсгыщцютфнгпкгшжэпмбб
нгфивунгркгийяхфаиктмнчфуоцнгклдхимнчфбфжшэстофкиебюмгэчэлщзлрбхзлнгцнгйтзпмд
мяртмдннйгэсарыйюпямгг
чяпвюцлгтмпйхпцнгйзмпкеэмшэнлиеббхопфжбктмэмбйзимвумсгойэйшйжцяйейтбыйфжшйб
блйейжэамукцрщцмдыхтнгэди
ебдмэсжржафгэлкдэсмтмашсгзэшйцкоипймбзлхкыузлвнлдгйзмсйсцргщюгэчэтцяпцюжтдлж
тюузлбгфидйшйхжкйгйцутт
клретбвузлебккскчезмбрржпмднсгявнийцкнвчкбшяжэцрпйфйдэтзгкяпямржшйймдгднбббгрхд
яшшпепвщшпклкбрржсмяп
сбжшээмжвчкумсжюмннтчнюбгфгзэхшоимвълкибгкнычтзхкямбйдужэафзэпмсгуаякжцднц
ахткйлкмщйсгшчьэбхрищшйж
дццлйзсгмчюхофжэзфжэлнеэдэубушееэбнтэтмжллкнлкшхфбомпглкжжеиякжцыцюхщюцюг
ншшфэентэхкошпмдмярсгиксб
ямхугвумпмцятбнйбщысгшсгнкщйцкшшпеемщдвууажмбшчэмпюхогчяйксийгтвклдгввпсбр
угвргфбопямюцмдргвцыцфукл
щмргжлэхосшпзлриэхкшдмпзейщмргэхйакщмумгэдэсгбиззхгюмюейцроивфччжьюсэншйф
йяцтфсбэсчштхщюгэбжкйбррш
гкцкцгрггтьцсбйеяйедргвцыцфуклщмжнтэйекншщяйукшйзнебтбймомакжэпкжэйеиубббгмму
кртяфюмсгычюцшйжвфбхьюх
щюгэсмсэйекнлиэбшээмнищйэзюмокзмйминзирибгвцюхямжтагфбшйпмнэсжчэнгйзцкцгрг
гтшщемциыщйфцюхямьщяфжэ
нгцксийщмбгантэтмикшрйздэсчбихтбокзмйкмкмиыгэхкжвьэямрнщйуквкюцриймечбгсмямхж
щнебпйфйжжзэькчэнгщкгшрш

ямцхямтэькфццнвкшйюмсиойюлдязачйгйбмзцбивфцнумецщэблцнжшсмямумщмжэаляпядчч
 жьяйэнэфсбтмаемчфйтсщлукл
 укдюхнщизаснеэдэзмециясжсмсээфсбэсюсмсэщнфшпйозаушенишчгкейзмсэсгсыамухжнил
 хкткйлвушмумнкзицнякикей
 яржэбнтчфзкмьгоцостмсгилэхцкгмсммпьцрхумгйямщмафщйзхшмсйкрюмярфкейартмргкйгэ
 црцйнийцкдуэиоцпксмчэжжгэ
 щцойлкцйнийкрдуэиоцпксмщцкшякрнлчшйашхйошямбцлгктиляхоидшлкнйцмкрсмсгмхдшет
 лкоэаекссмнфыцгштмбхфбвэнб
 рхбгрхдмфццнсийкыямдгзэжжйэйшйвнниеббхтфьюцмццнейзгрхлшсгвпямжэкийцьхтфкюш
 шекгкулнишчжмбшчэмпюхчюжн
 юмукюмбкшшхфжэпкршбйжэашбшькнюдуюжжнтэшйьнбтяфикжэафдуэиоцпксмикцкдутмжв
 сийжжэслдязасмчубимвумсгжнбб
 цнмелкюмллшезаейбхклдхриыфгвьэгклкдэагднсбьцфукльэлхычфккхшзгшвкгугнлгрершщиеб
 овдумчаххйбшшхгвкляфых
 мчрэьикгжьицлсгмчфбдудфжчулкицрасмзйнийсмэнейпццлпйщйвчщцксдэсгфягшккшинйщгчкаш
 рэтхрвтвлгиукльэумвтилпи
 кгклдхвпямиймкйчеилрвщйжжщцецксеузлгшдзэомотэлкюзцрпмйлмчриафдмярейпйхпцнбйргс
 чбиогфиясагопшчгнэшювум
 дэапгнгшхгзэхшдмччкюжэюмэмухтнзмдмфхруядргогнгклдхтвахычшйаепвумтшшйпйдгльцш
 гйтздмчиычезжцосэицнээяж
 пводчэярфжьцебшчьцжзтмлипйтэхкдябужнгквигншбгввпейиццюривфзэсгэкхбмкбкбйьэцкпб
 ыццющйюнпктэцрйзовшчхш
 нмсйщйзрмэ

Хід роботи

П'ять найчастіших біграм шифротексту

Біграма	Частота
сг	0.00814717
жэ	0.00788436
нг	0.00775295
ям	0.00735873
цр	0.00709592

Вивід програми(log.txt)

ст->сг , но->жэ key: (513,596)
 ст->жэ , но->сг key: (448,148)
 ст->сг , то->жэ key: (451,751)
 ст->жэ , то->сг key: (510,954)
 ст->сг , на->жэ key: (300,400)
 ст->жэ , на->сг key: (661,344)
 ст->сг , ен->жэ key: (243,713)
 ст->жэ , ен->сг key: (718,31)
 ст->жэ , но->ям key: (655,731)
 ст->ям , но->жэ key: (306,425)
 ст->жэ , то->ям key: (810,824)
 ст->ям , то->жэ key: (151,332)
 ст->жэ , на->ям key: (428,477)
 ст->ям , на->жэ key: (533,679)
 ст->жэ , ен->ям key: (462,206)

ст->ям , ен->жэ key: (499,950)
 ст->ям , но->нг key: (785,762)
 ст->нг , но->ям key: (176,586)
 ст->ям , то->нг key: (692,514)
 ст->нг , то->ям key: (269,834)
 ст->ям , на->нг key: (667,685)
 ст->нг , на->ям key: (294,663)
 ст->ям , ен->нг key: (473,705)
 ст->нг , ен->ям key: (488,643)
 ст->тм , но->нг key: (692,142)
 ст->нг , то->тм key: (362,121)
 ст->тм , то->нг key: (599,855)
 ст->нг , на->тм key: (635,291)
 ст->тм , на->нг key: (326,685)
 ст->нг , ен->тм key: (178,457)

ст->тм , ен->нг key: (783,519)
ст->тм , но->сг key: (661,700)
ст->тм , то->сг key: (568,452)
ст->сг , то->тм key: (393,648)
ст->тм , на->сг key: (853,809)
ст->сг , на->тм key: (108,291)
ст->тм , ен->сг key: (566,581)
ст->сг , ен->тм key: (395,519)
но->сг , на->жэ key: (709,865)
но->жэ , на->сг key: (252,840)
но->сг , ен->жэ key: (750,105)
но->жэ , ен->сг key: (211,639)
но->жэ , на->ям key: (909,756)
но->ям , на->жэ key: (52,400)
но->жэ , ен->ям key: (109,889)
но->ям , ен->жэ key: (852,267)
но->ям , на->нг key: (862,902)
но->нг , на->ям key: (99,446)
но->ям , ен->нг key: (226,878)
но->нг , ен->ям key: (735,470)
но->нг , на->тм key: (812,74)
но->тм , на->нг key: (149,902)
но->нг , ен->тм key: (146,67)
но->тм , ен->нг key: (815,909)
но->тм , на->сг key: (552,65)
но->сг , на->тм key: (409,74)
но->тм , ен->сг key: (691,723)
но->сг , ен->тм key: (270,377)
то->сг , на->жэ key: (616,865)
то->жэ , на->сг key: (345,840)
то->сг , но->жэ ЛП не розвязується
то->жэ , но->сг ЛП не розвязується
то->жэ , на->ям key: (661,756)
то->жэ , но->ям ЛП не розвязується
то->ям , но->жэ ЛП не розвязується
то->ям , на->нг key: (242,902)
то->нг , на->ям key: (719,446)
то->ям , но->нг ЛП не розвязується
то->нг , но->ям ЛП не розвязується
то->нг , на->тм key: (471,74)
то->тм , на->нг key: (490,902)
то->нг , но->тм ЛП не розвязується
то->тм , но->нг ЛП не розвязується
то->тм , на->сг key: (893,65)
то->сг , на->тм key: (68,74)
то->тм , но->сг ЛП не розвязується
то->сг , но->тм ЛП не розвязується
на->сг , ен->жэ key: (672,716)
на->жэ , ен->сг key: (289,28)
на->жэ , ен->ям key: (459,710)
на->ям , ен->жэ key: (502,446)
на->ям , ен->нг key: (264,260)

на->нг , ен->ям key: (697,127)
на->нг , ен->тм key: (77,127)
на->тм , ен->нг key: (884,849)
на->тм , ен->сг key: (450,849)
на->сг , ен->тм key: (511,251)
ен->сг , то->жэ key: (180,81)
ен->жэ , то->сг key: (781,663)
ен->жэ , то->ям key: (449,701)
ен->ям , то->жэ key: (512,455)
ен->ям , то->нг key: (208,594)
ен->нг , то->ям key: (753,754)
ен->нг , то->тм key: (381,785)
ен->тм , то->нг key: (580,191)
ен->тм , то->сг key: (704,501)
ен->сг , то->тм key: (257,599)
(513,596): entrophy: 4.776506102549494
FALSE
(448,148): entrophy: 4.812588642383965
FALSE
(451,751): entrophy: 4.806811544934764
FALSE
(510,954): entrophy: 4.829832317560015
FALSE
(300,400): entrophy: 4.453778442606628 OK
(661,344): entrophy: 4.745889348648549
FALSE
(243,713): entrophy: 4.773619413966931
FALSE
(718,31): entrophy: 4.825601702293138
FALSE
(655,731): entrophy: 4.810619175525809
FALSE
(306,425): entrophy: 4.811648609862594
FALSE
(810,824): entrophy: 4.799065962363571
FALSE
(151,332): entrophy: 4.797144000889637
FALSE
(428,477): entrophy: 4.826053007885836
FALSE
(533,679): entrophy: 4.823728934639757
FALSE
(462,206): entrophy: 4.799599710693173
FALSE
(499,950): entrophy: 4.788830375727821
FALSE
(785,762): entrophy: 4.818777443138326
FALSE
(176,586): entrophy: 4.810545062389985
FALSE
(692,514): entrophy: 4.810356399550786
FALSE

(269,834): entrophy: 4.80938093125307
FALSE
(667,685): entrophy: 4.8182839778778925
FALSE
(294,663): entrophy: 4.782867236444829
FALSE
(473,705): entrophy: 4.776243005348965
FALSE
(488,643): entrophy: 4.80839217587615
FALSE
(692,142): entrophy: 4.8138085346132335
FALSE
(362,121): entrophy: 4.828284355576494
FALSE
(599,855): entrophy: 4.792375778517261
FALSE
(635,291): entrophy: 4.807840652430018
FALSE
(326,685): entrophy: 4.8121987502520405
FALSE
(178,457): entrophy: 4.773369034313928
FALSE
(783,519): entrophy: 4.772446045447897
FALSE
(661,700): entrophy: 4.654420724705418
FALSE
(568,452): entrophy: 4.799240999821441
FALSE
(393,648): entrophy: 4.805075044588459
FALSE
(853,809): entrophy: 4.804547209320497
FALSE
(108,291): entrophy: 4.8015223042808275
FALSE
(566,581): entrophy: 4.794394250664731
FALSE
(395,519): entrophy: 4.801982900496792
FALSE
(709,865): entrophy: 4.820420014676816
FALSE
(252,840): entrophy: 4.808641592121414
FALSE
(750,105): entrophy: 4.76395992188967
FALSE
(211,639): entrophy: 4.845991675203188
FALSE
(909,756): entrophy: 4.823449375346538
FALSE
(52,400): entrophy: 4.780874423112842
FALSE
(109,889): entrophy: 4.764708724530793
FALSE

(852,267): entrophy: 4.799246034467532
FALSE
(862,902): entrophy: 4.827596145250082
FALSE
(99,446): entrophy: 4.825053374484248
FALSE
(226,878): entrophy: 4.803224354105291
FALSE
(735,470): entrophy: 4.797402065905258
FALSE
(812,74): entrophy: 4.836736441075865
FALSE
(149,902): entrophy: 4.833323177726318
FALSE
(146,67): entrophy: 4.728379312986515
FALSE
(815,909): entrophy: 4.771942249511494
FALSE
(552,65): entrophy: 4.8281023938636665
FALSE
(409,74): entrophy: 4.796024840591787
FALSE
(691,723): entrophy: 4.799762071164982
FALSE
(270,377): entrophy: 4.770216126461322
FALSE
(616,865): entrophy: 4.837899521064902
FALSE
(345,840): entrophy: 4.836814123709075
FALSE
(661,756): entrophy: 4.796715103453776
FALSE
(242,902): entrophy: 4.796518390011193
FALSE
(719,446): entrophy: 4.834110025616677
FALSE
(471,74): entrophy: 4.811576216757044
FALSE
(490,902): entrophy: 4.8309507526546716
FALSE
(893,65): entrophy: 4.812740682390155
FALSE
(68,74): entrophy: 4.816863762714933
FALSE
(672,716): entrophy: 4.793028350865116
FALSE
(289,28): entrophy: 4.778529371939756
FALSE
(459,710): entrophy: 4.788670704919342
FALSE
(502,446): entrophy: 4.832228637603338
FALSE

(264,260): entropy: 4.779314554607455
FALSE
(697,127): entropy: 4.800578741660462
FALSE
(77,127): entropy: 4.778936032919665
FALSE
(884,849): entropy: 4.800279633408805
FALSE
(450,849): entropy: 4.812504952759736
FALSE
(511,251): entropy: 4.768780207014592
FALSE
(180,81): entropy: 4.801894774529289
FALSE
(781,663): entropy: 4.75983548805054
FALSE

(449,701): entropy: 4.821827069312628
FALSE
(512,455): entropy: 4.802620621449912
FALSE
(208,594): entropy: 4.786055961137105
FALSE
(753,754): entropy: 4.771731977135991
FALSE
(381,785): entropy: 4.796847520493621
FALSE
(580,191): entropy: 4.812089396266736
FALSE
(704,501): entropy: 4.809039319754135
FALSE
(257,599): entropy: 4.787165159674546
FALSE

Ключ : (300,400)

Розшифрований текст:

поздновечером на веранде сидел коля и что то писал в темноте бумагу и тут толком нельзя было разглядеть время от времени он восклицал ага или это тоже значит ем у в голову приходило ещ что нибудь подходящее для его спуска потом дверь чуть стукнула точнов светку от москитов ударила с ночная бабочка лина шепнула уф манона сел рядом с ним на качели в одной ночной сорочке не тоненькая как семнадцать летняя девочка которую ещенелюбят и не толстая как пятидесятилетняя же нцина которую уж не любят но складная и крепкая и менно такая как на дотак вы же женщины во всяком возрасте если он и любимы она была удивительная ее тело какие го собственое всегда думалозане только подругоу она вынашивало дете и илив ходило вперед иле ов каждую комнату чтобы не уловимо изменить там самый воздух под стать настроению мужа казалось она и когдане задумывается на долго мыслит тотчас передавалась его голова плечам пальцами претворялась в действии так незаметно и естественно что леоне не смог бы да и не хотел изобразить это какими либо чертежами эта машина ска зала она на конец не нужна она нам да отозвал ся он но и тогда ну по заботиться и о других я втсе думаю что тут да встави ть кино картины радио приемники стереоскопические если собратъ все это вместе всякий человек пощупае тулыбн ет ся скажет да да это и есть счастье есочинить такую хитрую механику думать малончто попускайучеловека промокни или ин оетязвай или его мучает бессонница и он ворочается в постели всю ночь напролет идуше его грызут заботы авсерва нтовоя машина да ест ему счастье как тамагическая крупинка соли что брошена во веки вечны рождает соли и обратил авсерв в оляной растрвортк онерасшибся бывле пешку лишь бы изобреститакую машину пусть ему ответит на это то вопрос целый и и пусть ответит весь город пусть ответит жена лина смущенно молчала сидя рядом с ним на качелях и его молчание го ворилося не в сяких слов леото же умолкз апрокинул голову и слушал как свищев ветер вгустой листве могучего вяза не забы вайговори лонсе беиэ тот шелест листвевто же ну жендл я тво ей машины через минутув еранда опустела пустые качели не подвижно повислив в темноте дедушка улыбнулся авсе он почувствовал эту улыбку удивился ей и проснулся полежал не много прислушал ся к себе и понял откуда она взялась и бо он услышал не что то гораздо более важное не же ли пение иптицили шелест молодой листвывкаждый годнаступал день ког да он вот так просыпал ся и ждалэтого звука который означал что те п ерьтоужлетоначалось по настоящему она начиналось вот такое утро ког да кто нибудь из домочадцев или гостей племян ник сыни или внучкывыходил на улицу по де го окошкони металлическиеножи и спицы кружа и звеня под уш истой летней тра веприлежно обегали ес по краямна северна востокна югна западописывая все меньшие и меньшие квадраты косил каз во нкострелкотала из под ножей брызгали головки клевераредкие золотые искрыуцелевших после сбора одуванчиков мура выи палочки камешкиостатки прошлого днягопразднованиячетвертогоиюляобгорелые шутихи икусочитрутаноглав ноезанейстлался прохладный чистый поток сочной зеленой травы дедушкеуже представлялось как она щеко чете гоноги охлаждает разгоряченно елицонаполняет ноздри извечным ароматом вновь родившегося лета и обещает да мы в все пер оживемеще целый год великое чудо косилкаговорил себе дедушка какойэто дурак выдумал что новый годначинается пер вогаянваря надо было поставить дозорных караулить рост травы на миллион хуже акиллиной саогайой или а выи как з аметят что она созрела для сенокосавтосамое утро вмести фейерверковфанфарикриковпустыначинается великая бурна я симфония косилок срезающих свеж ие травы на необятных луговых просторах втот единственный день году который п онастоящем узнаменует собой начало людянадобы бросать друг в друга не конфетти и не серпантин апригоршн и све же скошенной травы дедушка мыкнулчтототужбольно дуло у философию развелстал подошел кув и высунул ся в лас ко вый солнечный свет так и есть форестерновый жилец молодой газетчик как раз заканчивае тряд доброе утро мистер спол динг такехорошенько бился жаром крикнул дедушка и вскоре уже сидел внизу иуплетал приготовленный бабушкой зав

тракшироекоеокинобылораскрытоиужужжәнекосилкисловноподпевалозавтракуотэтойкосилкинадушестановитяс покойнеезаметилдедушкатитолькопослушайтетеперьужнедолгонаееслушатьотозваласьбабушкаипоставиланасто лгоркупшеничныхлепешекбиллфорестерпосеетсегодняновыйсорттравыееенадобудеткоситьнепомнюкактамона называетсяноонакаквырастетскольконужнотаксамаиостановитсибольшенерастетдедушкасизумлениемуставилс янаженудовольноглупаяшуткаказалоннаконечидипосмотрисамбиллфорестерговоритэтоземленапользусказалаб абушкаонужепривезновыесеменаонисложенызадомомвмаленькихкорзинкахнужновразныхместахвырытьямкииз асыпатьгудасеменахконцугодановаятраваубьетвсюстаруюитогдаможешьпродаватьсвоюкосилкуонатебебольшене понадобитсядедушкасорвалсясостулаимигомвыскочилводворбиллфорестеростановилкосилкуижурысьотсолнца сулыбкойподошелкнемувоттактосказалонвчеракупилновыесеменадайдумаюзасеювамлужайкупоякаясвободенаме няпочемунеспросиллужайкатовсетакимозякричалдедушкаядумалвыбудетедовольнымистерсполдингничегояне доволенпокажитемнеэтучертовутравуонистояливозлемаленькихчетырехугольныхкорзиноксновооднымисемена мидедушкаподозрительнопыталоднуизнихноскомбашмакапомоемуэтосамаяобыкновеннаятраваавыуверенычт овасненадулиявкалифорнииивиделкаконарастетвотнастольковырастетивсееслитолькоонаприживетсяздесьнемкл иматенамуженабудущийгоднепридетсякаждуюнеделюподстригатьлужайкувтомтоибедасвашимпоколениемсказа лдедушкамнестыднозавасбиллаещежурналистыготовыуничтожитьвсечтоестьнасветехорошеготолькобытратить поменьшевременипоменьшетрудавотчеговыдобываетесьоннепочтительнопнулкорзинкуногойвотпоживетесмоето гдапойметечтомелкиерадостикудаважнеекрупныххраноутромповеснепрогулятьсяпешкомневпримерлучшеемкат итьвосемьдесятмилльсамомроскошномавтомобилеазнаетепочемупотомучтовсевокругблагоухаетвсерастетицвете ткогдаидешьпешкомествремяоглядетьсяявокругзаметитьсамуюмалуюкрасотуюпонимаюсейчасвамхочетсяхвати тьвсесразуизтонаверноеестественноэтосвойствомлодостоиногазетчикунадоуметьвидетьимелкийвинограданетоль коогромныеарбузывамподавайцелыйскелетасменядовольноиследапальцевчтожжепонятносейчасмелочикажутс явамскучныминоможетвыпростоеещенезнаетеимценыеумеетенаходитьвнихвкусдаивамволювыбыиздализаконоб устранииивсехмелкихделвсехмелочейнотогдавамнечегобылобыделатьвперерывемеждубольшимиделамииприш лосьбыдоисступленияпридумыватьсебеззанимаетчтобынесойтисуматакужлучшепоучилисьбыкоемууусамойприро дыподстригатьтравуивыпалыватьсорнякитожеднаизрадостейжизнисынокбиллфорестерласковоулыбнулсястари кузнаюзнаюсказалдедушкаястановлюсьслишкомболтливывжизниникогонеслушалстакимудовольствиемтогдап родолжимлекциюкустсиренилучшеорхидеииодуванчикитожеичертотолохапочемудапотомучтоониохотьненадолг оотвлекаютчеловекауводятегоотлюдейигородазаставляютпопотетьивозвращаютснебсназемлюнужкогдаывесьт утиниктотебенемешаетхотьненадолгоостаешьсянаединессамимсобойиначинаешьдуматьодинбезпостороннейпо мощикогдакопаешьсяясадусамоевремяпофилософствоватьниктообэтомнедогадываетсяниктотебянеобвиняетник тоинезнаетничегоатыстановишьсязаправскимфилософомэдакийплатонсредипионовсократкоторыйсамсебевыра щиваетцикутутотктотацитнаспинепо своейлужайкемешокнавозасродниатласуукоторогонаплечахвращаетсяземн ойшарсэмюэлсполдингэсквайрсказалоднаждыкопаяземлюпокопайсяусебявдушевертителопастизтойкосилкибил лидаороситвасживительнаяструяфонтанаюностилекцияоконченакрометогоизредкаоченьпользительноотведатьзе лениодуванчиковавыдавноелизеленьодуванчиковнаужинсэрнебудем уточнятьбиллквиулилегонькостукнулблиз айшуюкорзинкуноскомбашмакатаквотнасчетэтойтравыещеневсевамсказалонарастеттакгустотонаверняказаглу шитиклевериодуванчикигосподипомилуйзначитуженабудущийгодмыостанемсябезвинаизодуванчиковиниодной пчелынадлужайкойдавыпростосумасошлипослушайтескольковызаплатилизаэтисеменадолларкорзинкакупилде сятыштуквамвподарокдедушкаполезвкарманвытащилстаромодныйдлинныйкошелекотстегнулсеребрянуюзастеж куиизвлектрибумажиопятьдолларовбиллвытолькочтосовершилипревыгоднуюделкузаработалипятьдолларови звольтесейчасжеотправитьвсюэтучересчурпрозаическуютравувоврагнапомойкусловомкудахотитетолькопокорне йшепрошунесейтеееуменяводворезнаюувассамыепохвалыныенамеренияновсетакиужедостигвесьмапочтенног овозрастаисмоимжеланияминегрехсчитатьсьявпервуюочередьаа

Висновок

В результаті виконанні лабораторної роботи, було набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці. знайдені п'ять найчастіших біграм шифртексту. Було розшифровано шифртекст.