

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

ФБ-12 Приходько Юрій

Мета роботи:

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

Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. 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.
3. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
4. 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).
5. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
6. Повторювати дії 4-5 доти, доки дешифрований текст не буде змістовним.

Хід роботи:

Напишемо програму мовою python що задовольнить поставлену задачу.

Програма має

- Прочитати з файлу шифротекст
- Порахувати частоти біграм в шифротексті, обрати N-у кількість найімовірніших.

- Для 5-ти найімовірніших біграм відкритого тексту та N-тих біграм шифротексту спробувати розв'язати систему з двох рівнянь, знайти можливі ключі
- Для кожного потенційного ключа розшифрувати шифротекст, перевірити вихідний відкритий текст на адекватність за допомогою критерію Заборонених L-грам.
- Вивести на екран відкриті тексти що пройшли перевірку

Результат виконання програми - взлом шифру для наданого за варіантом шифротексту.

[illegible]

5 найчастіших біграм шифротексту:

'яф', 'аф', 'дю', 'хб', 'нф'

Насправді ми не можемо обмежитись верхніми п'ятьма біграмами тому що деякі з них мають однакову частоту, приклад:

td	0.006560182544209925727118903893142487504519522190093994140625
ml	0.0068454078712219953466065131533611713747564792633095664625
en	0.0068454078712219953466065131533611713747564792633095664625
lo	0.0068454078712219953466065131533611713747564792633095664625
yn	0.00713063320022818032672962185677387984695329661376953125
pr	0.00713063320022818032672962185677387984695329661376953125
ba	0.00741585852823730719285411083774306462146341800689697265625
yt	0.00741585852823730719285411083774306462146341800689697265625
aj	0.00741585852823730719285411083774306462146341800689697265625
sz	0.00741585852823730719285411083774306462146341800689697265625
wy	0.00741585852823730719285411083774306462146341800689697265625
nb	0.0077018038562464349263430847821228846419543741335449291875
td	0.007986390184255562659826561186815123073756694793701171875
cn	0.007986390184255562659826561186815123073756694793701171875
xb	0.007986390184255562659826561186815123073756694793701171875
td	0.008556759840273816392075545422812865581363439559365234375
en	0.008556759840273816392075545422812865581363439559365234375
lo	0.008556759840273816392075545422812865581363439559365234375
g	0.008556759840273816392075545422812865581363439559365234375
h	0.008556759840273816392075545422812865581363439559365234375
fa	0.008841958168292432582000350748785422183537246002197265625
en	0.009127210469292070124325427426944218855312096405029296875
ay	0.009127210469292070124325427426944218855312096405029296875
zh	0.00941243582430119872517249035581689990426957607269281709375
h	0.00941243582430119872517249035581689990426957607269281709375
xb	0.00941243582430119872517249035581689990426957607269281709375
vz	0.00969796115231032559129698007882665412634611297607421875
rk	0.009928864003194524571246959983131782534161539297734375
k	0.010268111808328579323544959312014901825221319354240046875
h	0.010553371363377618967804896704979664522451623382568359375
pn	0.010553371363377618967804896704979664522451623382568359375
lo	0.010838562434683479051841459295426750116348266015625
lo	0.011093112306588522767393870838207515152524768283125
h	0.01169423844837421538889188354914949712145137886865234375
lo	0.01169423844837421538889188354914949712145137886865234375
h	0.01169423844837421538889188354914949712145137886865234375
dx	0.01226469104392740855864383800879450980573892593387890625
ad	0.0151169423844837429865561873043589002918452074495838671875
lo	0.0151169423844837429865561873043589002918452074495838671875

Як видно з скріншоту результату частотного аналізу найімовірніші біграми треба брати за 5 частотами, адже частота для деяких повторюється (вони однаково ймовірні). Для повного:

1. 'яф', 'аф'
2. 'дю'
3. 'хб', 'нф', 'ап'
4. 'ло'
5. 'яю'

Таким чином в ідеалі ми повинні дивитись не на 5, а на 8 біграм. В моєму варіанті при повному переборі мені вдалось автоматично розшифрувати текст на наборі з 7ми найімовірніших біграм - 'яф', 'аф', 'дю', 'хб', 'нф', 'ап', 'ло'.

Розпізнавання мови виконано за допомогою перевірки наявності біграм які не можуть зустрітись в мові.

Знайдене значення ключа: 99, 60

Шифротекст мого варіанту:

Дюэорэджэорэтнтфээлкшэунскынайцбюовыоежэмюшыафткаэапжнечсюкэфэгябаейпблрщкбс
яфийпкдчаясюлохэитрэшуафюэмпсфэпбщзскынафвфюэбэеыпыфьркэяфщюхэнфкймюмфыф
тфрюсюээфээбжооафэьякюфьчтвлэйзцндюткяхмфяюкпнюзунонмынюбжалюхэзщпызхбврэвь
доанфхэкюжчеыжфдюжгзкжхяюзимощюяпэомоииаьэвынрихбйюзшюхыэфпкйэвунххяюннубяк
ецякзгевкерйыфафйртфмыпйрчяюыннцнюифмфяфйожхыфжюкесзпукыонмфвэкуафвфакжнйьр
юэоаизююивыйжщцюесюхфяюяндюткдчлзозэффпрбнфьфуфкебывыапщфкзациоечяфьойьнбрз
апубюаеюеориээхэлеуисфцовыюежэпвякафмювэьэафйбаилещыгмхблыххвпьеодкрефкзнфьязп
вьрхбддзчафкьяулпвэубунжотнххзешфнфабнцацхбзктэипукьэсфнфхддцяфеющюафэьзавэчкьэ
убгоуыбсцпхрэвьдрикийлроцдмлегйтэааихэыошайбпйьиэвмпфндюткяхуклооньцэврфяюбихэо
оарчмюжпывыжбфгнжотндчьэтфкьхбпюсыххгяюыфжюяфвфйьцнэпйьцнзвкрнфяюкюыннчгунф
цншыяьэвкэзяфжюкезфжнмоякчвнювфгьрзэфпжкцбрюеющкбзвыовнчыфнфцыфлупмюипкэ
ьяпжешожхейлюызхбххоэрмэнщпшушвщзпюйвоиаижиинжвомвтщпацзкюфтыщкьэвфжкцбрю
еюююзюфэдзяюлпапаяцхбзктэяьыдтфкюапйндюмулывыжвщпгоонвыбфжнжвлззвфгэньзуфшо
ыдевшэфиьпдьыдфгжвуыжбйинюгфмпдюзевлзуюпйевлоригвдтзкриепкэзягиюоуяфхошавэыь
тфепроуывыххгвэнрилзбэаняпзцлоыфжюкекьэвмгчвоэрмэнюусюмэьяяюзгпмфюэбндюткяхщю
ьяжэмфбэмпжнриывыжиййбаинфукыыдчукгонфилсзяюмюсмцбапюущюкнаишэкэьрзхэорхф
эсзунюэлпбняпзцлошвицвкоэфэеодкрйшгзешфнфсюбклргоаиубякецедезвстындюткдчвэжукэ
ийикжбтьххкэрюйныдпзийлойфвьдютвьсыотьлоепыкуняющпмфяфкумфяюрюфншзнотьрзхиф
жкьэпдшзгвнафрзяфтфсожфзбпкнфэьякхбрунинцрукбчыьчсытндюткяхмюлыапоэафбтнрзюэп
оывйьлзпкдччэлыгоммрумйевлоцсоэхвппкющфгбиижоикьэпдеваискынчийихбуфяфьянфжбцак
эмпкэлпгвнвщккрцуфпипбэьяфбиртюобыдцэнецжвбыйьгошзнфюмсэщфоббылотьрзхифрьхб
шзубрзчвдццкхэоажхшувщзщюяюугынвыцдчийфвфжзсьуфсфээхэафбиртюомдэвстлоынрэмю
оэйвщкюдюцэюоуывырэунпущювэзеукэввтэпщфюоякшэбээолзлеыншцаплгшзрюафрчйзуюкь
эдзрюеожпцдкртнжиинцхэээрэынцхэээрэяюуггчбээоцяжшувэыоынвэщфтуяфмпьддуюжб
йинюемяфмпвфыфяпикяфжузляфвэжбйинюзфмпфужпыоынвыфэьяшфмувэвфвэвьфыфифшоя

нгонплыоевэдюрддюденюынибевъщъшзнфцосързщъсэюцыпркынвокргоынвххкйфтымоын
дъецафзыефэошзэулысэрююэпяюэпойъецккэнчвпюйвлзжбзаесмвнзщфжбынгыврщюжбйинюсз
эулысэвъецафзыиыбзщфуюмигоуыэнунтпгорзяюмютцбреюжнтнгодьяпжажвюовыгоммругжн
моякюуяътфээдзхбддзчлехбевъзайедтфжээошэыфъэцооцйюяхэыошйоцчэжюапабнцшаэвщфъ
цжвстзккенчпюкэрчжяшфюцшзцнаивфшужбйинюиичйфпапсюмювфтфеошэубврывшцшмшзыэг
ыцбръяпккэнщквртфцошэнфыйюобзубяккйгэсзбэфънбфэъядерющпрзрюапаяшгикынъзфэфпсфн
иякпумнаигпмфыфдюкпнюиисюмютзяюмюсмцбаппумнунгпзтцднчылзбэаняпзцломэжырумкй
ыеспюбэхэлнюняпдоврврлохбэннбтыиэгюапжбйинюжцхбруюзунфьячовмффэьякюжпрзрюи
пяпйоцэрнбецлыгэшдыдуюошъшыэнчвнчшокйъцэвюоефнниякнвынжвсюшурпжншэмюапкешзэ
въжиидужющыонгоубавмфхнлолзкенцхбзкечбцсъзауфйбцдйионийлзгинфхэжхбшзбыжвибгм
юхщпшфрощэубрзрюэкпнюуфлыыфвяапжнмукэфэгязкяфьорзжкпйщйевлоиэжнбыуфнювфнншаг
огыыднбщфпюлнунйътфъэкчлыэвщйчвмфдууюкуъэжолешцуыьидъецшфрозайиыиьиецикафмю
эбзтлолеызрюжрхпзщмолеызуфшошыгонэмнлзрююежпжбйинюдорицдчвынйинпжзхэсйжв
шзлеббгмтэкужнфэрравнчтвынмпевшзэндюткяхгощюцэююооынмфрзыдлоафкувфыфяптцбрею
ыэщцчввккпяювфсюикяфжукюубэдывыххяфоуеоххмююяндюткяхаэфэцммбыэявлоафсфпйз
яюмюнилзбэаняпзцлоыфяфмпауцнэужнонуйврнбеццюйныдпзгпфэкчккцывтнмгшзрюручкп
йонйикияфжукюяндюткяхейипцрруапрзрюафипюзцняпзцлоифжнжвскхбвунфыйюопзубяккйгэо
бддцникрзяфшглоафмюыфшпапщкыэжншзмпыуушчвуынбзпрусюжбиктндцлркэгуаэакующю
мкщфсмжвщкиэпйхбпйкэаявэнфбцтьрзрюипапззжбоцдцичнбпэжндюафбэоэщягощзякыэббщзд
еююыннчяьдюзсмфпекэапсюжбикяугвынжвлзмокбямлзюээмюоххскфгцсдвдмпюухчеыгэмвш
зучцпындмафыфлыякшэтьевъзюогпжбацкэзбщзлышйпкжвяюзиафвфхэыошйоцпувьякммхбйис
юдюлуфбртлоафхлжндюкээрдюуфешзжбкужеяюннпъфжзжаепбнгувпапхинцлеынгубеяфюзб
эзящпжцибзгхбыдапнюузуунаипзхбеонбшйлююпнюцьжвдмнфакзешфнфндююэвфчапаяпб
брмюпббраифэкчлпцынпыэьяяюапскыиничрытмфифыюкеуирзсыйимфжнчыщкдчяюмвчийицд
дцяфэрдюжовыепүфлфвэдюрахгщкжвацйипкявюолефьеюжябаскбзшыьилзяфзмьшкнбунмпя
южпыилгкплейнвышабэхооасюфбзалюхэзооаыфтфюямяюпмяфяфвфэричфпмюифоотннчыфяф
мпрзрюсыпллпирзсыякяфьянфмюифпргэвфуеифлылзяочвнпубзкдюлпапаяоывыиэяфкэфэрчэо
иэыэепыфпйхбэвфгжваизвпюапыфкрэвъдиэцдчйочбэсоиэюезюыэявлоафгвшзяюеюаясдхэжнн
шшаяюеехюгюнювфафыфжюкеакъэвфыфяпапвфыфяпапкэучмышйжврзомяфгодьхблошзапаяо
ывыиэяфюоиэгбиихпжпжнхбжбацкэкзрюмкпббрсюфпыфщфуфифшюшвшйаувэвфвфзчыывивфд
убеэлхэняпаэлыгэеюэьдмщпкэзяубйьяенююзгоафчэжнфэыфсогоуыяфмпюущювэыьптчвшфжз
жажннбгошаыджиньжвхэепщюцэшфрощэпвякафрзрюафипуфаясюецафуишзбэлрэврзжбацкэс
юмфеоыижвнчдьоцжвлзжббыпйбзафнюапфкпйшууэяпйутйэвуншэвипфееуыфюекмевшйедд
юеюаяцжюэяфщпеуыгонейгонжбйинюсзяфавщфсмжвщкжхяфьопйвыэвифньюэжхнбуюгыдхэ
лыщкдчжзэввэюоадупюшбддцнсэапыевшэипботюсюгуяювмппккыэтшнцхбжююзгинцлеритьз
ажбйинюхпнфбцэнсьеакынхбшыжэюэапромошаецфгшуунвэынмгофжнтфююивундюткэсэтквэч
элыяпнфэътфхбэеюфпяущусывыяфяфейпбврруроиьнбоцаиххунгещюлюбэяпаэвфифэбврйьец
яибсэмяфвкщзчыдюмкбэцоаижбйинюдднвуншатпубюаеюеорзякыэмывынющнбыкркэяфорцсш
инбмглориублзжпфээтгэфэкрюмфюэпоывкйртмбхюэтгэвдтзкшэепкэзяхппзевлзъшпафщылпс
фкупйхбчымыюэбзтлоафхлжндюкэацкшэнрищфжняюмыунбшэежнчыщкбсвьецафуюжпуюгоу
вцхбзкжоружшзлоуюшзапацлпмфмпткифьячэфэуюиплешзжбмохцзпзамфюдртлюнфзняпзцло
шйрчкоывукгошыондюткяхмфчмжвнчсюмюжмхбчйдумзюкицрпжпркынйибфсыдцауцэжтуфшф
рощээфэсвшзэрнбецонтнщпхьямщзэюьялпкэфэыфпвякафжнлзруапкррзякыэзияфтфннпзцло
мюяфмипйчвщкщъплптцынхсюбэмпжнцсывыжгмцбапацбреюыьрэхэеоыибфжнмоякчвлзбуу
нфбднххбкхбдъхбнцбэмывыжньюннощздвоцружъецафзыефмпжюеоякуочпнюапащцзжпыф
щцзаубгокймолехлхэняпаэжныфжпвэскецчвэреюезоэрмэншыжбацкэсюсюыэеоххгунфцнпэшу
швщзмфшвоцчвээхэлеэдцбгюыожхщфызацлоечтшхбшйврчккэюзхбддтфыэпябэцошыдуюхххя
южквтфчмфяфуфлмяфуцрзипщюзягилзбэаняпзцложжкрякйиифэбврнбддцнсэмэюакыинчжпжн

хбжбацкэвэмэюацынчдющжвнчвэйбаищпакщцюакнпйвыюееюаябкхбуьецыддюьцапэожгу
үмэнжхтййылыеюеохмфеомгщпжбйинюбинцхээойььяемкмфвсьэвдцлолерйафычрмшзэвьж
икшзрфдюжгзкхжяюзимощюяпкзюеыбсцпрйэвунаигунфцншыжщпоедшызаскхбруэйоцжвн
орхбрэвлзфбнвнчубьжвкйшвшйдюукпйонстнфьямпнффкикяфжукюфьфэвбоневнощцбюкоывп
юйввтлрдчнфхфкпвэжбунцюдюпупункцыэввоуыывэвдцщзйзйфмфщцэнуьяпкэйэныдххубгишы
чкиэкуфбнвлжюкбпчоюоуыдцэнсьхбноофмфщцсэляфегтнпцбркеяфьянфмфшулюдоецбреюгз
яфавсюдужющыьпузафипкэсмяфжукэйийкжбцбеддмгэмюьярнфэьядевфзчкпкцбаидьунаимпъ
нецхглонцвроцсэйзмьяфнфбцэнпйкэаяжэбндюткяхфвэмнсьхбэпиискпкныфэкчрюэзмэцовраи
афвфхэыочйеддняляфсхбддзчафжцнбмгщплывгыгокйжвщкяхфэьяденютфцоощзрювэмнвыиэт
нтфрзловсапзпщфупапюэхоххубрзвэлянчгэпвюосьецхлпнфкоцюрзрюжанчйнсьуфчурнафкьрзб
эапвэубиилоафпзяерпляяюркэяфщюхэнфоужяпвтафчэбплпуклоонжбйинюупипцрцдяужблов
эчуапгесюрптфнфэътфйкэыэуцмбьяклежпзщцюжпгвэнмоякрчьфипдвлоякйнвтюосьхбнцбэмыв
ысюьоыннчеозксюпкйзпяерплямяюифщфгйсюнфеечймущппвякафмюлпяюрнпюдепвякафмф
яюлпйзузйбюаунаикэнчяфугевчйлезддмгонфжзуфшопйэнфэцпсыюеьягиюошйцбддэвстйшдчуб
ддэвстйшдчжнфэнфмюпвякафяюгубьяпвякафлюхэзяючлхэняпаэлыдчжужзпвякафвфдузюгиз
вмпгиевгывэвлплзаэочоынмюуклоонукгонфзндюткяхкйртдьоняфьорзщгогзецякххйьпзяюхпшоя
куьецмплюмьецафзыспшоякгынмвэйзузгонювфгьйьяеюэйзыфьизубэткьэщцюьяжэацжвстсьрзы
фымфрюлолешщикафранбгололеббевзйиавыххяфскиэкьунсээоххщюшорзсфтвээоххщэапм
фпвяубпсюмфвффчиичизубрзчвпюйвхххожфчкынчвшушвщзуафмфвффчиибю

Розшифрований текст мого варианту:

Раннеераннееутропервыеотсветызаринакрышезаокномвселистьянадеревьяхвзрагиваютотзы
ваясьнамалейшеедуновениеипредрассветноговетеркаиотгдетодалекоиззаповоротанасеребря
ныхрельсахпоявляетсятрамвайпокачиваясьначетырехмаленькихсероголубыхколесахяркооран
жевыйкакмандариннанемэполетымерцающеймедиизолотойкантпроводовижелтыйзвонокгро
мкозвякаетедвадопотопныйвожатыйстукнетпонемуногойвстоптанномбашмакецифрынабокахт
рамваяиспередияркозолотыекакклимонсиденьяточнопорослипрохладнымзеленыммхомнакры
шесловнозанесеногромныйкучерскойбичнабегуонскользитпосеребрянойпаутинепротянутойв
ысокосредидеревьевивзвсехоконбудтоладаномпахнетвсепроникающимголубымизагадочнымз
апахомлетнихгрозимолнийтрамвайзвенитвдольокаймленныххвзамиулицииобтянутаясеройперч
аткойрукавожатогоопятыопятылегкокасаетсярукоятквполденьвожатыйостановилвагонпосре
дикварталаивысунулсявокошкоэийзавидевпризывныйвзмахсеройперчаткидугласчарлитомвсе
мальчишкиидевчонкивсевокварталакубаремскатилисьсдеревьевпобросаливтравускалкиони
такиосталисьлежатьсловнобелыезмеиипобежаликтрамваюонирасселисьпозеленымплюшевы
мсиденьяминиктоснихнеспросилникакойплатымистертридденвожатыйположилперчаткунаще
лькассыиповелтрамвайдальшепотенистымлицамгромкозвякаязвонкомэйсказалчарликудаэто
мыедемпоследнийрейсответилтридденглядявпереднабегущиевысоконадвагономпроводабол
ьшетрамваянебудетзавтрапойдетавтобусаменяотправляютнапенсиювоткакпотомупокатайтес
ьнапоследоквсембесплатноосторожноонрывкомповернулмеднуюрукояткутрамвайзаскрипели
крутосвернулописываябесконечнуюзеленуюпетлюисамовремянавсембеломсветезамерлотоль
котридденидетиплыливегоудивительноймашинекудаতোдалекопонаскончаемойрекенапоследо
кпереспросилудивленныйдугласдакакжетакибезтоговсеплохозеленоймашиныбольшенетеезап
ерливгаражеиникакоеоттудапозволишьмоиновыетеннисныеутфлиужестановятсясовсемста
рымиибегутвсемедленнееимедленнеекакжетапеперьбудетнетнемогутониубратьтрамвайчтон
иговориавтобусэтонетрамвайонишумитнетакрельсовунегонетпроводовнетониискрынеразбрас
ываетирельсыпескомнепосыпаетдаицветунегонетакойизвонканетиподножкуютоннепускаетавед

ьверно подхватил чарли страхлюблю смотреть когда трамвай спускает подножку прямо гармоникат
отои оно сказал дугластун и приехали на конечную остановку в прочем серебряные рельсы заброш
енные восемнадцать лет назад бежали среди холмов дальше тысяча девятьсот девяносто трамва
е мездили на городные прогулки в час пик парк прихватил огромные корзины с провизией и тех пор
рельсы так и остались ржаветь среди холмов тут то мы и поворачиваем назад сказал чарли тут то ты и
ишь а мистер тридден щелкнул выключатель а аварийного генератора поехали трамвай дернул сяско
льзнул по рельсам и оставив позади городские окраины покатился вниз в долину он товылетал надущ
истые залитые солнцем лужайки тоны рял под тенистые деревья где пахло грибами там мисьям колю пе
ресекали ручейки солнцем просвечивало сквозь листву деревьев в точности сквозь зеленое стекло вагонти
хонько бормоча что то просебя скользил по лугам усеянным дикими подсолнухами мисьям колю пе
ошенных станций усыпанных словно конфетти старыми трамвайными билетами и в след за лесным
учем устремлялся в летние леса трамвай он даже пахнет по особенному говорил дуглас езди я в чика
гона автобусах у тех какой то чудной запах трамвай чересчур медленно ходит сказал мистер тридден
и то ни их хотят пустить по городу автобусы и ребята в школу то же станут возить в автобусах трамвай в
звизгнул и остановился тридден достал сверху корзину с провизией ребята восторженно завопили и в
месте с ним потащили корзину на траву туда где ручей впадал в молчаливое озеро здесь некогда поставили
эстраду для оркестрант теперь она совсем рассыпается в прах они сидели на траве уплетали сэндвичи
с ветчиной свежую клубнику и яркие блестящие точные носовые и апельсины и тридден рассказывал
ка много лет назад тут по вечерам на разукрашенной эстраде играл оркестр музыканты из всех сил тру
били в медные трубы толстый дирижер обливаясь потом усердно размахивал палочкой ввысоко
и траве гонялись друг за другом ребяташки и мелькали светлячки а подощатым мосткам постукивая
аблуками будто играя на аксилофоне расхаживали дамы в длинных платьях с высокими стоячими
воротниками и мужчины в таких тесных накрахмаленных воротничках что того и гляди задохнутся а то и
статки этих мостков только за долгие годы доски сгнили и превратились в какое то деревянное
мисьям колю пе озеро лежало молчаливое голубое и безмятежное рыба медленно плескалась в
блестящих камышах а вагоновожатый все говорил и говорил детям казалось что они перенеслись в
какое то иное время и мистер тридден стал вдруг надиво молодой а глаза у него рт как голубые
электрические лампочки день проплавал сонно без тревожники то никуда не спешил со
всех сторон их обступал лес и даже сол
нцесловно остановилось на одном месте а голостриддена поднимался и падал истрекозы
сновали в воздухе и суз золотые невидимые узоры пчела забралась в цветы и жужжит
жужжит трамвай стоял молчаливый точно заколдованный орган поблескивая в
солнечных лучах ребята ели апельсины и ананасы а у них все еще держался
медный запах трамвая и когда теплый ветерок шевелил на них одежду
то не то же остро пахло трамваем в небесном пролетела дикая утка то вздрогнул
порадой отцы да матери чего доброго подумают что вас укурал в темном трамвае
было тихо и прохладно все как в аптеке где торгуют мороженым присмирели
ребята повернули за шуршавшие плюшевые сиденья и уселись спиной к
ихому озеру за брошенной эстрадой дощатым мосткам которые выстуки
вают под ногами звонкую деревянную песенку если идти по ним вдоль берега
и нынче страны дзень по дбашмаком тридден завякнул звонок трамвай по
мчался назад через луг с вядшими цветами откуда уже ушло солнышко
через лес и город тут кирпичас фальти деревословности ну и его со
всех сторон тридден затормозил и выпустил детей на тенистую улицу чарли и дуглас
последними остановились у открытой двери перед тем как ступить на
складную подножку они жадно тягивали и озямив воздух про
низанный электричеством и несводили глаз сперчаток триддена на медную
рукоятку дугласа погладил зеленый бархатный мех сиденья еще раз оглядел
серебро медь темно красный каквишня потолок что ж до свиданья
мистер тридден все го вам доброго ребята еще увидимся мистер тридден
еще увидимся раздался громкий вздох это закрылась дверь подобра
в длинный рубчатый язык складной подножки трамвай медленно поплыл
в полуденный зной ярче солнца весь оранжевый как мандарин сверкающий
золотом рукоятки циферблатов свернула дальний угол и скрылась пропа
лиз глаз развозить школьников в автобусах презрительнофыркнул чарли шагая
как бо чинет рот у арату жу в школу

и как не удастся опоздать придет зато бой прямо к твоему крыльцу в жизни никуда теперь не опоздаешь вот жуть дуг ты только подумай но дуг ласстостаяла ужайке и ясно видел что будет завтра рабочие залы рельсы горячим варом и потом никто даже не догадается что когда то здесь шел трамвай и не теплое рье и музэтим ребятамещемного много лет не забытьэтой серебряной дорожки сколько конизаливай рельсы варом настанеттакое утро осеньюлизимой иливесной проснешься и еслинеподойти к окну аостаться в теплой уютной постели непременно услышишь как где то далеко чуты слышно бежит и звенит трамвай и визги беутренней улицы на широком проезде между ровными рядами платанов вязов и кленов в тишине перед тем как начнется дневная жизнь услышишь за домом знакомые звуки словно зати каютчасы словно покатысяс грохотом десятков железных бочонков словно затрещит крыльями на заре болющая преболющая стрекотасловно карусель словно маленькая электрическая буря словноголубая молния мелькнет и исчезнет за звенит звонком трамвай изашипит точно сифон с содовой о пуская и вновь поднимая подножку и вновь качнется сон вагон поплывет своим путем все дальше и дальше по своим потаенным давно схороненным рельсам какой то своей потаенной давно схороненной цели по слеужина погоняем мяч спросил чарли асноответил дуг ласстостаяла погоняемаа

Висновки:

При виконанні комп'ютерного практикуму я отримав навички частотного аналізу афінної біграмною підставноки, навчився методиці атак на цей шифр, навчився критеріям розпізнавання коректності відкритого тексту. При роботі з наданим шифротекстом я застосував отримані навички для визначення ключа та розшифрування тексту.