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.

Значення ключів і індекси відповідності для текстів, що були розшифровані з цими ключами:

Key	I(X)
(928, 839)	0.03901012672979492
(394, 686)	0.040021676995293534
(680, 498)	0.03881726880717218
(401, 715)	0.039422700191152654
(370, 312)	0.05470659825304335

Зашифрований текст:

*фелсэугиселбуйэятеополмхфкплоыющпбвуцакэюйкзыкусявялеюыкуешяэюазыкйюяьзвусяюыпдэжввя тедыюяячтхкзыереявйвтэебуьагзлчедэвюцэеямадюзвюечюцыющыешгфлцхазцччеолмхечнзпвледсдя мвзжевмэбйрбсюряийвюухыешлифвсочлюряийвюухыешгтбютазцчягтьчяяжцэфлпнитсетеуюйвзсд яшевэущенибсчхеюезючеузйьяюпсдямаээыгнзйвиснрижшдуйьюфлийэфазшгкякзшьяяпатбдспвясзги нкэтбыпрбггтбшсййсыдэядемечмяйвжзазлдткхчбчмчйвувтгинкэтбыпйлхьагвцкзьяэькамащлщзмх ыкмчуябллдпволмхечмчкбущтзвцйвнбюяеммччедэядаяэюнвшьюзщащлкэфлпнцьочпмменбюоззеяэяв чусвесехкчюгупвйбухввлэыволмхсьжектьясезвььдснлулшдяюпсюагякбжйуяичявуссеььхвжщтьжсуй сыхсмччесссвемнэсыеюолрщдэисшисерекэьбпэлддыеюрябенбауасызцчрецямеезфразлдагжчюзнйпуп ввеюкусцяэчретлкзтзцаущцоэчуегчрразыепуочссхсзмнзфкузмасызэыечеолрщссрятекщазшыжешьч екбмаедуззэитсефкфкемющээжйэьвррщтьжслеаявежчзлбрблфкдчщдсзсыыцущеюфлеяэюипччкггу техсаагямаэчяввемцщибыекичслвьчблтгинаузэеядюдэпббйььащябазуьхсэвчгээебсныьяплгхслшднзы свнслызенбйдэгэфлпнюяшжвмусвесехкмащлсющрэчретгкэбйцйсыхсфкемуйыгфлхуыкнзшжксмгээеб сьнытгжчюсйвзйюянюьююячеуспвссмеоеочхедэеюфцжедыющээвныпшжаюфнпвевхчфкаеуйгзшглс йэыежеаязвюерекэхуввжвэйяжссйвеьмчфкэьхедэеюфцкыюязсыечвпзлгвюаежзкювесехерглсрьхяэю еюзэбеаяэсевйувюухыешгеющразцччеолмхечнзвчичймсеатьяьччебддятеубфлцсрбрщюяевисувпзшгв юаежзчююячеумиежвемшдвчусмэебрябйвесехкпюмчзуеншжьвдядюсссввчумыепвплящыдхвощкчхсй ежещчссжвдюцыющфстепйцхыедэкяплгхазлдвнухокусызыцнздчузуьхвывпзкчуйцйрясетегльнйвйст ерирчссцяэььсжвдядющашсэбауретещцэщхрхвмчющцалсвчумыесыедшьдямзггээрспвеввьнзмчшж ксдякчдсбдемиваецяэююядчймхуыквщзлбйпцкэиузбвюдэпьфэрщэщхрхвнйпчячкгхеьбфтсличцдмщйв цяэюспвчсемщйвцяэюспвчввуеивхзшгебрщвюцэрякбсыюяхвывдщэщхрхвссверчпмхвхвхвегжчрчдэпвэя щаензэтьссувнзшупвзйазэяхвывувпвевшврбюятехльанйижректижуеивяькбгзблвюжгебткязрящаен квткелофчельсвузфнфлшпкякбсыеюаыедшьузьярякбуяевйвэясчищзэнгитьюдэтежвемсейвчясемзцчв есехерщфлюзщащлпсдбауячедемяиоьусшьоьпвевшвчебдувнэеюгщэщхрхвмчльсвфэьтсефкюкчеочшвх свеььсссьвмвнауслкззэсрюйгяевмчзьятеуйочдэвсмччехчгчхсвяослехехчрщзлсыйвгсмчхньяхвывдщэщ хрхвсеумвеолфрьщцэнзйьлвдсвчрбжавюблнззэиткясерщзлбйпбшзаzетуйячтхзэеяйэщедэхетекбьщм чаяверeывхвывисвззлшдзвьчбдцююяевкщкчехетцччедцющблфнмчььхедэеюжчьстевектзэзлфзюяудз жуныпкэяьввнбюязэшынзэсбсюнаувюпвевхчочдэсыячопдэядемюыячссхвхзфтдынзуйсыаечеечювемп врбвюблшдыузчмщпвоелбоыбйшьтлуймзссччхзюйзэебсыюяевыеисшмшдвнауслудзжунетибмчллыщц энгхекбвюцэпненрбкщээшдкэгчьвшбюясебнпбшпжжцэьбфншьаеыеэюьтыднэнйрбпукюбйпволеюьщ

эщхрчсхвйвдащлдэпббпгьхейлсюбпсьщщьясктнщазлцсуюряезбпвчмтсензтедсыехнпаябслсввчхерет
еонвюдчдэслтгбйряеввяевхкыыйвцупвшелеезфтщжреьдьзюяемукпвчесехенсдямзмечемщзэцсуоазйь
агзлкщкчехетцччеячяvемййряоьхвчсуммващжчфтгчдчакэбцймзбпдэьдрьшсусшдучхвуспвяюпсцютб
нзазпныцчеэнзэблчешчрчбдмнюяевнлазыеььуйклауесйвагйвиснрпаяьщзьщчюпцкэссьмкяпвьдокнлхупв
яютжллыщяьяяпэижьйябшьрсоенбижчедчячнрижхвчснзисилмзяьаешвячиязбцххвускэюяувхсйбашбл
ждкззбвсэцкэосмчпцкэссогющкразгупвнрипэюебоепцкэссьмпуеннзкювцслтефьунюнуясетеанкэтбф
цнздэядшбающайвмгеюющждджгйвисдямзьярщрчфтьюдэпьэямарыкэеюжйсыедшьдяхьакивэянгющр
чмчредэядрчрехвочщщщзебдэпбщзыкчзщецдьчрчнрипхуоежяуйазччййпбптьнсвймячтхслпвяютбээ
жчжлыцыцыеевяххуухябчюьсщненлендщзблфрьщмюфлвеввтецщгчуеивсцйыкряевхкйьрчллкябахуя
ютбшврежзьясечеввумхчтефьунрясеулзбзыыпдэжчгдпзыпйбашюйцэпнцеатыдпзбпхуоечсдэйвдэык
делеезфнйбашчедэпбщзыерглсткхнчюлгбличжчоелесеияебмаьдшьйтпбяьпцкэссьмопывичхвыехнпуе
нуяблпуггблчеэьсьсконыпяюкчрешжксюерефещщпсуммващжчфтфкузуйыешнинйвдчыеэющзмсхуок
ллаузчречеячйзаэпчнлоыыпюящаазыеплрявчхсжешьяьевпзбпнрпаяьйсудпвдчйлвсочлюкщжчечкненкэ
тбсыюящайвхсньедемиьоеияеюцдшьскусучхвусччййпбюьдэхесюьсзмчятенйкщзлюйтгсыедокжвузца
пбщзьявесехкюешхблрчхщкрвюльвьтгнзнйыддыжглсйэыеебьячеаеьчссрщецухввмглсйэыерейваыеют
бзчучкбээсчхсйечеячяваеюясехеюзеюкщыемхмеыефкаеютазпссуслрямсюяевыеисаезмчеывдсйбашсл
ифжисефкдяевлснюдчоедатбющчюьчаявемнггкэвсткуевемнфллвтчнэщащлвьезьяевзмосжвыежзкз
гзьяевзмосжвыежзггющусжсжвйчььеечесевяхвывчыйвюэпэфлпнщевэжгшпуюебйэмарщкзблгуьщья
цдзввяуяюйвнауслпвдэьяждсюкзеюпварарывьсхвчыйвгсщайвздзяндчочшьпвевумрсумщзфтшьисячд
ярбюяблнзуяуйазоыячнзцессагээхеусумфтуйкэювхетклаибждыецяевхскэгчьвдяуйазкляаыдзмсеьчвв
юкцелеоьфеумвьрсочлээыьдснлйчшмшддчочкненнззчмщцэьяхвывчыйвгцкэбажймхэсмчягтбюненмч
дсисемшдьйзлфлеювекзфнфлсроыячпвйлэщеювннйгчлцбйчэфлмюоржгкэбйагйвьсжвчыйвюэенсеьзю
ямхнзпувлэфщряевемевтэнзвехульыызпжатсеюкчщкзблыпзбзыыпйвмщсюущзчвярыеютбблдчочеупв
зтуйзыющцэбапбщзецтбфркчмщцэквпввемчсехввежвхвжэщзыгкязэпненпвочвзкяцссувюпбюсаячсла
ибждыеягбйхзклблкяпессичжчвненсюзэеяевхскэспусцвдэйвдэылфрьщсэгязтпбпарччвдчоеяьщчыкмч
хщуььэенсыбйфлющэвчекяхвемчекяхвемчегэтбблйбашисдсюеуеюврчзтсевектбльясэенвнтбтбытеяу
йазггпсвнзэеяхвываеыеэютбетсюыдчеаквьгнысоедэвюыдевивтчднгзюйрщссхввесеечвзсюеюдчэбдыс
лысткалцэенусявблсейсоехкляуйазмчоеретелсэьолфцвюэяыейвмщвювюьсиядюзслейюгульычреаячещ
юкюкзцчсзмафлэчщюецблцэжчгынзэслепзенаесскыфлеюыглсолкрслшднйфльвчейбгублшдивлсшьпвт
ктеоехззэьнхсрбфршгеваеигьдюепведоецявергеюзлюыйвцуцакюдэебээюьакгнуяхсэвьйкэжчмгебрщуе
фепюввумчеичжчюкхнвсмчфжявэщебювлютьтчевивтчдньюолрщывувуйуеивогюякшвдярыфлюяче
теоныгющкзыкпюивйсдэбпхефщкзблгяевеглсуерщщзбльяпничбюжйкбуйуеивхвусолщрыефкаехвлупб
чюзлкяывхстехыфлюяоынзэспявчюеуеечпзжйчещюкюкзцчмнкэтбкчолмхблжглсызенбйрепвчетеону
щкчехетцчмхазшгтбвнслщвклхлйнслыспуывцявцреаеуеююгяоьлвчыфлюяввссаксеивйсдэбпсербнзюсв
чумыесекнипреаечщкзблннауслюяфзггфлбдлюряылряткледсхссуслрямсуюютслврчвеягфлшглсолкрв
юьсзммчвнфлпнюяьнгзхйфльвйбашцчредэжчгдпзыппарщблкяптсеректцчйвиаблкяфзьщгчдэмсющпв
феумшвсбчючюшвшеуеечпзсытбзтюяевувущслйэеяэщтьдвзтьяемдэмсчемчольямюоеумчерчрьусюе
йбашмсрбтисеияевмащлюякшзцьшжшжхвпмрщкзбляеивнэюынзьяхсжвхсзмичжчхсжвхсзмыещау
ьвведхсзмдчочзюмщпцшьхспвдзклшдчэщажгйвисемяютбяьбнкэтбыпывфьевдяайфлющыпвеечумйба
шсеьчыуоеязклпуюйээсюцятеоптьтчевивтчднпеанхкрчвсоедэслуччеемпвывэнлсхзклдчочпзенщазлзн
кэтббпткдэыгблывжгкряьйбашыузбсышьхсибнзблевивтчднгзьяевзмосжвыежзьярчюсдэслчевзнйзэ
счдыйвгсдчочаяюекбзлщзкздыеюзбзыхвоисеьвдэщакюзчьупьщынзюйдзеюазыербжахсюсдязненсьяэе
юкэтеюгебрщссусзвусусфкхсуввоцчжэгящаенгьшжшжхвпмрщкзблцыйвнеллмзклшдщззгйвтеьюкщс
лусемяьвесехкпюннзэкювюьсусшдллауюйкяюекбзлпвйбашмсчевздюшвжнмьхвикжврчььягебрщпвзбз
ыиждэтбнзпаебдыпуенлсьваемэеннйреаеуемтсеисвзщащлитсенэюяаетеввжзцьччьэсвчумыербюя
блюяюмчрепвтьзьтгюяхвхвлюлгуязсцящаенчепврбвюрчссйнйбашзыйвгсдчочзюгяхвхвхспужгкрчсщз
слчющехямахьисввхстеоненкэтббпгдянжгебчюслсюыдзмзсбсвявевекгющвненсюслрчгчвсщнсеияюйы
пжгкртчюнкэтбыпнзкясеулпуаеизпчуеивчсисаышьхскятбжвнркяеяюятевгнзряхсзмнюфляьусюеыел
лфрьщоптеонрбжедэкзеюблечдззлеювехввафлфзыпювфергеюебшьдятехлщаьяоьтыфлеююнуеивхву

*севяхуйрывеичжчжвхсжвэянгхкдзклйвмщтьрещсюеезьючерчыеуцтедэбйвнхкдядюжгкряьгэмхуйщз аэесфгхезстечеаеюзыпжгкрчсмбчюбйчелеассзггувабьявчьдпзеюгявеэсувющпвзбзыыдкбээждректы дсюшддэыдчемчольянгжгфлзгкэбйуяюйбйцйряоьфщшгхерчфгхеечювлюфлнюолрщывректнйябьядэы гблкяпнуясктбзрссхвтгинаусльябаибыдчеччйзчюшвшеюгкэклфрьщещкзблтзьщхспзыпагщзэчьнбйит вейюслэямюичжчтякщзлввссувечгрггчсчярщжйсюдэжчлвпзжйсюфлюяюйщзьщьбьяыккгкэыкшлиф бйклхлхлчьшжшжьбфтслнзвефщцешьисввчыйвбвкыувывычреяюебхзклюйфлссххьбфншьаеуыхендзм чевзйэжйпбггссвесзоыйвбврбфлсюфлхвсепцкэссчсфненфкмчущюясесюыдвннзкььчпзсыпсагзыкзыере йбашьщслфзопьсцбауретехеюеаяеюдчнуаеферглсресенлазыечзоыйвбвущпбблчеююслсюьсвяайинхкю аинюйсьхереочлспвтгнзряшдывректнйюыйвыненпвхвывпзбпдэядаеллэщкюыдзмкяевйвэяюьакгныпт куюзэмюдчочмчуеюврчссьняюкчььчеаеьчссозюяуйазуььчмчфкаензтеечмщчеяьдэюйыввненсюслтеон цеьуьяьнкящюецдэтбнзевяхшгебряхвчсжвхсуюебшатбндезфнщзеюфлогфрзляьдэюйысссющщзпцкэс схзшгебвцжвзсрчрессвеувэбюясещййхльвчвясеулпвяюкчейрявчцхкщыдуюебегжглсплгхазяжжехщсла зяжрепвчеуююнюйреаеуеисуюряезфцуйуящаенчербжахсьчссьехщслазяжсюгуткччсстыфлюяеюоеху ювэслектьюдэтежврэитсеуегчррслюямююякбеюмееупвотсетедэхегчфкхсрбжащлпчюеаеоквссввчх кряевхкчюфлчснзызслчэсынзэсебауксхсзмпвщюряевфтсефщазжаущсэйвисхсфтсечэнзжаущеяэьэса езммчплоыжгфлютыемезюшдяьяяьнгзльпвяютждэтбнзмхввйугчьднзячуврэгязтябаухсьзфцрбрщче аеьчссдесемненкяхввеиясехеыкчеечасьугчймфненнзсьячвэйвисемдынзьщйхввьйазульябеатыдссуймчв нфлпнтбаунзщайвцвдязнфеньыйфлбатжкэбйчэщакюфлнющрзлпвмчрензюехсдяэявчвякбьяезжйкяею рямлсюжйдьцяэюбйвнкэтбжйюеедхяулящсюусишскйсумыеретеузазлдывисшдучрекэссчэцхыерглсэс ыкшьчэкэмарясецэретелсаеыасыуяячувемнэющедочбдызпжчэкэкюзлфнфтсейбвцвчщдрбюяцэбебис есзтбьщжасыьяячувттсефкпвочбдткрчпйзэеббпфтсефкхвйвчзоыувывпщэщхрчсвесехкпюнзкэоьввь йкэлсэюрчнсдяйчььочжэтещцжваныпкытбаескшддыйвуюнэтгфльвзвыгтбыксзггьдьчпзжйжарячев ечзжйыуллэщбйинкщкюслхедэеюжгкряьрчуецящюцйсбрщчсусльивуспвоейсыетккгющдчоеусеюйвфя пуюкскмнйвуйбрггяьудзжунфтаэмюкщмчнрдыюяоссуенуяевпврбвюнзээмчсьячюисеревтьяемэщцйсл хедэеюетсефкдэпсаемчсьячшймчцядыввсюхвжэмцщзвюыпмчтецяуймчвтьяемавуявчрлифкщфлпце юсбвеыефкдэхеьйазюдзмочумхвхсгчретещайвьчссцэфлпнщедсфбауфкпхпуссывкбвюцэийзэебсыеюф лхвфеумхчмзйхзлпжльсваепзггьддвэяэьбсббазцчсыедокжвэяфзслчюпсжгйэфзггйвтетглсолкрсюыдз мййслопьсюевэазхвзупьвекынзцезюаыедшьаеэдемпврбвюпсьюкщслчэжгжгуяскпзбйыгфлозвюдэжчд ьхзуйпайхслитсесемчюисемчюеьчсапэнгющцйслхедэеюцдьчаеыуокявзненыуокявээччаегчоглсуегчрра зыссеречэщащлющфлрецхкщзчюенйуегчррблюямюзлфтшпхчряьвдэсчцэенрбюясеечгрцйцахуплряхве чиеызюйазеюкзлдхедэеюмчгчлсдятенйллауюйкябймчссшисербющфлюваезмферчряьнгзоктеонечювл юичжчдсичжчрбцышьрэххзлтбпэисшьвесейвшащлкззчреоехебчнэщащлдэпббпуюебеядчоеяянсыещс зззчячпзжйьбыяежвскюаожлеюеыайхслмчсехетлсющеччисвзцьечощазыкттсесстэнзчюкщцэдыт бюясежзрщщрцеллмзклшдпвуеиввессрчювхсдэядхсмчисудтеонмсссччремччесссвэяевхктнпбшпывгч йзьюреаепьжевнслсюьчрэпчеьфкдчщщцэщесквнсюыдплпццозлхвхсуспвыввзыцедшнмцклхлхлхржгкэб йкэсечклсжврыпалгхеретелсшбюясецящаенкщхедзьюьчрчцнюйсювнитблщзьясехеаспььсхвйвргитря сляютжедшнесцяевузьясехеаспььскярчянюйкэшьхцтедэбйпввесехейюкязлсюыпаечсхчщязсфьвнзэфз шгуяхвемретелсдяюйдчечссвеувпюселбуйзнентеончещююыслшдхзуйпехщзлюдзмкэрчзвцщтьыюшдг сюснзбйлдтеонмспйазбльябезюмщхедзкльюкщвюуочюебядезнзфнсыввмчисввпзпчнйччаегччвнцчлла ууьдэжчшлазыказкздыпсолдыхвчетехезсбнпцкэссяьреаепьюяевыеисдямзауьщблсюичжчьицяйвжзе юичжчщюкщыехвваущсевнауслнззввямавсфьдэблшдягебрщмхазмеллэщкюыдзмгдяннйжчэннйтеум ыксзтбзрцээлфзжйвнинбйклхлозрятенйреаеуезуенлсьвузфнфлшпкяюйьящатждэжчхыувягнзряувзм дыющщайвулфрьщнгюшретьичжчвненсюыдччжчуюющбйпсыкягжгебьтмюфляьцчучфкдэжчмефе дзвюэччемчолкяеящаенщзфнфлшпмчолфцсляюкчреьбфнкзьтьюдэтежврэсыитсензвнетээмчисввузк ящаенссочдэггинкэтббйпеаяхвччсезюкщзлсеумветеоненкэтббпуяблсюяюыпечфяхвхвузшгебуйазюдп врбвюрчссегфлбощзшгебжвегинаусльямюплпупугчьдччйзжгдыыдьсхевеыввваййблхвкяевуврбжахсюв емшдлугчожплгхмахсьчтесепврбкяичувхзуйгзеюфлртаэнгинюяблшдпвмчвсщйрясесеречэщатзьщвве мхввепвнэеюдчфщьщзлслюйблхвцщтьэгющбдищтедэдэслуьнсйвемшдпвичжчвзцчыежсклхлхлхлйнлсь вузфнфлшпьбьяыкяльанйтквнитблпуывусонкякбуйцэзлфзщахейсдямзвюфлхвкяцюзэблдыгуоыетблхх

чсыввзыцыедзеюоьояьнгзлькяфьдвпзжгебрявеэсузьщтьньяясехешьтеонрбкязлучоншыйупаюйысжгй энгющбддяосчевненслягебрщрбеюцхзчюкчзкврръщзйвчясемзлдцяуйкящаенюйщзшглсплгхвюьсусшдхзу ймьиищээмчюисемчтепйцхыельсвузфнфлшпрбющфлювзнлсьвемпцлслзьюьсхыфлюябйхвйвбьшжшжь бфтслнзкэгячсжврыувывусдэпбсыинщазлйчдсаяэюазшьяятеозьщйхльхвйвщсуюдчпятеыцдэпбфцйсл юпэмзьюьсзмвнфлпнбйсыллэщмзвюфлхвцдьчаевненслцясехешькэуюебмзггебебхууйгзжгщагякбкэряв ехвтеонмсочйлазыедэкявехвуеивчсфкаеисвзитсейввтээхвйвшащлфржаитазссвеувбььчмчвврчвеягеб рщкямадюкщзлсемлряоевесехереоеечювююфляьищээпвгчйзкчягебрщтгинауслкяеящаеныспцкэссжях вхвнрипчечэщзвюдэжчдьуомащлкзьщйхввмчызенбйбпссвеуввйибзыипюеаеоеищхспзбпвеечумдькеия техкдэжчусвчумыечейлээзлагебрщфнтеонесчечэжербинщзклдыеюфлвагякбиненмчумндфкаецхкщзэ беездыжглсчевзулшджахейсдязнььтрееьвеечшжучоншыйупаюйысинхежвнлазыкияйвагтбкэжйфе вемнщазлнгхееуцэзлфзгувюпуювгэхзклшдреаетепюшчшлйнпбпжунцевчхгувхвузфнфлшпдэпббпвеечу мчятенйнйкэвюьсусшдпведшнмцэлинюйжауврееввьдрбпсоррщхчдедэкзеютчичжчжчикжвэщтбсыь юфляьфкэььчягйэброымцкэмчрехвваущсечедьцяэюеювюжгьяыедэмюфлогинюяблшдпвхвйвйчучввум хчагьдевягфлазпцтедэочощгзсыщзьщввдявеяьыеоьезфнфлшписячрэфлпнитсечэкэюяячуваезмвнпбзч юегйдзеюазыеитаэблшдпвтеонвсззнйщйрявччежвхсдязнпапбуйююющбйпсшьвесейвшащлггебрщссу севусшьеввефщкзфнфлшпьюкщслююющбйпсмчвечешвшспяэятеонбйуеивчсфгющвесехкцюкщмчувзм дчввуребдэмюфлхвдыеюпэмзьюшвэявуьщбдмзсымсаглсювскускрюйысагзыкзпвосывокяввоыдшдреае жвхвйвищебювув

Ключі:

a = 370, b = 312

Розшифрований текст:

борисзаэтовремясвоейслужбыблагодарязаботаманнымихайловнысобственнымвкусамисвойствамс воегосдержанногохарактерауспелпоставитьсебявсамоевыгодноеположениепослужбеоннаходилсяа дютантомпривесьмаважномлицеимелвесьмаважноепоручениевпруссиюитолькочтовозвратилсяот тудакурьеромонвполнеусвоилсебетупонравившуюсяемувольмюценеписаннуюсубординациюпокотор ойпрапорщикмогстоятьбезсравненияявышегенералаипокоторойдляуспеханаслужбебылинужнынеус илиянаслужбенетрудынехрабростьнепостоянствоанужнобылотолькоуменьеобращатьсястемико торыевознаграждаютзаслужбуиончастосамудивлялсясвоимбыстрымуспехамитомукакдругиемогл инепониматьэтоговследствиеэтогооткрытияеговесьобразжизниеговсеотношенияспрежнимизнак омымивсеегопланынабудущеесовершенноизменилисьонбылнебогатнопоследниесвоиденьгионупотре блялнаточтобыбытьодетымлучшедругихонскореелишилбысебямногихудовольствийчемпозволилбы себеехатьвдурномэкипажеилипоказатьсявстароммундиренаулицахпетербургасближалсяониискалз накомствтолькослюдьмикоторыебыливышеегоипотомумоглибытьемуполезныонлюбилпетербурги презиралмосквувоспоминаниеодомеростовыхиоегодетскойлюбвикнаташебылоемунеприятноионсса могоотездавармиюниразунебылуростовыхвгостинойанныпавловнывкоторойприсутствоватьонсчи талзаважноеповышениепослужбеонтеперьтотчасжепонялсвоюрольипредоставиланнепавловневос пользоватьсятеминтересомкоторыйвнемзаключалсявнимательнонаблюдаякаждоелицоиоцениваяв ыгодыивозможностисближенияскаждымизнихонселнауказанноеемуместовозлекрасивойэленивслу шивалсявобщийразговордядюшканеодобрительноогланулсянапетюинаташуоннелюбилсоединятьба ловствоссерьезнымделомохотыздравствуйтедядюшкаимыедемпрокричалпетяздравствуйтетоздр авствуйтедасобакнепередавитестрогосказалдядюшканиколенькакакаяпрелестнаясобакатрунилао нузналменясказаланаташапросвоюлюбимуюгончуюсобакутрунилавопервыхнесобакаавыжлецподум алниколайистроговзглянулнасеструстараясьейдатьпочувствоватьторасстояниекотороедолжноб ылоихразделятьвэтуминутунаташапонялаэтовыдядюшканедумайтечтобымыпомешаликомунибуд ьсказаланаташамыстанемнасвоемместеинепошевелимсяихорошееделографинечкасказалдядюшка толькослошадитонеупадитеприбавилонаточистоеделомаршиначемдержатьсятоостровотрадне

нскогозаказавиднелсясаженяхвостаидоезжачиеподходиликнемуростоврешивокончательносдядюш
койоткудабросатьгончихиуказавнаташеместогдеейстоятьигденикакничегонемоглопобежатьнапр
авилсявзаезднадоврагомнуплемянничекнаматерогостановишьсясказалдядюшкачурнегладитьпротр
авитькакпридетсяответчалростовкарайфюиткрикнулонотвечаяэтимпризывомнасловадядюшкикар
айбылстарыйиуродливыйбурдастыйкобельизвестныйтемчтоонводиночкубиралматероговолкавсес
талипоместамстарыйграфзнаяохотничьюгорячностьсынапоторопилсянеопоздатьиещенеуспелид
оезжачиеподехатькместукакильяандреичвеселыйрумяныйстрясущимисящекаминасвоихвороненьки
хподкатилпозеленямкоставленномуемулазуирасправившубкуинадевохотничьиснарядывлезнасвоюгл
адкуюсытуюсмирнуюидобруюпоседевшуюкакионвифлянкулошадейсдрожкамиотослалиграфильяан
дреичхотяинеохотникподушенознавшийтвердоохотничьизаконывехалвопушкукустоводкоторыхон
стоялразобралповодьяоправилсянаседлеичувствуясебяготовымоглянулсяулыбаясьподленегостоялег
окамердинерстаринныйноотяжелевшийездоксеменчекмарьчекмарьдержалнасворетрехлихихнотак
жезажиревшихкакхозяинилошадьволкодавовдвесобакиумныестарыеулеглисьбезсворшаговнастопо
дальшевопушкестоялдругойстремянной графамитькаотчаянныйездокистрастныйохотникграфпос
таринной привычкевыпилпередохотойсеребряную чаркуохотничьейзапеканочкизакусилизапилполубу
тылкойсвоеголюбимогобордоильяандреичбылнемножкокрасенотвинаиездыглазаегоподернутыевла
гойособенноблестелиионукутанныйвшубкусидянаседлеимелвидребенкакоторогособралигулятьхудо
йсовтянутымищекамичекмарьустроившисьссвоимиделамипоглядывалнабаринаскоторымонжилле
тдушавдушуипонимаяегоприятноерасположениедухаждалприятногоразговораещетретьелицопод
ехалоосторожновидноужеонобылоученоиззалесаиостановилосьпозадиграфалицоэтобылстариквсе
дойбородевженскомкапотеивысокомколпакеэтобылшутнастасьяивановнанунастасьяивановнапод
мигиваяемушопотомсказалграфтыталькооттопайзверятебеданилозадастясамсусамсказалнастас
ьяивановнашшшшзашикалграфиобратилсяксеменунатальюильиничнувиделспросилонусеменагдеона
ониспетромильичемотжаровыхбурьяновсталиотвечалсеменулыбаясьтожедамыаохотубольшуюи
меютатыудивляешьсясеменкаконаездитасказалграфхотьбымужчиневпорукакнедивитьсясмелолов
коаниколашагденадлядовскимверхомчтольвсшопотомспрашивалграфтакточносужонизнаютгдест
атьтактонкоездузнаютчтомысданилойдругойраздивудаемсяговорилсемензнаячемугодитьбаринух
орошоездитаанаконетокаковакартинуписатькакнамеднисьиззаварзинскихбурьяновпомкнулилисуон
иперескакиватьсталиотуймищастрастьлошадьтысячарублейаседокуценынетдаужтакогомолодц
апоискатьпоискатьповторилграфвидимосожалеячтоокончиласьтакскороречьсеменапоискатьсказа
лонотворачиваяполышубкиидоставаятабакеркунамедникакотобеднивовсейрегалиивышлитакмиха
илтосидорычсеменнедоговорилуслыхавясноразда вавшийсявтихомвоздухегонсподвываниемнеболеед
вухилитрехгончихоннаклонивголовуприслушалсяимолчапогрозилсябаринунавыводокнатеклипрошеп
талонпрямоналядовскойповелиграфзабывстеретьулыбкуслицасмотрелпередсобойвдальпоперемычк
еиненюхаядержалврукетабакеркувследзалаемсобакпослышалсяголосповолкуподанныйвбасистыйро
гданилыстаяприсоединиласькпервымтремсобакамислышнобылокакзаревелисзаливомголосагончихс
темособеннымподвываниемкотороеслужилопризнакомгонаповолкудоезжачиеуженепорскалиаулюл
юкалииззавсехголосоввыступалголосданилытобасистыйтопронзительнотонкийголосданилыказал
осьнаполнялвесьлесвыходилиззалесаизвучалдалековполеприслушавшисьнесколькосекундмолчаграфие
гостремянной убедились ьчтогончиеразбилисьнадвестаиоднабольшаяревевшаяособенногорячосталау
даляться ядругаячастьстаипонеслась вдольполесумимографаиприэтойстаебылослышноулюлюканьед
анилыобаэтигонасливалисьпереливалисьнообаудалялисьсеменвздохнулинагнулсячтобоправитьсворк
увкоторойзапуталсямолодойкобельграфтожевздохнулизаметиввсвоейрукетабакеркуоткрылееидо
сталщепотьназадкрикнулсеменнакобелякоторыйвыступилзаопушкуграфвздрогнулиуронилтабакер
кунастасьяивановнаслезисталподниматьееграфисеменсмотрелинанеговдругакакэточастобываетзв
укгонамгновенноприблизилсякакбудтовотвотпереднимисамимибылилающиертысобакиулюлюканье
данилыграфоглянулсяинаправоувидалмитькукоторыйвыкатывавшимисяглазамисмотрелнаграфаип
однявшапкууказывалемувпереднадругуюсторонуберегизакричалонтакимголосомчтовиднобылочтоэ
тословодавноужемучительнопросилосьунегонаружуипоскакалвыпустивсобакпонаправлениюкграф

уграфисеменвыскакалиизопушкиналевоотсебяувидаливолкакоторыймягкопереваливаясьтихимскок
омподскакиваллевееихктойсамойопушкеукоторойонистоялизлобныесобакивизгнулиисорвавшисьсос
ворпонеслиськволкумимоноглошадейволкприостановилбегнеловкокакбольнойжабойповернулсвоюло
бастуюголовуксобакамитакжемягкопереваливаясьпрыгнулраздругойимотнувполеномхвостомскры
лсявопушкувтужеминутуизпротивоположнойопушкисревомпохожимнаплачрастерянновыскочилао
днадругаятретьягончаяивсястаяпонеслась пополюпотомусамомуместугдепролезпробежалволквсле
дзагончимирасступилиськустыорешникаипоказалась буряяпочерневшаяотпотулошадьданилынадли
ннойспинеекомочкомвалясьвпередсиделданилабезшапкисседымивстрепаннымиволосаминадкрасны
мпотнымлицомулюлюлюулюлюкричалонкогдаонувидалграфавглазахегосверкнуламолнияжкрикнулон
грозясьподнятымарапникомнаграфапроливолкатоохотникиикакбынеудостоиваясконфуженногоис
пуганногографадальнейшимразговоромонсовсейзлобойприготовленнойнаграфаударилповвалившимс
ямокрымбокамбурогомеринаипонесся загончимиграфкакнаказанныйстоялоглядываясьистараясьулы
бкойвызватьвсеменесожалениексвоемуположениюносеменауженебылоонвобездпокустамзаскакива
лволкаотзасекисдвухсторонтакжеперескакивализверяборзятникиноволкпошелкустамииниодинохо
тникнеперехватилегониколайростовмеждутемстоялнасвоемместеожидаязверяпоприближениюио
тдалениюгонапозвукамголосовизвестныхемусобакпоприближениюотдалениювозвышениюголосов
доезжачихончувствовалточтосовершалосьвостровеонзналчтовостровебылиприбылыемолодыеима
терыестарыеволкионзналчтогончиеразбилисьнадвестаичтогденибудьтравилиичточтонибудьслуч
илосьнеблагополучноеонвсякуюсекундунасвоюсторонуждалзверяонделалтысячиразличныхпредполо
женийотомкакискакойстороныпобежитзверьикаконбудеттравитьегонадеждасменялась отчаяни
емнесколькоразонобращалсякбогусмольбоюотомчтобыволквышелнанегоонмолилсястемстрастны
мисовестливымчувствомскоторыммолятсялюдивминутысильноговолнениязависящегоотничтожн
ойпричинынучтотебестоитговорилонбогусделатьэтодляменязнаючтотывеликичтогрехтебяпроси
тьобэтомнорадибогасделайчтобынаменявылезматерыйичтобыкарайнаглазахдядюшкикоторыйво
ноттудасмотритвлепилсяемумертвойхваткойвгорлотысячуразвэтиполчасаупорнымнапряженны
мибеспокойнымвзглядомокидывалростовопушкулесовсдвумяредкимидубаминадосиновымподседоми
оврагсизмытымкраемишапкудядюшкичутьвидневшегосяиззакустанаправонетнебудетэтогосчаст
ьядумалростовачтобыстоилонебудетмневсегдаивкартахинавойневовсемнесчастьеаустерлицидоло
ховярконобыстросменяясьмелькаливеговоображенииитолькоодинразбывжизнизатравитьматерого
волкабольшеянежелаюдумалоннапрягаяслухизрениеоглядываясьналевоиопятьнаправоиприслушивая
ськмалейшимоттенкамзвуковгонаонвзглянулопятьнаправоиувидалчтопопустынномуполюнавстреч
укнемубежалочтотонетэтонеможетбытьподумалростовтяжеловздыхаякаквздыхаетчеловекпри
совершениитогочтобылодолгоожидаемоимсовершилосьвеличайшеесчастьеитакпростобезшумабе
зблескабезознаменованияростовневерилсвоимглазамисомнениеэтопродолжалосьболеесекундыволкб
ежалвпередиперепрыгнултяжелорытвинукоторуюбыланаегодорогеэтобылстарыйзверьсседоюспин
ойиснаеденнымкрасноватымбрюхомонбежалнетороплivоочевидноубежденныйчтониктоневидите
горостовнедышаоглянулсянасобаконилежалистоялиневидяволкаиничегонепонимаястарыйкарайзав
ернувголовуиоскаливжелтыезубысердитоотыскиваяблохущелкалиминазаднихляжкахулюлюшопо
томоттопыриваягубыпроговорилростовсобакидрогнувжелезкамивскочилинасторожившикарайп
очесалсвоюляжкуивсталнасторожившиислегкамотнулхвостомнакоторомвиселивойлокишерстип
ускатьнепускатьговорилсамсебениколайвтовремякакволкподвигалсякнемуотделяясьотлесавдругвс
яфизиономияволкаизменилась онвздрогнулувидавещевероятноникогданевиданныеимчеловеческиегла
заустремленныенанегоислегкаповоротивкохотникуголовуостановилсяназадиливпередэвсравновпере
двиднокакбудтосказалонсамсебеипустилсявпередуженеоглядываясьмягкимредкимвольнымнореши
тельнымскокомулюлюнесвоимголосомзакричалниколайисамасобоюстремглавпонесласьегодобраяло
шадьподгоруперескакиваячерезводомоиныв поперечьволкуещебыстреообогнавеепонеслись собакини
колайнеслыхалсвоегокриканечувствовалтогочтоонскачетневидалнисобакниместапокоторомуонск
ачетонвиделтольковолкакоторыйусиливсвойбегскакалнепеременяянаправленияполощинеперваяпока
залась вблизизверячернопегаяширокозадаямилкаисталаприближатьсякзверюближеближевотонапр

испелакнемуноволкчутьпокосилсянанееивместотогочтобынаддатькаконаэтовсегдаделаламилкавд ругподнявхвостсталаупиратьсянапередниеногиулюлюлюкричалниколайкрасныйлюбимвыскочилиз замилкистремительнобросилсянаволкаисхватилегозагачиляжкизаднихногновтужсекундуиспуганно перескочилнадругуюсторонуволкприселщелкнулзубамиионятьподнялсяипоскакалвпередпровожаем ыйнааршинрасстояниявсемисобакаминеприближавшимисякнемууйдетнетэтоневозможнодумални колайпродолжаякричатьохрипнувшимголосомкарайулюлюкричалонотыскиваяглазамистарогокобел яединственнуюсвоюнадеждукарайизвсехсвоихстарыхсилвытянувшисьсколькомогглядянаволкатяж елоскакалвсторонуотзверянапереземунопобыстротескокаволкаимедленностискокасобакибылов идночторасчеткараябылошибоченниколайуженедалековпередисебявиделтотлесдокоторогодобеж авволкуйдетнаверноевпередипоказалисьсобакииохотникскакавшийпочтинавстречуещебыланадеж данезнакомыйниколаюмуругиймолодойдлинныйкобельчужойсворыстремительноподлетелспередикв олкуипочтиопрокинулеговолкбыстрокакнельзябылоожидатьотнегоприподнялсяибросилсякмургом укобелющелкнулзубамиокровавленныйсраспоротымбокомкобельпронзительнозавизжавткнулсягол овойвземлюкараюшкаотецплакалниколайстарыйкобельссвоимимотавшимисяналяжкахклокамиблаг одаряпроисшедшейостановкеперерезываядорогуволкубылужевпятишагахотнегокакбудтопочувств овавопасностьволкпокосилсянакараяещедальшеспрятавполенохвостмеждуногинаддалскокунотут николайвиделтолькочточтотосделалосьскараемонмгновенноочутилсянаволкеиснимвместеповалил сякубаремводомоинукотораябылапереднимитаминутакогданиколайувидалводомоинекопошащихс ясволкомсобакизподкоторыхвиднелась седаяшерстьволкаеговытянувшаясязадняяногаисприжатым иушамииспуганнаяизадыхающаясяголовакарайдержала

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.