



Міністерство освіти і науки України  
Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Фізико-технічний інститут

**ЛАБОРАТОРНА РОБОТА №3**  
**з дисципліни**  
**«Криптографія»**  
**на тему: «Криптоаналіз афінної біграмної підстановки»**

Виконали:  
студенти 3 курсу ФТІ  
групи ФБ-73  
Петренко К.М  
Танчинець А.Є.

Перевірили:  
Чорний О.  
Савчук М. М.  
Завадська Л. О.

## Варіант 16

**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 №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 ( $a, b$ ) знайти можливі кандидати на ключ 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.

### Результати виконання роботи:

#### Найчастіші біграми:

Мови:	ст	но	то	на	ен
Шифртексту:	се	ве	хв	де	че

#### Можливі варіанти ключів:

[('ья', 'ье'), ('нш', 'мз'), ('бв', 'ба'), ('оа', 'не'), ('да', 'че'), ('сш', 'тз'), ('ев', 'ба'), ('та', 'уе'), ('сз', 'ба'), ('нз', 'еа'), ('тй', 'гь'), ('аз', 'ца'), ('юю', 'ыв'), ('щю', 'жв'), ('мц', 'цд'), ('мю', 'чв'), ('са', 'ье'), ('на', 'же'), ('яш', 'цз'), ('тв', 'еа'), ('жа', 'ве'), ('уь', 'шв'), ('эз', 'мэ'), ('ка', 'че'), ('ща', 'се'), ('нб', 'шв'), ('цэ', 'мэ'), ('ле', 'ое'), ('се', 'яе'), ('йв', 'йэ'), ('хе', 'фе'), ('вг', 'йе'), ('иг', 'ще'), ('хю', 'рв'), ('мг', 'пе'), ('ха', 'се'), ('ья', 'ве'), ('йб', 'шв'), ('тэ', 'мэ'), ('га', 'ще'), ('лн', 'шу'), ('то', 'еб'), ('еа', 'фе'), ('эа', 'ще'), ('ин', 'бу'), ('по', 'нб'), ('ва', 'эе'), ('ут', 'ну'), ('цт', 'ху'), ('зб', 'бп'), ('шт', 'ру'), ('мс', 'сб'), ('пс', 'щб'), ('чя', 'шп'), ('сс', 'фб'), ('ья', 'фе'), ('юа', 'эе'), ('жн', 'ыу'), ('но', 'иб'), ('ха', 'ве'), ('бю', 'рв'), ('ое', 'бэ'), ('ка', 'се'), ('лю', 'рв'), ('ше', 'бэ'), ('оа', 'че'), ('юв', 'це'), ('ув', 'зе'), ('мз', 'жэ'), ('вв', 'эе'), ('рв', 'фе'), ('жб', 'ее'), ('тш', 'ув'), ('фь', 'ье'), ('ья', 'се'), ('са', 'ве'), ('эю', 'рв'), ('ке', 'бэ'), ('па', 'ше'), ('гг', 'ыш'), ('ки', 'сс'), ('ща', 'ие'), ('ра', 'ье'), ('уг', 'еш'), ('ыи', 'ьс'), ('ыэ', 'кн'), ('лэ', 'сн'), ('зе', 'кш'), ('хэ', 'бн'), ('фч', 'др'), ('дч', 'лр'), ('чб', 'пе'), ('оч', 'ьр'), ('жа', 'бе'), ('ха', 'ие'), ('йг', 'лш'), ('ри', 'бс'), ('тз', 'иа'), ('лю', 'кв'), ('оз', 'та'), ('зю', 'фв'), ('мш', 'яз'), ('рш', 'ез'), ('шц', 'чд'), ('юш', 'йз'), ('ув', 'ма'), ('чв', 'та'), ('жй', 'вь'), ('ев', 'ца'), ('бз', 'да'), ('аг', 'чш'), ('бг', 'йш'), ('вг', 'ьш'), ('гг', 'мш'), ('дг', 'юш'), ('ег', 'пш'), ('жг', 'бш'), ('зг', 'тш'), ('иг', 'дш'), ('йг', 'хш'), ('кг', 'зш'), ('лг', 'шш'), ('мг', 'кш'), ('нг', 'ыш'), ('ог', 'нш'), ('пг', 'яш'), ('рг', 'рш'), ('сг', 'вш'), ('тг', 'уш'), ('фг', 'цш'), ('хг', 'иш'), ('цг', 'щш'), ('чг', 'лш'), ('шг', 'эш'), ('щг', 'ош'), ('ьг', 'аш'), ('ыг', 'сш'), ('эг', 'гш'), ('юг', 'фш'), ('яг', 'жш'), ('ае', 'сэ'), ('бе', 'гэ'), ('ве', 'фэ'), ('ге', 'жэ'), ('де', 'чэ'), ('ее', 'йэ'), ('же', 'ьэ'), ('зе', 'мэ'), ('ие', 'юз'), ('йе', 'пэ'), ('ле', 'тэ'), ('ме', 'дэ'), ('не', 'хэ'), ('ое', 'зэ'), ('пе', 'шэ'), ('ре', 'кэ'), ('се', 'ьэ'), ('те', 'нэ'), ('уе', 'яэ'), ('фе', 'рэ'), ('хе', 'вэ'), ('це', 'уэ'), ('че', 'еэ'), ('ше', 'цэ'), ('ше', 'из'), ('ье', 'щэ'), ('ые', 'лэ'), ('эе', 'ээ'), ('юе', 'оэ'), ('яе', 'аэ'), ('аз', 'мр'), ('бэ', 'юр'), ('вэ', 'пр'), ('гэ', 'бр'), ('дэ', 'тр'), ('еэ', 'др'), ('жэ', 'хр'), ('зэ', 'зр'), ('из', 'шр'), ('йэ', 'кр'), ('кэ', 'ыр'), ('лэ', 'нр'), ('мэ', 'яр'), ('нэ', 'рр'), ('оэ', 'вр'), ('пэ', 'ур'), ('рэ', 'ер'), ('сэ', 'цр'), ('тэ', 'ир'), ('уэ', 'шр'), ('фэ', 'лр'), ('хэ', 'эр'), ('цэ', 'ор'), ('чэ', 'ар'), ('шэ', 'ср'), ('щэ', 'гр'), ('ьэ', 'фр'), ('ыэ', 'жр'), ('ээ', 'чр'), ('юэ', 'йр'), ('яэ', 'ьр'), ('ав', 'ьи'), ('бв', 'ни'), ('вв', 'яи'), ('гв', 'ри'), ('дв', 'ви'), ('ев', 'уи'), ('жв', 'еи'), ('зв', 'ци'), ('ив', 'ии'), ('йв', 'щи'), ('кв', 'ли'), ('лв', 'эи'), ('мв', 'ои'), ('нв', 'аи'), ('ов', 'си'), ('пв', 'ги'), ('рв', 'фи'), ('св', 'жи'), ('тв',

('чи'), ('ув', 'йи'), ('фв', 'ьи'), ('хв', 'ми'), ('цв', 'юи'), ('чв', 'пи'), ('шв', 'би'), ('щв', 'ти'), ('ьв', 'ди'), ('ьв', 'хи'), ('эв', 'зи'), ('юв', 'ши'), ('яв', 'ки'), ('ав', 'ин'), ('бв', 'щн'), ('вв', 'лн'), ('гв', 'эн'), ('дв', 'он'), ('ев', 'ан'), ('жв', 'сн'), ('зв', 'гн'), ('ив', 'фн'), ('йв', 'жн'), ('кв', 'чн'), ('лв', 'йн'), ('мв', 'ьн'), ('нв', 'мн'), ('ов', 'юн'), ('пв', 'пн'), ('рв', 'бн'), ('св', 'тн'), ('тв', 'дн'), ('ув', 'хн'), ('фв', 'зн'), ('хв', 'шн'), ('цв', 'кн'), ('чв', 'ьн'), ('шв', 'нн'), ('щв', 'ян'), ('ьв', 'рн'), ('ьв', 'вн'), ('эв', 'ун'), ('юв', 'ен'), ('яв', 'цн'), ('аю', 'пв'), ('бю', 'бв'), ('вю', 'тв'), ('гю', 'дв'), ('дю', 'хв'), ('ею', 'зв'), ('жю', 'шв'), ('зю', 'кв'), ('ию', 'ьв'), ('йю', 'нв'), ('кю', 'яв'), ('мю', 'вв'), ('ню', 'ув'), ('ою', 'ев'), ('пю', 'цв'), ('рю', 'ив'), ('сю', 'щв'), ('тю', 'лв'), ('ую', 'эв'), ('фю', 'ов'), ('хю', 'ав'), ('цю', 'св'), ('чю', 'гв'), ('шю', 'фв'), ('ью', 'чв'), ('ью', 'йв'), ('эю', 'ьв'), ('юю', 'мв'), ('яю', 'юв'), ('пю', 'рв'), ('щю', 'рв'), ('фе', 'бэ'), ('пв', 'це'), ('ев', 'зе'), ('щз', 'жэ'), ('ув', 'эе'), ('фв', 'фе'), ('кв', 'ее'), ('еш', 'ув'), ('шв', 'ье'), ('же', 'бэ'), ('би', 'кс'), ('дг', 'ощ'), ('си', 'ус'), ('лэ', 'бн'), ('ээ', 'ин'), ('не', 'щц'), ('еэ', 'чн'), ('юч', 'лр'), ('нч', 'тр'), ('св', 'ае'), ('чч', 'вр'), ('щг', 'фш'), ('зи', 'щс'), ('жа', 'се'), ('щв', 'фе'), ('нэ', 'ще'), ('ша', 'ве'), ('уь', 'ее'), ('зэ', 'ке'), ('да', 'ве'), ('ее', 'тв'), ('ле', 'тв'), ('ув', 'ьв'), ('пе', 'тв'), ('сг', 'ьэ'), ('чг', 'ьэ'), ('лю', 'яэ'), ('ыг', 'ьэ'), ('ха', 'че'), ('ыа', 'че'), ('пв', 'ье'), ('гэ', 'ае')]

### Критерії перевірки на змістовність тексту:

Заборонені біграми:

['ав', 'ов', 'ув', 'ьв', 'эв', 'ив', 'йв', 'ьы', 'ьь', 'йй']

### Знайдений ключ, що приводить до змістовного тексту:

('лю', 'кв') ог (370, 312)

### Шифротекст:

фелсэугиселбуйэатеоплмхфкплоынощпбвуцакэюйкзкусявяляеюкуешяэюазыкйюязвсусяюыпдэжввятедыноячтхк  
зыере  
явийтэбеубагзлчедэвюцэеямадюзвюеюцынощыешгфлцхазцчеолмхечнзпвледсдямвзжевмэбйрбсюряийвюухышли  
фвсоч  
люряийвюухыешгтбютазцягтьчяяжцэфлпнитсетеуюйвзсдяшевэушенибсчхеюезючеузийяюпсдямаэыгнзийвиснриж  
шдуй  
ьюфлийэфазшгкякзшыяпатбдспвясзгинкэтбыпрбгтбшйсйсыдэядемечмайвжзаслзткхчбчмчйвувтгинкэтбыпилхьягв  
ц  
кзьяэькамащлщзмхыкмчуябллдпволмхечмчкбуштзвцйвнбюяеммччедэядаяэюнвшьюзщашцкэфлпнцочпмменбюозэ  
еязявч  
усвесехкчюгупвийбухввлэыволмхсьжектьясезвььдснлулшдяюпсюагякбжйуяичявуссеьхвжщтьжсуйсыхсмччесссем  
нэ  
сыеюолрщдэисшисерекэьбпэлддыеюрябенбауасызццрецямеезфразлдагжчюзнйпупввеюкусяэчретлктзцаушцозчуе  
гч  
рразыепуочссхсзмнзфкузмасызэыечеолрщсррятекщазшыжешьчекбмаедуззэитсефкфкемюцээжйэвррщтьжслеаяве  
жчзл  
брблфкдчщдсзсыщущенофлеяэюипчккггутехсаагямаэчявемцщибыекичслвьчблтгинауэеядюдэпббийьащябазуьхсэ  
вчг  
ээбсьныньаплгхслшднзысвнслзыенбйдэгэфлпнюяшжвмусвесехкмащлсюшрэреттгкэбйцйсыхсфкемуийгфлхуыкнзш  
жксмг  
ээбсьнытгжчюсийвзийюаньюююячеуспвссмеоеочхедэеюфцжедынощээвныпшжаюфнпвевхчфкаеуйгзшглсйэыежеаязв  
юерекэ  
хуввжэийжссийвемчфкэьхедэеюфцкыноязсыечвплгвюаежзкювесехерглсрьхяэюеозэбеаяэсвейувюухыешгеюшрац  
чче  
олмхечнзвчичймсеатьяьччебддятеубфлцсрбрщюяевисувпзшгвюаежзчююячеумиежвемшдвчусмэебрябйвесехкпюмч  
зуен  
шжвьдядюсссввчумыепвплящыдхвоцкчхсйежещцсжвдюцынощфстейцхыедэяплгхазлдвнухокусызыцнздузуьхв  
ывпзкч  
уйцйрасетегльнйвйстерирчссцяэьсьжвдядюащсэбауретещэщхрхвмчющчалсвчумыесыедшьдямзггээрспвевьнз  
мчшж  
кскякчдсбдемиваецяэюядчймхуыквщзлбйпцкэиузбвюдэпфэрщэщхрхвнйпчячкхэьбфтсличцдмщйвцяэюспвсем  
щйвця  
эюспвчввуеивхзшгебрщвюцэрякбсыюяхвывдщэщхрхвсверчпмхвххвегжчрчдэпвэящаензэтьссувнзшупвзйазэяхвы  
вув  
пвевшврбюятехльянийжректижуеивьяькбгзблвюжгебткязрящаенквткелофчельсвузфнфлшпкякбсыеюаыедшьузьряк  
буя

евйвэясчищзэнгитыюдэтежвемсейвчясемзцвсесехерщфлюзщашлпсдбауячедемяиоьусшьоьпвевшвчебдувнэюгщэщ  
хрхв  
мчльсвфэътсефкюкчеочшвхсвеьссьсвмвнауслкззэсрюйгяевмчсзьятеуйочдэвсмччехчгчхсвясолехехчрщзлсьйвгсмч  
хньяхвывдщэщхрхвсеумвеолфрыщцэнзийлвдсвчрбжавюблнззэйткясерщзлбйпбшзаетуйячтхзэеяйэщедэхетекбыщмч  
ая  
веревхвывисвзлшдзвьчбдцюояевкшкчхетцччедцющблфнмчьхедэеюжчстевектззлфзюяудзжуныпкэяьвнбюя  
зэшы  
нзэсбсюнаувюпвевхчочдэсыячопдэдемоуячсхсхзфтдынзуйсыаечечюемпврбвюблшдыузчмщпвоелбоыбйшьтлу  
ймзсс  
чххзюйзэебсыюяевыеисшмшдвнауслудзжунетибмчлльщцэнгхекбвюцэппенрбкцээшдкэгчвьшбюясебнпбшпжжцэьб  
фншьае  
ыеэюьтыднэнийрбпукюбйпволеюьщэщхрчсхвйвдащлдэпббпгьхейлсюбпсьщщьясктнщазлцсуюоряезбпвчмтсензтедсы  
ехнпа  
ябслсввчхеретеонвюдчдэслтгбйряеввяевхкыйвцупвшелеезфтщжредьзюяемукпвчесехенсямзмечемщзэцсуоазья  
г  
злкшкчхетцччечячевейряоьхвчсуммвашжчфтгчдчакэбцймзблдэьдрышсусшдучхвуспвяюпсцютбнзапныщчезнзэб  
лче  
шчрчбдмнюяевнлазыеьуйклауесйвагйвиснрпаяьщзыщцюпцкэссьмкяпвьдокнлхупвяютжлльщьяяпэижйябшьрсое  
нбиж  
чедчячнрижхвчснзисилмзяаешвячиязбцххвускэюяувхсйбашблждкззбвсэцкэосмчпцкэссогюшкразгупвнрипэюебое  
пц  
кэссьмпуеннзкювцслтефьунюнюясетеанкэтбфцнзэдшбаушайвмгеююшжджгйвисдямзьярщрчфтьюдэпэямарыкэе  
южйсы  
едшьдяхакивэянгюшрчмчредэядрчрехвочщщцебдэпбщзыкчщцецдьчрчнрипхуоежяуйазччийпбптьнсвиймачтхслпв  
яютб  
ээжжлыщыщыеевяххуухябчюьсценлендщзблфрыщмюфлеввтещгчуеивсцйыкряевхкйьрчллкабахуаяютбшврежз  
ьясече  
ввумхчтефьунрясеулзбыыпдэжгдпзыпйбашнойцэппцеатыдпзбпхуоечсдэйдэыкделеезфнйбашчедэпбщзыерглсткх  
нчю  
лгбличжчоелесеияебмадьшйтпбяьпцкэссьмопывичхвыехнпуенуяблпугблчезьськоныпяюкчрешжксюерефещпс  
уммв  
ашжчфтфкузуийешнинйвдчыеэюшзмсхуоклаузчречечайзапчнлоыпюнящаазыеплрявчхсжешьяевпзбпнрпаяьйс  
дпвдч  
йлвсочлюкшжчечкненкэтбсыюяшайвхсньедемьюеояеюцдшьскусучхвусччийпбюьдэхесюьсзмчатенийкщзлюйтгсyed  
окжв  
уцапбщзьявесехкюешхблрчхщкрвюльвьтгнзийдыжглсйэыеебьячаеьчсрщцецухвмглсйэыерейваыеютбзучкбээ  
сч  
хсйечечяваеюясехеюзеюкщыемхмеефкаеютазпссуслрямсюяевыеисаезмчевдсйбашслифжисефкдяевлснюдчоеда  
тбюш  
чюьчаывемнгкэвсткуевемнфлвтчнэщашлвьезьяевзмосжвыежзкзгзьяевзмосжвыежзггюшусжжвийчьеечесевяхвыв  
чы  
йвюэпэфлпнщевэжгшпуюебйэмаршкзблгуьщьяцдзввяуюйвнауслпвдэьяждсюкзеюпварарывьсхвчийвгсшайвзсдз  
дчоч  
шьпвевумрсумщзфтшсьячдярбюяблнзуаяуязоыячнзцссагээхеусумфтуикэювхетклаибждыецяевхскэгчвьдяуязкля  
а  
ыдзмсеьчввюкцелеоьфеумвьрсочлзэзыьдснлйчшмшддчочкненнзчмщцэьяхвывчийвгцкэбажймхэсмчягтбюненмчдс  
исем  
шдъйлфлеюевекзфнфлсроячпвилэщцеювннийгчлцбйчэфлмюоржгкэбйагйвьсжвчийвюэенсеьзюямхнзпупвлэфшряеве  
мевтэ  
нзвехулызпжатсеюкшкзблыпзбыыпйвмщсюущзчвярыеютблдчочеупвзтуизынощцэбапбщцецбфркмщцэквпвве  
мчсехв  
вежвхвжэщзыгкязэппенпвочвзкяцссувюпбюасячслаибждыеягбйхзклбкляпессичжчвненсюзэеявхскэспусцвдэйдзы  
л  
фрыщсэгзтпбпарчвдчоеяьщчыкмчхщуьэенсыбйфлюшэвчехяхвемчехяхвемчегэтбблйбашисдсюеуеюврчтсевектб  
лья  
сэенвнтбтбтьеяуйазггпсвнзэеяхвываеыеэютбетсюидчаевгнысоедэвююдевивтчднгзюйрщсхсвсеечвзсоеюдчэбд  
ы  
слысткалценусявблсейсоехкляуязмчоеретелсэюлфцвюэяйейвмшвювюьсиядюзслейюгульычреаячещюкюкзццсзм  
афл  
эчщюецблцэжчгынзэслепзенаесскыфлеюыглсолкрслшднийфльвчейбгублшдивлшьпвтктеоехззэьнхсрбфршгеваеигь  
дую

[illegible]

зисталподниматьееграфисеменсмотрелинанеговдругкакэточастобываетзвукгонамгновенноприблизилсякакбудтовот переднимисамимибылилающиеиертысобакинулюлюканьеданилыграфоглянулсянаправоувидалмитькукоторыйвык атывавшимисяглазамисмотрелнаграфаиподнявшапкууказывалемувпереднадругуюсторонуберегизакричалонтакимг олосомчтовиднобылочтоэтословодавноужемучительнопросилосьунегонаружуипоскакалвыпустивсобакпонаправле ниюкграфуграфисеменвыскакалиизопушкииналевоотсебяувидаливолкакотрыймягкопереваливаясьтихимскокомпо дскакиваллестееихтойсамойопушкеукоторойонистоялизлобныесобакиизгнулиисорвавшисьсворпонеслиськволк умимонголошадейволкприостановилбегнеловкокакбольнойжабойповернулсвоюлобастуюголовуксобакамитакемя гкопереваливаясьпрыгнулраздругойимотнувполеномхвостомскрылсявопушкувтужеминутуизпротивоположнойопу шкисревомпохожимнаплачрастерянновыскочилаоднадругаятретьягончаяивсястаяпонесласьпополюпотомусамому естугдепролезпробежалволквследзагончимирасступилиськустыорешникаипоказаласьбураяпочерневшаяотпотулош адьданилынадлиннойспинееекомочкомвалясьвпередсиделданилабезшапкиседымивстрепаннымиволосаминадкрас нымпотнымлицомулюлюлюулюлююккричалонкогдаонувидалграфаглазахегосверкнуламолящаяжрикнулонгрозясьпо днятымарапникомнаграфапроливолкаотоохотникиикакбынеудостоиваясконфуженноиспуганногографадажнейши мразговоромонсовсейзлойприготовленнойнаграфаударилповвалившимсямокрымбокамбурогомеринаипонессязаг ончимиграфакнаказанныйстоялоглядываясьистараясулыбкойвызватьвсеменесожалениексвоемуположениюносем енауженебылоонвобездпокустамзаскакивалволкаотзасекисдвухсторонтакжеперескакивализверяборзятникиноволкп ошелкустамииниодиохотникнеперехватилегоникалайростовмеждустоялнасвоеместеожидаязверяпоприближе ниюиотдалениюгонапозвукамголосовизвестныхемусобакпоприближениюотдалениюивозвышениюголосовдоезжач ихончувствовалчточтосовершалосьвостровеонзналчточтовостровебылиприбылымолодыеиматерыестарыеволкионзнал чтогончиеразбилисьнадвестаичтогденибудьтравилиичточтоонибудьслучилосьнеблагополучноеонвсякуюсекундуна суюсторонууждалзверяонделалтысячиразличныхпредположенийотомкакисккакойстороныпобежитзверьякаконбудетт равитьегонадеждасменяласьотчаяниемнесколькоразонобращалсякбогусмольбоюотомчтобыволквышелнанегоонмол илсястемстрастнымисовестливымчувствомскоторыммолятсялюдивминутысильноговолнениязависящегоотничтожн ойпричинынучтотебестоитговорилонбогусделатьэтодляменязнаюттывеликичтогрехтебяпроситьобэтомнорадибог асделайчтобынаменявылезматерыйичтобыкарайнаглазахдядюшкикоторыйвоноттудасмотритвлепилсяемуертвойх ваткойвгорлотысячуразэтиполчасуаупорнымнапряженнымибеспокойнымвзглядомокидывалростовопушкулесовсдв умяредкимидубаминадосиновымподседомиоврагсизмытымкраемишапкудядюшкичутьвидневшегосяиззакустанапра вонетнебудетэтогосчастьядумалростовачтобыстоилонебудетмневсегдаивкартахинавойнево всемнесчастьяаустерлиц идолоховярконобыстросменяясьмелькаливеговоображениитолькоодинразбыжизнизатравитьматероговолкабольше янежелаюдумалоннапрягаяслухизрениеогляд

## Висновок:

Виконавши роботу, ми засвоїли методи частотного криптоаналізу на прикладі розшифрування афінного шифру біграмної заміни та опанували прийоми роботи в модулярній арифметиці.