



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

## **КРИПТОГРАФІЯ**

### **КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3**

#### **Криптоаналіз афінної біграмної підстановки**

Перевірили Виконав:

студент 3 курсу ФТІ

групи ФБ-91

Подус Олексій

Викладач:

Завадська Л.О

Савчук М.М.

Чорний О.М

КИЇВ 2021

**Мета:** Набуття навичок частотного аналізу на прикладі розкриття моноalfавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

### **Постановка задачі:**

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

### **Варіант 16**

#### **Хід роботи:**

Були спочатку написані функції: розширений алгоритм Евкліда, обчислення оберненого елемента за модулем, розв'язок лінійного рівняння. Потім було зроблено розбиття тексту на біграми, пошук частот літер та біграм і знаходження найчастіших біграм в тексті. Були написані допоміжні функції для знаходження потенційних ключів та функція знаходження самого ключа.

#### **Найчастіші біграми шифртексту:**

```
5 Most popular bigrams in text ['се', 'ве', 'хв', 'дэ', 'че']
```

#### **Розпізнавач російської мови:**

Перевіряємо, чи найчастіші букви, які зустрічаються у тексті «о», «а», «е», та серед п'яти біграм, які найчастіше зустрічаються у тексті, є хоча б три з цього переліку «то», «на», «но», «ко», «от».

## Шифрованный текст:

фелсэугиселбуйэатеополмхфкплоынощпбвуцакэюйкзыкусявялеюыкуешяэюазык  
йноязвусяюыпдэжввятедыюячтхкзыеревйвтэебуагзлчедэвюцэеамадюзвюеч  
юцыющыешгфлцхазцччеолмхечнзпвледсямвзжевмэбйрбсюраййвюухыешлифв  
сочлюраййвюухыешгтбютазцчягтьчяяжцэфлпнитсетеуойвзсдяшевэушенибсчхе  
юезючеузийьяюпсдямаэыгнзийвиснрижшдуйьюфлийэфазшгкякзшьяпатбдспвясз  
гинкэтбыпрбггтбшсйсыдэядемечмайвжзалдткхчбчмчйвувтгинкэтбыпйлхьягвц  
кзьяэькамащлцзмхыкмчуябллдповолмхечмчкбуцтзвцйвнбюаеммччедэдаяэюнв  
шьюзщащлкэфлпнцочпмменбюозэеяэявчусвесехкчюгупвийбухввлэыволмхсьже  
ктьясезвьдснлулшдяюпсюагакбжйуаичявуссеьхвжщтьжсуйсыхсмччесссвемнэ  
сыеюолрщдэисшисерекэбпэлддыенорябенбауасызцчрецямеезфразлдагжчюзнийп  
упввеюкусцяэчретлкзтзцаушцозчуегчрразыепуочсхсзмнзфкузмасызэыечеолрщ  
ссрятекшазшыжешьчекбмаедуззэитсефкфкемющээжйэвррщтьжслеаявежчзлбр  
блфкдчшдсзсыыцущеюфлеяэюипччкггутехсаагямаэчявемщибыекичслвьчблтги  
наузэеядюдэпббйьящябазуьхсэвчгээбсьныьяплгхслшднзысвнслзыенбйдэгфл  
пнюяшжвмусвесехкмащлсющрэчретгкэбйцийсыхсфкемуйыгфлхуыкнзшжксмгээ  
бсьнытгжчюсийвзийюяннюююячеуспвссмеоеочхедэеюфцжедыющээвныпшжаюфн  
пвевхчфкаеуйгзшглсйэыежеаязвюерекэхуввжвэйяжссийвеьмчфкэьхедэеюфцкыю  
язсыечвпзлгвюаежзкювесехерглсрьхяэюеюзэбеаяэсвийувюухыешгеющразцччео  
лмхечнзвчичиймсеатьяьччебддятеубфлцсрбрщюяевисувпзшгвюаежзчююячеумие  
жвемшдвчусмэебриябйвесехкпюмчзуеншжвьдядюсссввчумыепвплящыдхвошкчх  
сийежешчссжвдюцыющфстепйцхыедэяплгхазлдвнухокусызыцнздчузуюхвывпзк  
чуйцйрасетегльнйвийстерирчссцяэьсжвдядющашсэбауретешцэщхрхвмчюшщал  
свчумыесыедшьдямзггээрспвеввынзмчшжксдякдсбдемиваецяэююядчймхуыкв  
щзлбйпцкэиузбвюдэпфэрщэщхрхвнйпчячкгхьбфтсличцдмщйвцяэюспвчсемщ  
йвцяэюспвчввуеивхзшгебрщвюцэрякбсыюяхвывдщэщхрхвсверчпмхвхвхегжч  
рчдэпвэящаензэтьссувнзшупвзийазэяхвыувувпвевшврбюятехльанийжректижуеивя  
ькбгзблвюжгебтказрящаенквткелофчельсвузфнфлшпкякбсыеюаыедшьузьарякбу  
яевйвэясчищзэнгитыюдэтежвемсейвчясемзцчвесехерщфлюзщащлпсдбауячедемя  
иобусшьоьпвевшвчебдувнэеюгщэщхрхвмчльсвфэйтсефкюкчеочшвхсвеьссьсвм  
внаулкззэсрюйгяевмчсзьятеуйочдэвсмччехчгхсвясослехехчрщзлсыйвгсмчхня  
хвывдщэщхрхвсумвеолфрыщцэнзийльвдсвчрбжавюблнззэиткясерщзлбйпбшзазе  
туйячтхзэеяйэщедэхетекбыщмчаяверевхвывисвзлшдзвьчбдцююяевкщкчехетц  
ччедцющблфнмчьхедэеюжчьстевектзэлфзюяудзжуныпкэяьвнбюязэшынзэсбс  
юнаувиупвевхчочдэсыачопдэдемюбчсххзфтдынзуйсыаечесечюемпврбвюбл  
шдыузчмщпвоелбоыбйшьтлуймзссччхзюйзэебсьюяевыеисшмшдвнауслудзжуне  
тибмчлльщцэнгхекбвюцэппненрбкщээшдкэгчвьшбюясебнпбшпжжцэьбфншьаеые  
эюьтыднэнийрбпукнубйпволеюыщэщхрчсхвйвдащлдэпббпгьхейлсюбпсьщцьяскт

нщазлщсуюряезбпвчмтсензтедсыехнпаябслсввчхеретеонвюдчдэслтгбйряеввяевх  
кыыйвцупвшелеезфтщжреьдзьюемукпвчесехенсдямзмечемщзэцсуоазйьагзлкщ  
кчехетцччечявемйряоьхвчсуммващжчфтггчдчакэбцймзбпдэьдрьшсусшдучхвус  
пвяюпсцютбнзазпныцчеэнзэблчешчрчбдмнюяевнлазысььуйклауесйвагйвиснрпа  
ьящзыщчюпцкэссъмкяпвьдокнлхупвяютжлльщяьяяпэижъйябшьрсоенбижчедчяч  
нрижхвчснзисилмзяьаешвячиязбцххвускэюяувхсйбашблждкззбвсэцкэосмчпцкэс  
согющкразгупвнрипэюебоепцкэссъмпуеннзкювцслтефьунюноуясетеанкэтбфцнзд  
эядшбаушайвмгеюющжджгйвисдямзьярщрчфтьюдэпьэмарыкэеюжйсыедшьдях  
ьакивэянгющрчмчредэдрчрехвочщщцебдэпбщзыкчзщецдьчрчнрипхуоежяуйа  
зччййпбптьнсвиймачтхслпвяютбээжчжлыцыцыеевяххуухябчюьсщненлендщзблф  
рыщмюфлевевтецшгчуеивчсцйыкряевхкйьрчллкабахуяютбшврежзьясечеввумхч  
тефьунрясеулзбыыпдэжчгдпзыпйбашюйцэпнцэатыдпзбпхуоечсдэйвдэыкделеез  
фнйбашчедэпбщзыерглсткхнчюлгбличжчоелесеияебмаьдшьйтпбяьпцкэссъмпы  
вичхвыехнпуенуяблпуггблчезьсьсконыпяюкчрешжксюерефещцпсуммващжчфт  
фкузуйыешнинйвдчыееющзмсхуоклаузчречечайзаэпчнлоыпюящаазыеплявч  
хсжешьяьевпзбпнрпаяйсудпвдчйлвсочлюкщжчечкненкэтбсыюящайвхсньедеми  
ьоеияеюцдшьскусучхвусччййпбюьдэхесюьсзмчатенийкщзлюйтгсыедокжвузцапб  
щзьявесехкюешхблрчхщкрвюльвьтгнзнийддыжглсйэыеебьячаеьчсрщещухвм  
глсйэыерейваыеютбзчучкбээсчхсйечечяваеюясехеюзеюкщьемхмеефкаеютаз  
пссуслрямсюяевыеисаезмчеывдсйбашслифжисефкдяевлснюдчоедатбющчюьчая  
вемннгкэвсткуевемнфллтчнэщащлвьезьяевзмосжвыежзкзгзьяевзмосжвыежзггю  
щусжсжвйчьеечесевяхвывчийвюэпэфлпнщевэжгшпуюебйэмарщкзблгуьщьяцд  
зввяуяюйвнауслпвдэьждсюкзеюпварарывьсхвчийвгсщайвзсдзяндчочшьпвевум  
рsumщзфтшьисячдярбюяблнзуяуйазоыячнзцессагээхеусумфтуйкэювхетклаибжд  
ыецяевхскэгчвьдяуйазкляаьдзмсеьчввюкцелеоьфеумвьрсочлэзэьдснлийчшмшд  
дчочкненннзчмщцэьяхвывчийвгцкэбажймхэсмчягтбюненмчдсисемшдьйзлфлею  
векзфнфлсроыячпвйлэщеюовннийгчлцбйчэфлмюоржгкэбйагйвьсжвчийвюэенсеьз  
юямхнзпупвлэфщряевемевтэнзвехульызпжатсеюкчщкзблыпзбыыпйвмщсюущз  
чвярыеютбблдчочеупвзтуйзыюущцэбапбщзецтбфркчмщцэквпввемчсехввежвхвж  
эщзыгкязэппненпвочвзкяцссувюпбюсаячслаибждыеягбйхзклбкляпессичжчвненс  
юзэеяевхскэспусцвдэйвдэылфрыщсэгязтпбпарччвдчоеящчыкмчхщуьэенсыбйф  
люощэвчекяхвемчекяхвемчегэтбблйбашидсюеуеюврчзтсевектблясэенвнтбтбьт  
еяуйазггпсвнзэеяхвываеыеэютбетсюыдчаеквыгнысоедэвюыдевивтчднгзюйрщс  
хввесеечвзсюеюдчэбдыслысткалцэенусявблсейсоехкляуйазмчоеретелсэолфцв  
юэяыейвмщвювюьсиядюзслейюгульычреаячещюкюкзцчсзмафлэчщюецблцэжчг  
ынзэслепзенаесскыфлеюыглсолкрслшднйфльвчейбгублшдивлсшьпвтктеохззэь  
нхсрбфршгеваеигьдюепведоецявергеюзлюыйвцуцакюдэебээюбакгнухсэвькэж  
чмгебрщуефепюввумчеичжчюкхнвсмчфжявэщобювлютьтчевивтчдньюолрщыву  
вуйуеивогюяакшвдярыфлюячетеоныгюшкззыкпюивйсдэбпхефщкзблгяевеглсуер

щцзбляпничбюжйкбуйуеивхвусолщрыефкаехвлупбчюзлкяывхстехыфлюяоынз  
эспявчюеуеечпзжйчещюкюкзцчмнкэтбкчолмхблжглсызенбйрепвчетеонушкчехе  
тцчмхазшгтбвнслщвклхлйнслыспуывцявцреаеуююгяоьлвчыфлюяввссаксеивйс  
дэбпсербнзюсвчумыесекнипреаечщкзблннауслюяфзггфлбдлюряылряткледсхссу  
слрямсуюютслврчвеягфлшглсолкрвюьсзммчвнфлпнюяьнгзхйфльвйбашцчредэ  
жчгдпзыппарщблкуптсеректцйвиабляфзыщгчдэмсющпвфеумшвсбчючюшвше  
уеечпзсытбзтюяевувущслйэеяэщтьдвзтьямдэмсчемчольямюоеумчерчрьусуюейб  
ашмсрбтисеияевмашлюяакшзцышжшжхвпмрщкзбляеивнэюынзьяхсжвхсзмичжч  
хсжвхсзмыешауьвведхсзмдчочзюмщпцшьхспвдзклшдчэщажгйвисемяютбяьбнкэ  
тбыпывфьевдяйфлющыпвеечумйбашсеьчыуоеязклпуюйээсюцятеоптьтчевивтч  
днпеанхкрчвсоедэслучеемпвывэнлсхзклдчочпзенщаазлзнкэтббпткдэыгблывжгк  
ряьйбашыузбсышьхсибнзблевивтчднгзьяевзмосжвыежзьярчюсдэслчевзньзэсчд  
ыйвгсдчочаяюекбзлщзкздыеюзбзыхвоисеьвдэщакюзчьупыщынзюйдзеюазыербж  
ахсюсдязненсьяэеюкэтеюгебрщссузсвусуфкхсувоцжэгящаенгышжшжхвпмр  
щкзблцыйвнеллмзклшдщзггйвтеьюкцслусемяьвесехкпюннзэкуююьсусшдллаую  
йкяюекбзлпвийбашмсчевздюшвжнмьхвикжврчьягебрщпвзбыиждэтбнзпаебдып  
уенлсьваемэеннйреаеуемтсеисвзщашлитсенэюяаетеввжзцььчьэсвчумыербюябл  
юяюьмчрепвтзьтгюяхвхвлюлгуязсцящаенчепврбвюрчссьнйбашзыйвгсдчочзюг  
яхвхвхспужгкрчсщзслчющехямахыисвхстеоненкэтббпгдянжгебчюслсюыдзмзсб  
сывевекгющвненсюслрчгчвсщнсеияюйыпжгкртчюнкэтбыпнзкясеулпуаеизпчуе  
ивчисаышьхскятбжвнркаяеяюатеьгнзряхсзмнюфляьусуюеыеллфрыщоптеонрбжед  
экзеюблечдззлеювеххвафлфзыповфергеюебшьдятехлщаьяоьтыфлеююнуеивхву  
севяхуирывеичжжвхсжвэянгхкдзклйвмщтьрещсюеезьючерчыеуцтедэбйвнхкдя  
дюжгкряьгэмхуйцзаэесфгхезстечеаеюзыпжгкрчсмбчюбйчелеассзггувабьявчьдп  
зеюгявеэсувоцпвзбыыдкбээждректыдсюшддэйдчемчольянжгфлзгкэбйуаяюйб  
йцйряоьфщшгхерчфгхеечювлюфлнюолрщывректнйябьядэыгбляпнуясктбзрссх  
втгинаусльябаибьдчечйзчюшвшеюгкэклфрыщещкзблтзыщхспзыпагщзэчньбит  
вейюслэямюичжчтякщзлввссувечгрггчсчярщжйсюдэжчлвпзжйсюфлюяойщзыщ  
ьбьяыккгкэыкшлифбйклхлхлчышжшжьбфтслнзвешщещьысввчыйвбвкыувывыч  
реяюебхзклуюфлссххьбфншьаеуыхендзмчевзйэжйпбггссвесзыйвбврбфлсюфлх  
всепцкэссчсфненфкмчущюясесюыдвннзкьчпзсыпсагзыкзыерейбашыщслфзопьс  
цбауретехеюеаяеюдчнуаеферглсресенлазыечзыйвбвушпбблчеююслсюьсваяин  
хкюаинюйсьхереочлспвтгнзряшдывректнйюыйвыненпвхвывпзбпдэядаеллэщкю  
ыдзмкяевйвэяюакгныпткуюзэмюдчочмчуеюврчссьняюкчььчаеьчсозюяуйазуь  
ьчмчфкаензтеечмщчеяьдэюйывненсюслтеонцеуььяьнкящюецдэтбнзевяхшгебр  
яхвчсжвхсуюебшатбндезфнщзеюфлогфрзляьдэюйысссющщзпцкэссхзшгебвцжв  
зсрчрессвеуэбюясещйхльвчвясеулпвяюкчейрявчцхкщыдуюебегжглсплгхазяж  
жехщслазяжрепвчеуююнонйреаеуеисуюряезфцуйуящаенчербжахсьчссьехщслазя  
жсюгуткхчсстыфлюяеуюехуювэслектыдэтежврэйтсеуегчррслюямююякбеюее

упвотсетедэхе г ч ф к х с р б ж а щ л п ч ю е а е о к в с с в в ч х к р я е в х к ч ю ф л ч с н з ы з с л ч э с ы н з э с б  
ауксхсзм п в щ ю р я е в ф т с е ф щ а з ж а у щ с э й в и с х с ф т с е ч э н з ж а у щ е я э э с а е з м м ч п л о ы ж г ф  
люты е мезюш д я я я н г з л ы п в я ю т ж д э т б н з м х в в й у г ч д н з я ч у в р э г з я т б а у х с ь з ф ц р б р  
щ ч а е ь ч с с д е с е м н е н к я х в в е и я с е х е ы к ч е е ч а с ь у г ч й м ф н е н н з с ь я ч в э й в и с е м д ы н з ы щ й х  
в в ь й а з у л ь я б е а т ы д с с у й м ч в н ф л п н т б а у н з ц а й в ц в д я з н ф е н ь ь ф л б а т ж к э б й ч э щ а к ю ф  
л н ю щ р з л п в м ч р е н з ю е х с д я э я в ч в я к б ь я е з ж й к я е ю р я м л с ю ж и д ь ц я э ю б й в н к э т б ж и ю е е  
д х я у л я щ с ю у с ь с к й с у м ы е р е т е у з а з л д ы в и с щ д у ч р е к э с с ч э ц х ы е р г л с э с ы к ш ь ч э к э м а р  
я с е ц э р е т е л с а е ы а с ы у а я ч у в е м н э ю щ е д о ч б д ы з п ж ч э к э к ю з л ф н ф т с е й б в ц в ч щ д р б ю а ц э  
б е б и с е с з т б ы щ ж а с ы ь я ч у в т т с е ф к п в о ч б д т к р ч п и з э е б б п ф т с е ф к х в и в ч з о ы у в ы в п щ э щ  
х р ч с в е с е х к п ю н з к э о ь в в ь к э л с э ю р ч н с д я й ч ь о ч ж э т е щ ц ж в а н ы п к ы т б а е с к ш д д ь в у  
ю н э т г ф л ь в з в ы г т б ы к с з г ь д ь ч п з ж и ж а р я ч е в е ч з ж и ы у л л э щ б й и н к щ к ю с л х е д э ю ж г к р  
я р ч у е щ а щ о ц й с б р щ ч с у с ь л и в у с п в о е й с ы е т к k г ю щ д ч о е у с е ю й в ф я п у о к с к м н и в у й б р  
г г я ь у д з ж у н ф т а м ю к щ м ч н р д ы ю а о с с у е н у я е в п в р б ю н з э м ч с ь я ч ю и с е р е в т ь я е м э щ ц  
й с л х e д э ю е т с e ф к д э п с а e м ч с ь я ч ш и м ч ц я д ы в в с ю х в ж э м ц щ з в ю ы п м ч т e ц я у й м ч в т ь я e  
м а в у я в ч р л и ф к щ ф л п ц e ю с б в e ы e ф к д э х e ь й а з ю д з м o ч у м х в x c г ч р e т e щ а й в ь ч c c ц ф л п n  
щ e d c f б a y f k п x п у c c ы в к б в ю ц э и з э e б c ы e ю ф л x в ф e y m x ч м з и x з л п ж л ь c в a e п з г ь d d в э  
я э ь б c б б a з ц c ы e d o k ж в э я ф з c л ч ю п c ж г i э ф з г t i в t e t г л c o л k p c ю ы d з м i ь c л o п ь c ю e в a z  
x в з y п ь в e k ы н z c e з ю a ы e d ш ь a e э д e m п в p b в ю п c ы ю k щ c л ч э ж г ж г y a c k п з б i ы г ф л o z в ю d э  
ж ч д ь x з y п a й x c л и t c e c e m ч ю и c e m ч ю e ь ч a п э н г ю щ ц i ь c л x e d э ю ц д ь ч a e ы o к я в з н e н ы  
y o к я в э э ч a e г ч o г л c y e г ч p p a z ы c c e p e ч э щ a щ л ю щ ф л p e ц x k щ з ч ю e н i y e г ч p r b л ю я м ю z л  
ф t ш п x ч p я ь в d э c ц э н p б ю я c e e ч r ц i ь a x y п л p x в e ч и e ы з i o y a z e ю k z l d x e d э ю м ч г c л c  
д я т e н i л л a y o i k ь б i m ч c c ш i c e p б ю щ ф л ю в a e z m ф e p ч p я ь n g z o k t e o н e ч ю в л ю и ч ж ч d c и ч  
ж ч p б ц ы ш ь p э x x z l t b п э i c ш ь в e c e i v ш a щ л k z z ч p e o e x e б ч н э щ a щ л d э п b б п y o e б e a d ч o e я  
я н c ы e щ c z z z ч a ч п z ж i ь б ь я ы e ж в c k ю a o ж л e ю e ы a i x c л m ч c e x e t л c ю щ e ч c и c в z ц ь e ч o щ a z  
ы k t t c e c c t э н z ч ю k щ ц э д ы t б ю я c e ж з p щ ц p c e л l m z k l ш d п в y e i v c e c c p ч ю v x c d э a d x c m ч  
и c y d t e o n m c c c c ч p e m ч c e c c c c в я e v x k t n п б ш п ы в г ч i ь з ю p e a e п ь ж e v n c л ю ь ч p э п ч ь e ф k d  
ч щ ц э щ e c k v n c ю ы d п л п ц o z л x v x c y c п ы в v v z ы c e d ш n m ц k л x л x p ж г k э б i k c e c k л c ж  
v p ы п a л г x e p e t e л c ш b ю я c e ц я щ a e n k щ x e d з ь ю ч p ч ц н i o y c ю v n i t б л щ z ь a c e x e a c п ь c x v  
i v p г и t p я c л я ю т ж e d ш n e c ц я e v y з ь a c e x e a c п ь c k я p ч я n i o y k э ш ь x ц t e d э б i p v c e c e x e i y o k  
я z л c ю ы п a e c x ч щ a z c f ь v n z э f z ш г y a x v e m p e t e л c d я ю ы d ч e c c c e u v п o c e л б y i z n e n t e o  
н ч e щ o y o ы c л ш d x з y i п e x щ z л ю d z m k э p ч z v ц щ t ь ы o ш d г c ю c n z б i l d t e o n m c п i a z б л ь a б e  
з ю m щ x e d z k л ь ю k щ v o y o ч ю e б я d e z n z f n c ы v m ч i c c v п z п ч n i ь ч a e г ч ч v n ц л l a u y ь d э  
ж ч ш л a z ы k a z k z d ы c o л d ы x v ч e t e x e z c b n п c k э c c ь p e a e п ь ю e v ы e i c d я m z a y ь щ б л c ю i ч  
ж ч ы i ц i ь i v ж z e o i ч ж ч ц ю k щ ы e x v a u щ c e v n a u c л n z z v v я m a v c f ь d э б л ш d я e б p ц m x a z m  
e л l э щ k ю ы d z m г d я n n i ь ж ч э n n i t e y m ы k c z t b z p c э z л f z ж i v n i n б i k л x л o z p я t e n i ь p e a e y e z  
y e n л c ь v y z f n ф л ш п k я ю ь ь a щ a t ж d э ж ч x ы y v a г n з p y a v z m d ы o щ щ a i y u л ф p ы щ n g ю щ p e t  
ы i ч ж ч v n e n c ю ы d ч ж ч ю ю щ б i п c ы k я г ж e б ь t м ю ф л ь ц ч y c f k d э ж ч m e f e d z v i o э ч e m  
ч o л k я e я щ a e n щ z f n ф л ш п m ч o л ф c л я ю k ч p e ь б f n k з ь t ь ю d э t e ж v p э c ы i t c e n z v n e t э м ч  
и c c v y z k ь a e n c c o c d э г г i n k э t б i ь п e a y x v ч c c e z ю k щ z л c e y m v e t e o n e n k э t б b п y a б л c ю я

юыпечфяхвхвузшгебуйазюдпврбвюрчсsegфлбоцзшгебжвегинаусльямюплпупут  
чъдчйзжгдыдыдсхевеывввайблхвкяевуврбжахсюемшдлугчожплгхмахсъчтесеп  
врбкяичувхзуйгзеюфлртаэнгинюяблшдпмчвсщйрясесеречэщатзыщвемхввепн  
эеюдчфщщзлслюйблхвщцтьэгющбдицтедэдэслуьнсйвемшдпвижчжвзцчыесжкл  
хлхлхлйнлсьвузфнфлшпъбъякьяланйтквнитблпуывусонкякбуйцэзлфзцахейсдя  
мзвюфлхвкяцюзэблдыгуоыетблххчсыввзыцыедзеюоояынгзлькяфьдвпзжгебряве  
эсузыщтьняясехешьтеонрбкязлучоншьйупаюйысжгйэнгющбддяосчевненслягеб  
рщрбеюцхзчюкчзквррщзйвчясемзлджяуйкящаенюйщзшглсплгхвюьсусдхзуймь  
ищээмчюисемчтепйцхыельсвузфнфлшпрбющфлювзнлсьвемпцлслзьюьсхыфлюя  
бйхвйвбышжшжъбфтслнзкэгячсжврыувывусдэпбсынщазлйчдсаяэюазшьятеозь  
щйхлхвйвщсуюдчпятещдэпбфцйслюпэмзьюьсзмвнфлпнбйсыллэщмзвюфлхвц  
дъчаевненслцясехешькэуюебмзггебебхууйгзжгцагякбкэрявехвтеонмсочйлазыед  
экявехвуеивчсфкаеисвзитсейввтээхвйвшащлфржаитазссвеувбъчмчвврчвеягебр  
цкямадюкщзлсемлряоевесехереоеечювоююфляьищээпвгчйзкчягебрщтгинауслкя  
еящаеныспцкэссжяхвхвнрипчечэщзвюдэжчдьуомащлкзыщйхввмчызенбйбпссве  
уввийбзыипюеаеоеищхспзбпвеечумдькеиятехкдэжчусвчумыечейлээзлагебрщфн  
теонесчечэжербинщзклдыеюфлвагякбиненмчумндфкаецхкщзэбеездыжглсчевзу  
лшджахейсдзньтьреььвеечшжучоншьйупаюйысинхежвнлазыкияйвагтбкэжйф  
евемнщазлнгхееуцэзлфзгувюпуювгэхзклшдреаетепюшчшлйнпбпжунцевчхгувхв  
узфнфлшпдэпббпвеечумчятенийнкэвюьсусдпведшнмцэлинойжаувреввьдрбпс  
оррщхчдедэкзеютчичжжжчикжвэщтбсыюфляьфкэьчягйэброымцкэмчрехввау  
щсечедыцяэюеювоюжгьяыедэмюфлогинюяблшдпхвйвйчучввумхчагьдевягфлазп  
цтедэочоцгзсыщзщввдявеляьеоеьезфнфлшписячрэфлпнитсечэкэюячуваезмвн  
пбзчюегйдзеюазыеитаэблшдпвтеонвсззнийщйрявччежвхсдззппабуйююющбйпс  
шьвесейвшащлгтебрщсусевусшьевефцкзфнфлшпьюкщслююющбйпсмчвечеш  
вшспяэатеонбйуеивчсфгющвесехкцюкщмчувзмдчввуребдэмюфлхвдыеюпэмзью  
швэявуыщбдмзсымсаглсювскускрюйысагзыкзпвосывокяввоыдшдреаежвхвйвищ  
ебюув

### Дешифрованный текст:

борисзаэто время своей службы благодаря работаманнымихайловны собственным  
кусамисвойствам своегосдержанного характерауспелпоставитьсебявсамоевыгодн  
оеположениеипослужбеоннаходилсяадютантомпривесьмаважномлицеимелвесъм  
аважноепоручениевпруссииитолькотчтовозвратилсяоттудакурьеромонвполнеусв  
оилсебетупонравившуюсяемувольмюценеписаннуюсубординациюпокоторойпр  
апорщикмогстоятьбезсравнениявышегенералаипокоторойдляуспеханаслужбебы  
линужнынеусилиянаслужбенетрудынехрабростьнепостоянствоанужнобылотоль  
коуменьеобращатьсястемикоторыевознаграждаютзаслужбуиончастосамудивлял  
сясвоимбыстрым успехамитомукакдругиемоглинепониматьэтоговследствиеэтого

открытия его весь образ жизни его все отношения с прежними знакомыми в его планы на будущее совершенно изменились он был небогатно последние свои деньги он употреблял на то чтобы быть детьми лучше других он скорее ели и шил бы себя многих удовольствий чем позволил бы себе ехать в дурном экипаже или показаться в старом мундире на улицах петербурга сближался с ним и искал знакомств только с людьми которые были выше его и потому могли бы быть ему полезны он любил петербург и презирал москву в поминание о домеростовых и его детской любви к наташе было ему неприятно и он с самого отъезда в армию ни разу не был у ростовых в гостиную анны павловны в которой присутствовать он считал заважное повышение по службе он теперь тотчас же понял свою роль и предоставил анне павловне воспользоваться тем интересом который в нем заключался в внимательно наблюдая каждое лицо и оценивая выгоды и возможности сближения с каждым из них он сел на указанное ему место возле красивой элены и слушивался в общий разговор дядюшки не одобрительно оглянувшись на петю и наташу он не любил соединять баловство с серьезным делом охоты и здравствуйте дядюшка и мы едем прокричал петя здравствуйте то здравствуйте да собака не передавит строго сказал дядюшка николенка какая прелестная собака трунила он узнал меня сказала наташа просуюлюбимую гончую собаку трунила во первых не собака а выжлец подумал николай и строга взглянул на сестру стараясь ей дать почувствовать то расстояние которое должно было их разделять в эту минуту наташа поняла это выдядюшка не думайте чтобы мы мешали комунибудь сказала наташа мы станем на своем месте и не пошевелимся их хорошо ее дело графинечка сказал дядюшка только лошади не упадите прибавил он то есть дело марш не наче м держаться то островотраденского заказавиднелся саженях востай до езда жачие не подходили к нему ростовы решили окончательно дядюшкой откуда брать осать гончих и указав наташе место где ей стоять и где никаким образом не могло побегать она пошла и с везе на доврагом ну племянничек наматерогостановишься сказал дядюшка чур не гладить и протравить как придется я отвечал ростовка райфю и крикнул он отвечая этим призывом на слова дядюшки карай был старый и уродливый бурдастый кобель известный тем что он в одиночку бил матерого волка в сестали по местам старый графзная охотничья горячность сына поторопился не опоздать и еще не успел до езда жачи не подехать к месту как илья андреич веселый румяный и трясущими щеками на свои хвороненьких подкатил по зеленым ко ставленному ему лазу и исправив шубку и на де вохотничьи снаряды влез на свою гладкую сытую смирную и добрую по седевшую как и он в флянку лошадей с дрожками и отослал и граф илья андреич хотя и не охотник по душе но знавший твердо охотничьи законы ве хал во пушку кустов от которых он стоял разобрав поводья поправился на седле и чувствуя себя готовым оглянулся улыбаясь подле него стоя ле го ка мердинер старинный но отяжелевший ез док се мен чек марь чек марь держал на своретрехлихих нотах же за жиревших как хозяин и лошадь волко да во двесо баки умные старые улеглись без сворша го на сто по даль ше во пушке стоял другой стрелянной граф амить ка отчаянный ез до ки страстный охотник граф старинной прив



ычкевыпилпередохотойсеребрянуючаркуохотничьейзапеканочкизакусилзапил  
полубутылкойсвоеголюбимогобордоильяандреичбылнемножкокрасенотвинаиез  
дыглазаегоподернутыевлагойособенноблестелионукутанныйвшубкусидянасед  
леимелвидребенкакоторогособралигулятьхудойсовтянутымищекамичекмарьуст  
роившисьсвоимиделамипоглядывалнабаринаскоторымонжиллетдушавдушуип  
онимаяегоприятноерасположениедухаждалприятногоразговораещетретьелицоп  
одехалоосторожновидноужеонобылоученоиззалесайостановилосьпозадиграфал  
ицоэтобылстариквседейбородеженскомкапотевысокомколпакеэтобылшутнас  
тасьяивановнанунастасьяивановнаподмигиваяемушопотомсказалграфтытолькоо  
ттопайзверятебеданилозадастясамсусамсказалнастасьяивановнашшшшзашикалг  
рафиобратилсяксеменунастасьяилиничнувиделспросилонусеменагдеонаониспе  
тромильичемотжаровыхбурьяновсталиотвечалсеменулыбаясьтожедамыаохотуб  
ольшуюимеютатыудивляешьсясеменкаконаездитасказалграфхотьбымужчиневи  
орукакнедивитьсясмельоловкоаниколашагденадлядовскимверхомчтольвсшопото  
мспрашивалграфтакточносужонизнаютгдестатьтактонкоездузнаютчтомысданил  
ойдругойраздивудаемсяговорилсемензнаячемугодитьбаринухорошеездитанако  
нетокаковакартинуписатькакнамеднисьиззаварзинскихбурьяновпомкнулилисуо  
ниперескакиватьсталиотуймищастрасьлошадтысячарублейаседокуценынетдау  
жтакогомолодцапоискатьпоискатьповторилграфвидимосожалеячтокончиласьта  
кскороречьсеменапоискатьсказалонотворачиваяполышубкиидоставаятабакерку  
намедникакотобеднивовсейрегалиивышлитакмихаилтосидорычсеменнедоговор  
илуслыхавяснораздававшийсявтихомвоздухегоисподвываниемнеболеедвухилит  
рехгончихоннаклонивголовуприслушалсяимолчапогрозилисьбаринунавыводокна  
теклипрошепталонпрямоналядовскойповелиграфзабывстеретьулыбкуслицамот  
релпередсобойвдальпоперемычкеиненюхаядержалврукебакеркувследзалаемсо  
бакпослышалсяголосповолкуподанныйвбасистыйрогданилыстаяприсоединилас  
ькпервымтремсобакамислышнобылокакзаревелисзаливомголосагончихстемособ  
еннымподвываниемкотороеслужилопризнакомгонаповолкудоезжачиеуженепор  
скалиаулюлюкалииииззавсехголосоввыступалголосданилытобасистыйтопронзит  
ельнотонкийголосданилыказалосьнаполнялвесьлесвыходилиззалесаизвучалдале  
ковполеприслушавшисьнесколькосекундмолчаграфиегостремяннойубедилисьчт  
огончиеразбилисьнадвестаиоднабольшаяревевшаяособенногорячосталаудалятьс  
ядругаячастьстаипонесласьвдольполесумимографаиприэтойстаебылослышноул  
юлюканьеданилыобаэтигонасливалисьпереливалисьнообаудалялисьсеменвдох  
нулинагнулсячтобоправитьсворкувкоторойзапуталсямолодойкобельграфтожевз  
дохнулизаметиввсвоейрукебакеркуоткрылееидосталщепотьназадкрикнулсеме  
ннакобелякоторыйвыступилзаопушкуграфвздروгнулиуронилтабакеркунастасья  
ивановнаслезисталподниматьееграфисеменсмотрелинанеговдругкакэточастоыв  
аетзвукгонамгновенноприблизилсякакбудтовотвотпереднимисамимибылилающ

иертысобакиулюлюканьеданилыграфоглянулсяинаправоувидалмитькукоторыйв  
ыкатывавшимисяглазамисмотрелнаграфаиподнявшапкууказывалемувпереднадр  
угуюсторонуберегизакричалонтакимголосомчтовиднобылочтоэтословадавноуж  
емуучительнопросилосьунегонаружуипоскакалвыпустивсобакпонаправлениюкгр  
афуграфисеменвыскакалиизопушкииналевоотсебяувидаливолкакоторыймягкопе  
реваливаясьстихимскокомподскакиваллевееихтойсамойопушкеукоторойонисто  
ялизлобныесобакивизгнулиисорвавшисьссосворпонеслиськволкумимоноглошаде  
йволкприостановилбегнеловкокакбольнойжабойповернулсвоюлобастуюголовку  
собакамитажжемягкопереваливаясьпрыгнулраздругоймотнувполеномхвостомс  
крылсявопушкувтужеминутуизпротивоположнойопушкисревомпохожимнаплач  
растерянновыскочилаоднадругаятретьягончаяивсястаяпонесласьпополюпотому  
самомуместугдепролезпробежалволквследзагончимираступилиськустыорешни  
каипоказаласьбураяпочерневшаяотпотулошадьданилынадлиннойспинееекомочк  
омвалясьвпередсиделданилабезшапкиседымивстрепаннымиволосаминадкрасн  
ымпотнымлицомулюлюлюулюлюкричалонкогдаонувидалграфавглазахегосверк  
нуламолияжкрикнулонгрозясьподнятымарапникомнаграфапроливолкатоохотн  
икиикакбынеудостоиваясконфуженногоиспуганногографадажнейшимразгово  
ромсовсейзлойприготовленнойнаграфаударилповвалившимсямокрымбокамбу  
рогомеринаипонессязагончимиграфкакнаказанныйстоялоглядываясьистараясьу  
лыбкойвызыватьвсеменесожалениексвоемуположениюносеменауженебылоонвоб  
ездпокустамзаскакивалволкаотзасекисдвухсторонтакжеперескакивализверяборз  
ятникиноволкпошелкустамииниодинокхотникнеперехватилегониколайростовме  
ждутемстоялнасвоемместеожидаязверяпоприближениюиотдалениюгонапозвука  
мголосовизвестныхемусобакпоприближениюотдалениюивозвышениюголосовдо  
езжачихончувствовалчтосовершалосьвостровеонзналчтовостровебылиприбыл  
ыемолодыеиматерыестарыеволкионзналчтогончиеразбилисьнадвестаичтогдени  
будьтравилиичтоонибудьслучилосьнеблагополучноеонвсякуюсекундуна свою  
сторонуждалзверяонделалтысячиразличныхпредположенийотомкакискакойстор  
оныпобежитзверьякаконбудеттравитьегонадеждасменяласьотчаяниемнесколько  
разонобращалсякбогусмольбоюотомчтобыволквышелнанегоонмолилсятемстра  
стнымисовестливымчувствомскоторыммолятсялюдивминутысильноговолнения  
зависящегоотничтожнойпричинынучтотобестоитговорилонбогусделатьэтодляме  
нязнаючтотывеликичтогрехтебяпроситьобэтомнорадибогасделайчтобынаменяв  
ылезматерыйичтобыкарайнаглазхдядюшкикоторыйвооттудасмотритвлепился  
емумертвойхваткойвгорлотысячуразвэтиполчасаупорнымнапряженнымибеспок  
ойнымвзглядомокидывалростовопушкулесовсдвумяредкимидубаминадосиновы  
мподседомиоврагсизмытымкраемишапкудядюшкичутьвидневшегосяиззакустан  
аправонетнебудетэтогосчастьядумалростовачтобыстоилоннебудетмневсегдаивка  
ртахиनावойнево всемнесчастьеаустерлицидолоховярконобыстросменяясьмелька

ливего воображении только один раз быв жизни за травить матерего волка больше не  
желаю думать на прягая слух и зрение оглядываясь налево и опять направо и прислуш  
иваясь к малейшим оттенкам звуков гона он взглянул опять направо и увидал что по пу  
стынному полю навстречу к нему бежал что тот нет-это не может быть подумал ростов  
желовздыхая как вздыхает человек при совершении того что было долго ожидаемо им  
совершилось величайшее счастье и так просто без шума без блеска без означения  
ростов не верил своим глазам и сомнение это продолжалось более секунды волк бежал  
вперед и перепрыгнул тяжелорытвиную которая была на его дороге это был старый звер  
ь с седой спиной и снаденным красноватым брюхом он бежал неторопливо очевидно  
убежденный что никто не видит его ростов не дыша оглянулся на собаку и лежалая  
лине видя волка и ничего не понимая старый карай завернул голову и оскалил желтые зу  
бы сердито отыскивая блоху щелкали ми на задних ляжках улюлюлюшопотом оттопы  
ривая губы проговорил ростов собака дрогнув железками вскочила на стороживушик  
арай почесал свою ляжку и встал на стороживушии и лег камотнул хвостом на котором  
висели войлоки шерсти пускаться не пускаться говорил сам себе николай в то время как вол  
к подвигался к нему утешаясь от лесавдругся физиономия волка изменилась он вздр  
огнул увидав еще вероятнее ни когда не виданные им человеческие глаза устремленные  
на него и слегка поворотив кохотнику голову остановился назади или впереди в сравнов  
передвижко как будто сказал он сам себе и пустился вперёд уже не оглядываясь мягким  
редким вольным и решительным скоком улюлюнес своим голосом закричал николай  
и самасобой стремглав понеслась его добрая лошадь под горуперескакивая через вод  
о и нырив поперечь волку и еще быстрее обогнав ее понеслись собака и николай не слыша  
своего крика не чувствовал того что он скачет не видал ни собаки ни места по которому  
он скачет он видел только волка который усилил свой бег скакал не переменив направле  
ния по ложине первая показалаась вблизи зверя чернопегая широкозадая милка и стала  
приближаться к зверю ближе ближе вот она приспела к нему волк чуть покосился на  
нее и вместо того чтобы наддаться как она это всегда делала милка вдруг подняв хвост ста  
ла упираться на передние ноги улюлюлюлю кричал николай красный любим выскочи  
ли замили стремительно бросился на волка и схватил его за гачилижки задних ног  
в ту же секунду испуганно перескочил на другую сторону волк присел щелкнул зубами и  
опять поднялся и поскакал вперед провожаемый на аршин расстояния всеми собаками  
не приближавшимися к нему уйдет нет-это невозможно подумал николай продолжая кри  
чать хрипнувшим голосом карай улюлю кричал он отыскивая глазами старого кобеля  
единственную свою надежду карай из всех своих старых сил вытиснувшись с нескольк  
о оглядя на волка тяжело скакал в сторону от зверя наперерез ему по быстрым скакам  
олка и медленности кока собака было видно что расчет карая был ошибочен николай у  
же не далеко вперед себя видел тот лес до которого бежал волк уйдет наверное впе  
ред показали собаки и охотник скакавший почти навстречу еще была надежда не знак  
омый николаю муругий молодой длинный кобель чужой своры стремительно подлет

елспередикволкуипочтипрокинулеговолкбыстрокакнельзябылоожидатьотнего  
приподнялсяибросилсякмуругомукобелющелкнулзубамииокровавленныйсраспо  
ротымбокомкобельпронзительнозавизжавткнулсяголовойвземлюкараюшкаотец  
плакалниколайстарыйкобельссвоимимотавшимисяналяжкахклокамиблагодаряп  
роисшедшейостановкеперерезываядорогуволкубылужеВПЯТИШАХОТНЕГОКАКБУД  
ТОПОЧУВСТВОВАВопасностьволкпокосилсянакараяещедальшеспрятавполенохвост  
междуногинаддалскокунотутниколайвиделтолькочточтоотсделалосьскараемонм  
гновенноочутилсянаволкеиснимвместеповалилсякубаремвводомоинукотораябы  
лапереднимитаминутакогданиколайувидалвводомоинекопошашихсясволкомсоб  
акизподкоторыхвиднеласьседаяшерстьволкаеговытянувшаясязадняяногаисприж  
атымиушамииспуганнаяизадыхающаясяголовакарайдержала

**Ключ:**

**a = 370, b = 312**

**Висновки:** Після виконання цієї роботи я набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанував прийоми роботи в модулярній арифметиці.