Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки.
Варіант – 16.

Виконали:
студенти III курсу ФТІ
групи ФБ-82
Сумовська Юлія та Руднік Анатолій
Перевірили:
Завадська Л.О.
Савчук М.М.
Чорний О.М.

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 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 No1, 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.

Опис роботи та основні труднощі:

Програма містить наступні функції:

- gcd – знайти найбільший спільний дільник;
- findModInverse – знайти обернений елемент за модулем;
- linear_equation – лінійне порівняння;
- icx – індекс збігів;
- break_affine – скласти систему рівнянь для взлому шифру.

Спочатку програма шукає топ 5 найчастіших біграм в шифртексті, потім комбінує по 2 біграми (найчастіша, наступна за частотою і т.д.). Те ж саме відбувається і з частими біграмами мови. Потім вони об'єднуються в кортежі такого вигляду: (найчастіша біграма мови, наступна по частоті, найчастіша біграма шифртексту, наступна по частоті біграма шифртексту).
В функції break_affine ми проходимося циклом по масиву кортежів, знаходимо ключі, розшифровуємо текст цими ключами і алгоритм розпізнавання видає нам єдиний змістовний текст.

5 найчастіших біграм зашифрованого тексту:

се
дэ
хв
те
че

Розпізнавач російської мови:

Змістовний текст відрізняється від не змістовного на основі індексу збігів. Для не змістовного тексту від лежить в межах 0,38-0,42. В той час як у змістовного – він більше ніж 0,5. Ґрунтуючись на цьому спостереженні, був написаний розпізнавач. Він коректно обробляє всі варіанти, залишаючи тільки один змістовний.

Зашифрований текст:

фелсэугиселбуйэятеополмхфкплоыющпбвуцакэюйкзыкусявялеюыкуешяэюазыкйюяьзвусяюыпдэжввя
тедыюяячтхкзыереявйвтэебуьагзлчедэвюцэеямадюзвюечюцыющыешгфлцхазиччеолмхечнзпвледсдя
мвзжевмэбйрбсюряийвюухыешлифвсочлюряийвюухыешгтбютазцчягтьчяяжцэфлпнитсетеуюйвзсд
яшевэущенибсчхеюезючеузйьяюпсдямаээыгнзйвиснрижшдуйьюфлийэфазшгкякзшьяяпатбдспвязги
нкэтбыпрбггтбшсййсыдэядемечмяйвжзазлдткхчбчмчйвувтгинкэтбыпйлхьагвцкзьяэькамащлщзмх
ыкмчуябллдпволмхечмчкбущтзвцйвнбюяеммччедэядаяэюнвшьюзщащлкэфлпнцьочпмменбюоззеяэяв
чусвесехкчюгупвйбухввлэыволмхсьжектьясезвььдснлулшдяюпсюагякбжйуяичявуссеььхвжщтьжсуй
сыхсмччесссвемнэсыеюолрщдэисшисерекэьбпэлддыеюрябенбауасызцчрецямеезфразлдагжчюзнйпуп
ввеюкусцяэчретлкзтзцаущцоэчуегчрразыепуочссхсзмнзфкузмасызэыечеолрщссрятекщазшыжешьч
екбмаедуззэитсефкфкемющээжйэьвррщтьжслеаявежчзлбрблфкдчщдсзсыыцущеюфлеяэюипччкггу
техсаагямаэчявемцщибыекичлвьчблтгинаузэеядюдэпббйььащябазуьхсэвчгээебсныьяплгхслшднзы
свнслызенбйдэгэфлпнюяшжвмусвесехкмащлсющрэчретгкэбйцйсыхсфкемуйыгфлхуыкнзшжксмгээеб
сьнытгжчюсйвзйюянюьююячеуспвссмеоеочхедэеюфцжедыющээвныпшжаюфнпвевхчфкаеуйгзшглс
йэыежеаязвюерекэхуввжвэйяжссйвеьмчфкэьхедэеюфцкыюязсыечвпзлгвюаежзкювесехерглсрьхяэю
еюзэбеаяэсевйувюухыешгеющразцччеолмхечнзвчичймсеатьяччебддятеубфлцсрбрщюяевисувпзшгв
юаежзчююячеумиежвемшдвчусмэебрябйвесехкпюмчзуеншжьвдядюсссввчумыепвплящыдхвощкчхсй
ежещчссжвдюцыющфстепйцхыедэкяплгхазлдвнухокусызыцнздчузуьхвывпзкчуйцйрясетегльнйвйст
ерирчссцяэььсжвдядющашсэбауретещщэщхрхвмчющщалсвчумыесыедшьдямзггээрспвеввьнзмчшж
ксдякчдсбдемиваецяэююядчймхуыквщзлбйпцкэиузбвюдэпьфэрщэщхрхвнйпчячкгхеьбфтсличцдмщйв
цяэюспвчсемщйвцяэюспвчввуеивхзшгебрщвюцэрякбсыюяхвывдщэщхрхвссверчпмхвхвхвегжчрчдэпвэя
щаензэтьссувнзшупвзйазэяхвывувпвевшврбюятехльанйижректижуеивяькбгзблвюжгебткязрящаен
квткелофчельсвузфнфлшпкякбсыеюаыедшьузьярякбуяевйвэясчиищзэнгитьюдэтежвемсейвчясемзцчв
есехерщфлюзщащлпсдбаучедемяиоьусшьоьпвевшвчебдувнэеюгщэщхрхвмчльсвфэьтсефкюкчеочшвх
свеььсссьвмвнауслкззэсрюйгяевмчсзьятеуйочдэвсмччехчгчхсвяослехехчрщзлсыйвгсмчхньяхвывдщэщ
хрхвсеумвеолфрьщцэнзйьлвдсвчрбжавюблнззэиткясерщзлбйпбшзаземуйячтхзэеяйэщедэхетекбьщм
чаяверeывхвывисвззлшдзвьчбдцююяевкщкчехетччедцющблфнмчььхедэеюжчьстевектзэзлфзюяудз
жуныпкэяьввнбюязэшынзэсбсюнаувюпвевхчочдэсыячопдэядемюыячссхвхзфтдынзуйсыаечеечювемп
врбвюблшдыузчмщпвоелбоыбйшьтлуймзссччхзюйзэебсыюяевыеисшмшдвнауслудзжунетибмчллыщц
энгхекбвюцэпненрбкщээшдкэгчьвшбюясебнпбшпжжцэьбфншьаеыеэюьтыднэнйрбпукюбйпволеюьщ
эщхрчсхвйвдащлдэпббпгьхейлсюбпсьщщьясктнщазлцсуюряезбпвчмтсензтедсыехнпаябслсввчхерет
еонвюдчдэслтгбйряеввяевхкыыйвцупвшелеезфтщжреьдьзюяемукпвчесехенсдямзмечемщзэцсуоазйь
агзлкщкчехетччеячявемййряоьхвчсуммващжчфтгчдчакэбцймзбпдэьдрьшсусшдучхвуспвяюпсцютб
нзазпныцчеэнзэблчешчрчбдмнюяевнлазыеььуйклауесйвагйвиснрпаяьщзьщчюпцкэссьмкяпвьдокнлхупв
яютжллыщяьяяпэижсьйябшьрсоенбижчедчячнрижхвчснзисилмзяьаешвячиязбцххвускэюяувхсйбашбл
ждкззбвсэцкэосмчпцкэссогюцкразгупвнрипэюебоепцкэссьмпуеннзкювцслтефьунюнуясетеанкэтбф
цнздэядшбаущайвмгеюющжджгйвисдямзьярщрчфтьюдэпьэямарыкэеюжйсыедшьдяхьакивэянгющр
чмчредэядрчрехвочщщщзебдэпбщзыкчзщецдьчрчнрипхуоежяуйазччййпбптьнсвймячтхслпвяютбээ
жчжлыцыцыеевяххуухябчюьсщненлендщзблфрьщмюфлвеввтецщгчуеивчсцйыкряевхкйьрчллкябахуя
ютбшврежзьясечеввумхчтефьунрясеулзбзыыпдэжчгдпзыпйбашюйцэпнцеатыдпзбпхуоечсдэйвдэык
делеезфнйбашчедэпбщзыерглсткхнчюлгбличжчоелесеияебмаьдшьйтпбяьпцкэссьмопывичхвыехнпуе

нуяблпуггблчеэьсьсконыпяюкчрешжкскюерефещщпсуммващжчфтфкузуйыешнинйвдчыеэющзмсхуок
ллаузчречеячйзаэпчнлоыыпюящаазыеплрявчхсжешьяьевпзбпнрпаяьйсудпвдчйлвсочлюкщжчечкненкэ
тбсыюящайвхсньедемиьоеияеюцдшьскусучхвусччййпбюьдэхесюьсзмчятенйкщзлюйтгсыедокжвузца
пбщзьявесехкюешхблрчхщкрвюльвьтгнзнйыддыжглсйэыеебьячеаеьчссрщецуххвмглсйэыерейваыеют
бзчучкбээсчхсйечеячяваеюясехеюзеюкщыемхмеыефкаеютазпссуслрямсюяевыеисаезмчеывдсйбашсл
ифжисефкдяевлснюдчоедатбющчюьчаявемнггкэвсткуевемнфллвтчнэщащлвьезьяевзмосжвыежзкз
гзьяевзмосжвыежзггющусжсжвйчььеечесевяхвывчыйвюэпэфлпнщевэжгшпуюебйэмарщкзблгуьщья
цдзввяуяюйвнауслпвдэьяждсюкзеюпварарывьсхвчыйвгсщайвзсдязндчочшьпвевумрсумщзфтшьисячд
ярбюяблнзуяуйазоыячнзцессагээхеусумфтуйкэювхетклаибждыецяевхскэгчьвдяуйазкляаыдзмсеьчвв
юкцелеоьфеумвьрсочлээыьдснлйчшмшддчочкненнззчмщцэьяхвывчыйвгцкэбажймхэсмчягтбюненмч
дсисемшдьйзлфлеювекзфнфлсроыячпвйлэщеюввннйгчлцбйчэфлмюоржгкэбйагйвьсжвчыйвюэенсеьзю
ямхнзпувлэфщряевемевтэнзвехульыызпжатсеюкчщкзблыпзбзыыпйвмщсюущзчвярыеютбблдчочеупв
зтуйзыющцэбапбщзецтбфркчмщцэквпввемчсехввежвхвжэщзыгкязэпненпвочвзкяцссувюпбюсаячсла
ибждыеягбйхзклблкяпессичжчвненсюзэеяевхскэспусцвдэйвдэылфрьщсэгязтпбпарччвдчоеяьщчыкмч
хщуььэенсыбйфлющэвчекяхвемчекяхвемчегэтбблйбашисдсюеуеюврчзтсевектбльясэенвнтбтбытеяу
йазггпсвнзэеяхвываеыеэютбетсюыдчеаквьгнысоедэвюыдевивтчднгзюйрщссхввесеечвзсюеюдчэбдыс
лысткалцэенусявблсейсоехкляуйазмчоеретелсэьолфцвюэяыейвмщвювюьсиядюзслейюгульычреаячещ
юкюкзцчсзмафлэчщюецблцэжчгынзэслепзенаесскыфлеюыглсолкрслшднйфльвчейбгублшдивлсшьпвт
ктеоехззэьнхсрбфршгеваеигьдюепведоецявергеюзлюыйвцуцакюдэебээюьакгнуяхсэвьйкэжчмгебрщуе
фепюввумчеичжчюкхнвсмчфжявэщебювлютытчевивтчдньюолрщывувуйуеивогюякшвдярыфлюяче
теоныгющкзыкпюивйсдэбпхефщкзблгяевеглсуерщщзбльяпничбюжйкбуйуеивхвусолщрыефкаехвлупб
чюзлкяывхстехыфлюяоынзэспявчюеуеечпзжйчещюкюкзцчмнкэтбкчолмхблжглсызенбйрепвчетеону
щкчехетцчмхазшгтбвнслщвклхлйнслыспуывцявцреаеуеююгяоьлвчыфлюяввссаксеивйсдэбпсербнзюсв
чумыесекнипреаечщкзблннауслюяфзггфлбдлюряылряткледсхссуслрямсуюютслврчвеягфлшглсолкрв
юьсзммчвнфлпнюяьнгзхйфльвйбашщчредэжчгдпзыппарщблкяптсеректцчйвиаблкяфзьщгчдэмсющпв
феумшвсбчючюшвшеуеечпзсытбзтюяевувущслйэеяэщтьдвзтьяемдэмсчемчольямюоеумчерчрьусюе
йбашмсрбтисеияевмащлюякшзцьшжшжхвпмрщкзбляеивнэюынзьяхсжвхсзмичжчхсжвхсзмыещау
ьвведхсзмдчочзюмщпцшьхспвдзклшдчэщажгйвисемяютбяьбнкэтбыпывфьевдяайфлющыпвеечумйба
шсеьчыуоеязклпуюйээсюцятеоптьтчевивтчднпеанхкрчвсоедэслуччеемпвывэнлсхзклдчочпзенщазлзн
кэтббпткдэыгблывжгкряьйбашыузбсышьхсибнзблевивтчднгзьяевзмосжвыежзьярчюсдэслчевзнйзэ
счдыйвгсдчочаяюекбзлщзкздыеюзбзыхвоисеьвдэщакюзчьупьщынзюйдзеюазыербжахсюсдязненсьяэе
юкэтеюгебрщссусзвусусфкхсуввоцчжэгящаенгьшжшжхвпмрщкзблцыйвнеллмзклшдщзггйвтеьюкщс
лусемяьвесехкпюннзэкювюьсусшдллауюйкяюекбзлпвйбашмсчевздюшвжнмьхвикжврчььяягебрщпвзбз
ыиждэтбнзпаебдыпуенлсьваемэеннйреаеуемтсеисвзщащлитсенэюяаетеввжзцььчььэсвчумыербюя
блюяюьмчрепвтьзытгюяхвхвлюлгуязсцящаенчепврбвюрчссйнйбашзыйвгсдчочзюгяхвхвхспужгкрчсщз
слчющехямахьисввхстеоненкэтббпгдянжгебчюслсюыдзмзсбсвявевекгющвненсюслрчгчвсщнсеияюйы
пжгкртчюнкэтбыпнзкясеулпуаеизпчуеивчсисаышьхскятбжвнркяеяюятевгнзряхсзмнюфляьусюеыел
лфрьщоптеонрбжедэкзеюблечдззлеювехввафлфзыпювфергеюебшьдятехлщаьяоьтыфлеююнуеивхву
севяхуйрывеичжчжвхсжвэянгхкдзклйвмщтьрещсюеезьючерчыеуцтедэбйвнхкдядюжгкряьгэмхуйщз
аэесфгхезстечеаеюзыпжгкрчсмбчюбйчелеассзггувабьявчьдпзеюгявеэсувющпвзбзыыдкбээждректы
дсюшддэыдчемчольянгжгфлзгкэбйуяюйбйцйряоьфщшгхерчфгхеечювлюфлнюолрщывректнйябьядэы
гблкяпнуясктбзрссхвтгинаусльябаибыдчеччйзчюшвшеюгкэклфрьщещкзблтзьщхспзыпагщзэчьнбйит
вейюслэямюичжчтякщзлввссувечгрггчсчярщжйсюдэжчлвпзжйсюфлюяюйщзьщьбьяыккгкэыкшлиф
бйклхлхлчьшжшжьбфтслнзвефщцешьисввчыйвбвкыувывычреяюебхзклюйфлссххьбфншьаеуыхендзм
чевзйэжйпбггссвезсоыйвбврбфлсюфлхвсепцкэссчсфненфкмчущюясесюыдвннзкььчпзсыпсагзыкзыере
йбашьщслфзопьсцбауретехеюеаяеюдчнуаеферглсресенлазыечзоыйвбвущпбблчеююслсюьсвяайинхкю
аинюйсьхереочлспвтгнзряшдывректнйюыйвыненпвхвывпзбпдэядаеллэщкюыдзмкяевйвэяюьакгныпт
куюзэмюдчочмчуеюврчссьняюкчььчеаеьчссозюяуйазуььчмчфкаензтеечмщчеяьдэюйыввненсюслтеон
цеьуьяынкящюецдэтбнзевяхшгебряхвчсжвхсуюебшатбндезфнщзеюфлогфрзляьдэюйысссющщзпцкэс

схзшгебвцжвзсрчрессвеувэбюясещййхльвчвясеулпвяюкчейрявчцхкщыдуюебегжглсплгхазяжжехщсла зяжрепвчеуююнюйреаеуеисуюряезфцуйуящаенчербжахсьчссьехщслазяжсюгуткхчсстыфлюяеюоеху ювэслектьюдэтежврэитсеуегчррслюямююякбеюмееупвотсетедэхегчфкхсрбжащлпчюеаеоквссввчх кряевхкчюфлчснзызслчэсынзэсебауксхсзмпвщюряевфтсефщазжаущсэйвисхсфтсечэнзжаущеяэьэса езммчплоыжгфлютыемезюшдяьяяьнгзльпвяютждэтбнзмхввйугчьднзячуврэгязтябаухсьзфцрбрщче аеьчссдесемненкяхввеиясехеыкчеечасьугчймфненнзсьячвэйвисемдынзьщйхввьйазульябеатыдссуймчв нфлпнтбаунзщайвцвдязнфеньыйфлбатжкэбйчэщакюфлнющрзлпвмчрензюехсдяэявчвякбьяезжйкяею рямлсюжйдьцяэюбйвнкэтбжйюеедхяулящсюусишскйсумыеретеузазлдывисшдучрекэссчэцхыерглсэс ыкшьчэкэмарясецэретелсаеыасыуяячувемнэющедочбдызпжчэкэкюзлфнфтсейбвцвчщдрбюяцэбебис есзтбьщжасыьяячувттсефкпвочбдткрчпйзэеббпфтсефкхвйвчзоыувывпщэщхрчсвесехкпюнзкэоьввь йкэлсэюрчнсдяйчььочжэтещцжваныпкытбаескшддыйвуюнэтгфльвзвыгтбыксззгьдьчпзжйжарячев ечзжйыуллэщбйинкщкюслхедэеюжгкряьрчуецящюцйсбрщчсусльивуспвоейсыетккгющдчоеусеюйвфя пуюкскмнйвуйбрггяьудзжунфтаэмюкщмчнрдыюяоссуенуяевпврбвюнзээмчсьячюисеревтьяемэщцйсл хедэеюетсефкдэпсаемчсьячшймчцядыввсюхвжэмцщзвюыпмчтецяуймчвтьяемавуявчрлифкщфлпце юсбвеыефкдэхеыйазюдзмочумхвхсгчретещайвьчссцэфлпнщедсфбауфкпхпуссывкбвюцэийзэебсыеюф лхвфеумхчмзйхзлпжльсваепзггьддвэяэьбсббазцчсыедокжвэяфзслчюпсжгйэфзггйвтетглсолкрсюыдз мййслопьсюевэазхвзупьвекынзцезюаыедшьаеэдемпврбвюпсьюкщслчэжгжгуяскпзбйыгфлозвюдэжчд ьхзуйпайхслитсесемчюисемчюеьчсапэнгющцйслхедэеюцдьчаеыуокявзненыуокявээччаегчоглсуегчрра зыссеречэщащлющфлрецхкщзчюенйуегчррблюямюзлфтшпхчряьвдэсчцэенрбюясеечгрцйцахуплряхве чиеызюйазеюкзлдхедэеюмчгчлсдятенйллауюйкябймчссшисербющфлюваезмферчряьнгзоктеонечювл юичжчдсичжчрбцышьрэххзлтбпэисшьвесейвшащлкззчреоехебчнэщащлдэпббпуюебеядчоеяянсыещс зззчячпзжйьбьяыежвскюаожлеюеыайхслмчсехетлсющеччисвзцьечощазыкттсесстэнзчюкщцэдыт бюясежзрщщрцеллмзклшдпвуеиввессрчювхсдэядхсмчисудтеонмсссччремччесссвэяевхктнпбшпывгч йзьюреаепьжевнслсюьчрэпчеьфкдчщщцэщесквнсюыдплпццозлхвхсуспвыввзыцедшнмцклхллхржгкэб йкэсечклсжврыпалгхеретелсшбюясецящаенкщхедзьюьчрчцнюйсювнитблщзьясехеаспььсхвйвргитря сляютжедшнесцяевузьясехеаспььскярчянюйкэшьхцтедэбйпввесехейюкязлсюыпаечсхчщязсфьвнзэфз шгуяхвемретелсдяюйдчечссвеувпюселбуйзнентеончещююыслшдхзуйпехщзлюдзмкэрчзвцщтьыюшдг сюснзбйлдтеонмспйазбльябезюмцхедзкльюкщвюуочюебядезнзфнсыввмчисввпзпчнйччаегччвнцчлла ууьдэжчшлазыказкздыпсолдыхвчетехезсбнпцкэссяьреаепьюяевыеисдямзауьщблсюичжчьицяйвжзе юичжчщюкщыехвваущсевнауслнззввямавсфьдэблшдягебрщмхазмеллэщкюыдзмгдяннйжчэннйтеум ыксзтбзрцэзлфзжйвнинбйклхлозрятенйреаеуезуенлсьвузфнфлшпкяюйьящатждэжчхыувягнзряувзм дыющщайвулфрьщнгющретьичжчвненсюыдччжчуюющбйпсыкягжгебьтмюфляьцчучфкдэжчмефе дзвюэччемчолкяеящаенщзфнфлшпмчолфцсляюкчреьбфнкзьтьюдэтежврэсыитсензвнетээмчисввузк ящаенссочдэггинкэтббйпеаяхвччсезюкщзлсеумветеоненкэтббпуяблсюяюыпечфяхвхвузшгебуйазюдп врбвюрчссегфлбощзшгебжвегинаусльямюплпупугчьдччйзжгдыыдьсхевеыввваййблхвкяевуврбжахсюв емшдлугчожплгхмахсьчтесепврбкяичувхзуйгзеюфлртаэнгинюяблшдпвмчвсщйрясесеречэщатзьщвве мхввепвнэеюдчфщьщзлслюйблхвцщтьэгющбдищтедэдэслуьнсйвемшдпвичжчвзцчыежсклхлхлхлйнлсь вузфнфлшпьбыякяльанйтквнитблпуывусонкякбуйцэзлфзщахейсдямзвюфлхвкяцюзэблдыгуоыетблхх чсыввзыцыедзеюоьояьнгзлькяфьдвпзжгебрявеэсузьщтньяясехешьтеонрбкязлучоншыйупаюйысжгй энгющбддяосчевненслягебрщрбеюцхзчюкчзквррщзйвчясемздцяуйкящаенюйщзшглсплгхвюьсусшдхзу ймьищээмчюисемчтепйцхыельсвузфнфлшпрбющфлювзнлсьвемпцлслзьюьсхыфлюябйхвйвбьшжшжь бфтслнзкэгячсжврыувывусдэпбсыинщазлйчдсаяэюазшьяятеозьщйхльхвйвщсуюдчпятеыцдэпбфцйсл юпэмзьюьсзмвнфлпнбйсыллэщмзвюфлхвцдьчаевненслцясехешькэуюебмззгебебхууйгзжгщагякбкэряв ехвтеонмсочйлазыедэкявехвуеивчсфкаеисвзитсейввтээхвйвшащлфржаитазссвеувбььчмчвврчвеягеб рщкямадюкщзлсемлряоевесехереоеечювююфляьищээпвгчйзкчягебрщтгинауслкяеящаеныспцкэссжях вхвнрипчечэщзвюдэжчдьуомащлкзьщйхввмчызенбйбпссвеуввйибзыипюеаеоеищхспзбпвеечумдькеия техкдэжчусвчумыечейлээзлагебрщфнтеонесчечэжербинщзклдыеюфлвагякбиненмчумндфкаецхкщзэ беездыжглсчевзулшджахейсдязнььтрееьвеечшжучоншьйупаюйысинхежвнлазыкияйвагтбкэжйфе вемнщазлнгхееуцэзлфзгувюпуювгэхзклшдреаетепюшчшлйнпбпжунцевчхгувхвузфнфлшпдэпббпвеечу

мчятенйнйкэвюьсусшдпведшнмцэлинюйжаувреввьдрбпсоррщхчдедэкзеютчичжчжчикжвэщтбсыь юфляьфкэььчягйэброымцкэмчрехвваущсечедьцяэюеювюжгьяыедэмюфлогинюяблшдпвхвйвйчучввум хчагьдевягфлазпцтедэочощгзсыщзьщввдявеяьыеоьезфнфлшписячрэфлпнитсечэкэюяячуваезмвнпбзч юегйдзеюазыеитаэблшдпвтеонвсззнйщйрявччежвхсдязнпапбуйююющбйпсшьвесейвшащлггебрщссу севусшьеввефщкзфнфлшпьюкщслююющбйпсмчвечешвшспяэятеонбйуеивчсфгющвесехкцюкщмчувзм дчввуребдэмюфлхвдыеюпэмзьюшвэявуьщбдмзсымсаглсювскускрюйысагзыкзпвосывокяввоыдшдреае жвхвйвищебювув

Ключі:

a = 370, b = 312

Розшифрований текст:

борисзаэтовремясвоейслужбыблагодарязаботаманнымихайловнысобственнымвкусамисвойствамс воегосдержанногохарактерауспелпоставитьсебявсамоевыгодноеположениепослужбеоннаходилсяа дютантомпривесьмаважномлицеимелвесьмаважноепоручениевпруссиюитолькочтовозвратилсяот тудакурьеромонвполнеусвоилсебетупонравившуюсяемувольмюценеписанную юсубординациюпокотор ойпрапорщикмогстоятьбезсравнениявышегенералаипокоторойдляуспеханаслужбебылинужнынеус илиянаслужбенетрудынехрабростьнепостоянствоанужнобылотолькоуменьеобращатьсястемико торыевознаграждаютзаслужбуионачастосамудивлялсясвоимбыстрымуспехамитомукакдругиемогл инепониматьэтоговследствиеэтогооткрытияеговесьобразжизниеговсеотношенияспрежнимизнак омымивсеегопланынабудущеесовершенноизменилисьонбылнебогатнопоследниесвоиденьгионупотре блялнаточтобыбытьодетымлучшедругихонскореелишилбысебямногихудовольствийчемпозволилбы себеехатьвдурномэкипажеилипоказатьсявстароммундиренаулицахпетербургасближалсяониискалз накомствтолькослюдьмикоторыебыливышеегоипотомумоглибытьемуполезныонлюбилпетербурги презиралмосквувоспоминаниеодомеростовыхиоегодетскойлюбвикнаташебылоемунеприятноионсса могоотездавармиюниразунебылуростовыхвгостинойанныпавловнывкоторойприсутствоватьонсчи талзаважноеповышениепослужбеонтеперьтотчасжепонялсвоюрольипредоставиланнепавловневос пользоватьсятеминтересомкоторыйвнемзаключалсявнимательнонаблюдаякаждоелицоиоцениваяв ыгодыивозможностисближенияскаждымизнихонселнауказанноеемуместовозлекрасивойэленивслу шивалсявобщийразговордядюшканеодобрительнооглянулсянапетюинаташуоннелюбилсоединятьба ловствоссерьезнымделомохотыздравствуйтедядюшкаимыедемпрокричалпетяздравствуйтетоздр авствуйтедасобакнепередавитестрогосказалдядюшканиколенькакакаяпрелестнаясобакатрунилао нузналменясказаланаташапросвоюлюбимуюгончуюсобакутрунилавопервыхнесобакаавыжлецподум алниколайистроговзглянулнасеструстараясьейдатьпочувствоватьторасстояниекотороедолжноб ылоихразделятьвэтуминутунаташапонялаэтовыдядюшканедумайтечтобымыпомешаликомунибуд ьсказаланаташамыстанемнасвоемместеинепошевелимсяихорошееделографинечкасказалдядюшка толькослошадитонеупадитеприбавилонаточистоеделомаршненачемдержатьсятоостровотрадне нскогозаказавиднелсясаженяхвостаидоезжачиеподходиликнемуростоврешивокончательносдядюш койоткудабросатьгончихиуказавнаташеместогдеейстоятьигденикакничегонемоглопобежатьнапр авилсявзаезднадоврагомнуплемянничекнаматерогостановишьсясказалдядюшкачурнегладитьпротр авитькакпридетсяотвечалростовкарайфюиткрикнулонотвечаяэтимпризывомнасловадядюшкикар айбылстарыйиуродливыйбурдастыйкобельизвестныйтемчтоонводиночкубиралматероговолкавсес талипоместамстарыйграфзнаяохотничьюгорячностьсынапоторопилсянеопоздатьиещенеуспелид оезжачиеподехатькместукакильяандреичвеселыйрумяныйстрясущимисящекаминасвоихвороненьки хподкатилпозеленямкоставленномуемулазуирасправившубкуинадевохотничьиснарядывлезнасвоюгл адкуюсытуюсмирнуюидобруюпоседевшуюкакионвифлянкулошадейсдрожкамиотослалиграфильяан дреичхотяинеохотникподушенознавшийтвердоохотничьизаконывехалвопушкукустоводкоторыхон стоялразобралповодьяоправилсянаседлеичувствуясебяготовымоглянулсяулыбаясьподленегостоялег

*окамердинерстаринныйноотяжелевшийездоксеменчекмарьчекмарьдержалнасворетрехлихихнотак жезажиревшихкакхозяинилошадьволкодавовдвесобакиумныестарыеулеглисьбезсворшаговнастопо дальшевопушкестоялдругойстремянной графамитькаотчаянныйездокистрастныйохотникграфпос таринной привычкевыпилпередохотойсеребряную чаркуохотничьейзапеканочкизакусилизапилполубу тылкойсвоеголюбимогобордоильяандреичбылнемножкокрасенотвинаиездыглазаегоподернутыевла гойособенноблестелиционукутанныйвшубкусидянаседлеимелвидребенкакоторогособралигулятьхудо йсовтянутымищекамичекмарьустроившисьссвоимиделамипоглядывалнабаринаскоторымонжилле тдушавдушуипонимаяегоприятноерасположениедухаждалприятногоразговораещетретьелицопод ехалоосторожновидноужеонобылоученоиззалесаиостановилосьпозадиграфалицоэтобылстариквсе дойбородевженскомкапотеивысокомколпакеэтобылшутнастасьяивановнанунастасьяивановнапод мигиваяемушопотомсказалграфтытолькооттопайзверятебеданилозадастясамсусамсказалнастас ьяивановнашшшшзашикалграфиобратилсяксеменунатальюильиничнувиделспросилонусеменагдеона онис петромильичемотжаровыхбурьяновсталиотвечалсеменулыбаясьтожедамыаохотубольшуюи меютатыудивляешьсясеменкаконаездитасказалграфхотьбымужчиневпорукакнедивитьсясмелолов коаниколашагденадлядовскимверхомчтольвсшопотомспрашивалграфтакточносужонизнаютгдест атьтактонкоездузнаютчтомысданилойдругойраздивудаемсяговорилсемензнаячемугодитьбаринух орошоездитаанаконетокаковакартинуписатькакнамеднисьиззаварзинскихбурьяновпомкнулилисуон иперескакиватьсталиотуймищастрастьлошадьтысячарублейаседокуценынетдаужтакогомолодц апоискатьпоискатьповторилграфвидимосожалеячтокончиласьтакскороречьсеменапоискатьсказа лонотворачиваяполышубкиидоставаятабакеркунамедникакотобеднивовсейрегалишвышлитакмиха илтосидорычсеменнедоговорилуслыхавсяноразда вавшийсявтихомвоздухегонсподвываниемнеболеед вухилитрехгончихоннаклонивголовуприслушалсяимолчапогрозилсябаринунавыводокнатеклипрошеп талонпрямоналядовскойповелиграфзабывстеретьулыбкуслицасмотрелпередсобойвдальпоперемычк еиненюхаядержалврукетабакеркувследзалаемсобакпослышалсяголосповолкуподанныйвбасистыйро гданилыстаяприсоединиласькпервымтремсобакамислышнобылокакзаревелисзаливомголосагончихс темособеннымподвываниемкотороеслужилопризнакомгонаповолкудоезжачиеуженепорскалиаулюл юкалишиззавсехголосоввыступалголосданилытобасистыйтопронзительнотонкийголосданилыказал осьнаполнялвесьлесвыходилиззалесаизвучалдалековполеприслушавшисьнесколькосекундмолчаграфие гостремянной убедились чтогончиеразбились надвестаиоднабольшаяревевшаяособенногорячосталау даляться ядругая часть стаипонеслась вдольполесумимографаиприэтойстаебылослышноулюлюканьед анилыобаэтигонаслива лись переливались нообаудалялись семенвздохнулинагнулсячтобоправитьсворк увкоторойзапуталсямолодойкобельграфтожевздохнулизаметиввсвоейрукетабакеркуоткрылееидо сталщепотьназадкрикнулсеменнакобелякоторыйвыступилзаопушкуграфвздрогнулиуронилтабакер кунастасьяивановнаслезисталподниматьеерафисеменсмотрелинанеговдругакакэточастобываетзв укгонамгновеннопри близилсякакбудтовотвотпереднимисамимибылилающиертысобакиулюлюканье данилыграфоглянулсяинаправоувидалмитькукоторыйвыкатывавшимисяглазамисмотрелнаграфаип однявшапкууказывалемувпереднадругуюсторонуберегизакричалонтакимголосомчтовиднобылочтоэ тословодавноужемучительнопросилосьунегонаружуипоскакалвыпустивсобакпонаправлениюкграф уграфисеменвыскакалиизопушкиналевоотсебяувидаливолкакоторыймягкопереваливаясьтихимскок омподскакиваллевееихктойсамойопушкеукоторойонистоялизлобныесобакивизгнулиисорвавшисьсос ворпонеслисьволкумимоноглошадейволкприостановилбегнеловкокакбольнойжабойповернулсвоюло бастуюголовуксобакамитакжемягкопереваливаясьпрыгнулраздругойимотнувполеномхвостомскры лсявопушкувтужеминутуизпротивоположнойопушкисревомпохожимнаплачрастерянновыскочилао днадругаятретьягончаяивсястаяпонеслась пополюпотомусамомуместугдепролезпробежалволквсле дзагончимирассту пилиськустыорешникаипоказалась буряяпочерневшаяотпотулошадьданилынадли нной спинеееекомочкомвалясьвпередсиделданилабезшапкисседымивстрепаннымиволосаминадкрасны мпотнымлицомулюлюлюулюлюкричалонкогдаонувидалграфавглазахегосверкнуламолнияжкрикнулон грозясьподнятымарапникомнаграфапроливолкатоохотникиикакбынеудостоиваясконфуженногоис пуганногографадальнейшимразговоромонсовсейзлобойприготовленнойнаграфаударилповвалившимс

ямокрымбокамбурогомеринаипонессязагончимиграфкакнаказанныйстоялоглядываясьистараясьулы бкойвызватьвсеменесожалениексвоемуположениюносеменауженебылоонвобездпокустамзаскакива лволкаотзасекисдвухсторонтакжеперескакивализверяборзятникиноволкпошелкустамиинодинохо тникнеперехватилегониколайростовмеждутемстоялнасвоемместеожидаязверяпоприближениюио тдалениюгонапозвукамголосовизвестныхемусобакпоприближениюотдалениювозвышениюголосов доезжачихончувствовалточтосовершалосьвостровеонзналчтовостровебылиприбылыемолодыеима терыестарыеволкионзналчтогончиеразбилисьнадвестаичтогденибудьтравилиичточтонибудьслуч илосьнеблагополучноеонвсякуюсекундунасвоюсторонуждалзверяонделалтысячиразличныхпредполо женийотомкакискакойстороныпобежитзверьикаконбудеттравитьегонадеждасменялась ьотчаяни емнесколькоразонобращалсякбогусмольбоюотомчтобыволквышелнанегоонмолилсястемстрастны мисовестливымчувствомскоторыммолятсялюдивминутысильноговолнениязависящегоотничтожн ойпричинынучтотебестоитговорилонбогусделатьэтодляменязнаючтотывеликичтогрехтебяпроси тьобэтомнорадибогасделайчтобынаменявылезматерыйичтобыкарайнаглазахдядюшкикоторыйво ноттудасмотритвлепилсяемумертвойхваткойвгорлотысячуразвэтиполчасаупорнымнапряженны мибеспокойнымвзглядомокидывалростовопушкулесовсдвумяредкимидубаминадосиновымподседоми оврагсизмытымкраемишапкудядюшкичутьвидневшегосяиззакустанаправонетнебудетэтогосчаст ьядумалростовачтобыстоилонебудетмневсегдаивкартахинавойневовсемнесчастьеаустерлицидоло ховярконобыстросменяясьмелькаливеговоображениитолькоодинразбывжизнизатравитьматерого волкабольшеянежелаюдумалоннапрягаяслухизрениеоглядываясьналевоиопятьнаправоиприслушивая ськмалейшимоттенкамзвуковгонаонвзглянулопятьнаправоиувидалчтопопустынномуполюнавстреч укнемубежалочтотонетэтонеможетбытьподумалростовтяжеловздыхаякаквздыхаетчеловекпри совершениитогочтобылодолгоожидаемоимсовершилосьвеличайшеесчастьеитакпростобезшумабе зблескабезознаменованияростовневерилсвоимглазамисомнениеэтопродолжалосьболеесекундыволкб ежалвпередиперепрыгнултяжелорытвинукотораябыланаегодорогеэтобылстарыйзверьсседоюспин ойиснаеденнымкрасноватымбрюхомонбежалнетороплivоочевидноубежденныйчтониктоневидите горостовнедышаоглянулсянасобаконилежалистоялиневидяволкаиничегонепонимаястарыйкарайзав ернувголовуиоскаливжелтыезубысердитоотыскиваяблохущелкалиминазаднихляжкахулюлюшопо томоттопыриваягубыпроговорилростовсобакидрогнувжелезкамивскочилинасторожившикарайп очесалсвоюляжкуивсталнасторожившиислегкамотнулхвостомнакоторомвиселивойлокишерстип ускатьнепускатьговорилсамсебениколайвтовремякакволкподвигалсякнемуотделяясьотлесавдругвс яфизиономияволкаизменилась онвздрогнулувидавещевероятноникогданевиданныеимчеловеческиегла заустремленныенанегоислегкаповоротивкохотникуголовуостановилсяназадиливпередэвсравновпере двиднокакбудтосказалонсамсебеипустилсявпередуженеоглядываясьмягкимредкимвольнымнореши тельнымскокомулюлюнесвоимголосомзакричалниколайисамасобоюстремглавпонесласьегодобраяло шадьподгоруперескакиваячерезводомоинывпоперечьволкуещебыстреобогнавеепонеслись собакини колайнеслыхалсвоегокриканечувствовалтогочтоонскачетневидалнисобакниместапокоторомуонск ачетонвиделтольковолкакоторыйусиливсвойбегскакалнепеременяянаправленияполощинеперваяпока залась вблизизверячернопегаяширокозадаямилкаисталаприближатьсякзверюближеближевотонапр испелакнемуноволкчутьпокосилсянанееивместотогочтобынаддатькаконаэтовсегдаделаламилкавд ругоднявхвостсталаупиратьсянапередниеногиулюлюлюкричалниколайкрасныйлюбимвыскочилиз замилкистремительнобросилсянаволкаисхватилегозагачиляжкизаднихногновтуюсекундуиспуганно перескочилнадругуюсторонуволкприселщелкнулзубамиопятьподнялсяипоскакалвпередпровожаем ыйнааршинрасстоянияевсемисобакаминеприближавшимисякнемууйдетнетэтоневозможнодумални колайпродолжаякричатьохрипнувшимголосомкарайулюлюкричалонотыскиваяглазамистарогокобел яединственнуюсвоюнадеждукарайизвсехсвоихстарыхсилвытянувшисьсколькомоглядянаволкатяж елоскакалвсторонуотзверянапереземунопобыстротескокаволкаимедленностискокасобакибылов идночторасчеткараябылошибоченниколайуженедалековпередисебявиделтотлесдокоторогодобеж авволкуйдетнаверноевпередипоказалисьсобакиихотникскакавшийпочтинавстречуещебыланадеж данезнакомыйниколаюмуругиймолодойдлинныйкобельчужойсворыстремительноподлетелспередикв

олкуипочтиопрокинулеговолкбыстрокакнельзябылоожидатьотнегоприподнялсяибросилсякмуругом укобелющелкнулзубамиокровавленныйраспоротымбокомкобельпронзительнозавизжавткнулсяголовойвземлюкараюшкаотецплакалниколайстарыйкобельссвоимимотавшимисяналяжкахклокамиблагодаряпроисшедшейостановкеперерезываядорогуволкубылужевпятишагахотнегокакбудтопочувствовавопасностьволкпокосилсянакараяещедальшеспрятавполенохвостмеждуногинаддалскокунотутниколайвиделтолькочточтотосделалосьскараемонмгновенноочутилсянаволкеиснимвместеповалилсякубаремвводомоинукотораябылапереднимитаминутакогданиколайувидалвводомоинекопошащихсясволкомсобакизподкоторыхвиднелась седаяшерстьволкаеговытянувшаясязадняяногаисприжатымиушамииспуганнаяизадыхающаясяголовакарайдержала

Висновки:

В даному лабораторному практикумі ми набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, отримали практичні навички у частотному криптоаналізі та опанували прийоми роботи в модулярній арифметиці.