



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-74  
Стурчак Максим та Харламова Катерина

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

## Варіант 17

**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:	уф	иж	ьи	кщ	хф

#### Критерії перевірки на змістовність тексту:

Заборонені біграми:

{ “кщ”, “ся”, “щ”, “вй”, “гй”, “жш”, “аа” }

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

(рн , гз)  $a = 509$   $b = 100$

## Можливі варіанти ключів:

(хт , ву)	(фо , ои)	(ел , уд)	(хщ , йс)	(од , кф)	(ня , мз)
(от , шу)	(нг , юо)	(ат , нз)	(цщ , шс)	(лт , их)	(рз , жт)
(ту , цж)	(нн , юз)	(ша , кщ)	(пю , лп)	(щс , зи)	(ба , хф)
(дз , гн)	(рн , гз)	(ня , ии)	(вю , яп)	(ны , жи)	(юц , ищ)
(йн , щз)	(кс , аф)	(юл , ид)	(рц , ши)	(ры , жи)	(яж , щэ)
(ша , уф)	(аа , аф)	(су , шщ)	(рн , гз)	(эо , ои)	(пз , ет)
(эб , ьж)	(пв , ця)	(кб , эщ)	(пв , ця)	(эг , яо)	(яа , хф)
(нф , ек)	(эв , гя)	(сб , эщ)	(та , иж)	(рн , гз)	(эц , ищ)
(рн , гз)	(ой , кж)	(пм , ыщ)	(аш , уи)	(ун , из)	(юж , кэ)
(за , уф)	(от , аз)	(вз , иб)	(ап , бг)	(вс , вф)	(ср , ьф)
(дб , ьж)	(пю , лп)	(щф , сю)	(эв , гя)	(зз , эт)	(бй , чф)
(фф , рк)	(на , ьи)	(бф , эю)	(на , иж)	(жз , ыт)	(вй , чф)
(мм , еф)	(яз , пж)	(пу , йи)	(нш , уи)	(чр , шф)	(ап , рф)
(вя , бф)	(яр , вл)	(от , ьу)	(нп , ьг)	(юб , уз)	(сб , фз)
(ья , бф)	(вю , яп)	(зт , су)	(ой , кж)	(чш , бы)	(ащ , жс)
(ру , вф)	(та , ьи)	(ву , цж)	(яз , пж)	(яа , кщ)	(бщ , хс)
(ьш , шн)	(сз , пж)	(гз , дн)	(сз , пж)	(рй , хф)	
(сл , цр)	(ср , ил)	(рн , гз)	(яц , жж)	(хщ , йс)	
(кл , лр)	(рц , ши)	(ша , хф)	(от , аз)	(шш , вы)	
(ом , щж)	(аш , уи)	(уб , ьж)	(яр , вл)	(ба , кщ)	
(ях , еэ)	(нш , уи)	(уф , кк)	(ср , ил)	(сй , хф)	
(ых , пэ)	(ай , эи)	(чн , мз)	(ай , эи)	(цщ , шс)	
(вс , зи)	(рн , гз)	(за , хф)	(чх , зо)	(зп , ещ)	
(нг , юо)	(ап , бг)	(ьб , ьж)	(фх , со)	(оц , ищ)	
(ак , йа)	(нп , ьг)	(ьф , хк)	(сс , цщ)	(нц , ищ)	
(эа , уф)	(яц , жж)	(эм , зф)	(мг , ра)	(ер , пщ)	
(вы , жи)	(зт , цз)	(ля , гф)	(зк , лс)	(бя , лз)	
(нн , юз)	(ат , нз)	(дя , гф)	(эа , иж)	(йж , фэ)	
(гк , яа)	(су , шщ)	(ау , дф)	(шы , хщ)	(иж , еэ)	
(га , уф)	(вз , иб)	(ыш , щн)	(ун , чш)	(щп , оф)	
(еы , жи)	(чн , оь)	(лл , ур)	(кк , бс)	(зк , лс)	
(рн , гз)	(ша , ьи)	(дл , ир)	(га , иж)	(кк , бс)	
(эо , зф)	(кб , эщ)	(ям , щж)	(ыы , хщ)	(но , ьж)	
(эд , иф)	(щф , сю)	(лх , юэ)	(цн , эш)	(тэ , га)	
(щд , иф)	(ян , чь)	(их , иэ)	(но , ьж)	(чх , зо)	
(кс , аф)	(за , ьи)	(щс , зи)	(жд , эж)	(га , кщ)	
(сэ , ро)	(сб , эщ)	(эг , яо)	(гд , эж)	(жд , эж)	
(ст , рх)	(бф , эю)	(ук , та)	(щс , фж)	(лт , ьз)	
(от , лх)	(нм , ми)	(эа , хф)	(тэ , га)	(фх , со)	
(фо , ои)	(фя , ии)	(ны , жи)	(лт , ьз)	(эа , кщ)	
(чш , бы)	(ня , ии)	(рн , гз)	(ит , хз)	(гд , эж)	
(шш , вы)	(пу , йи)	(цк , иа)	(ео , ющ)	(ит , хз)	
(зп , ещ)	(эш , юб)	(га , хф)	(ак , йа)	(сс , цщ)	
(бя , лз)	(ел , уд)	(ры , жи)	(гк , яа)	(шы , хщ)	
(зз , эт)	(юл , ид)	(ун , из)	(эо , зф)	(ыы , хщ)	
(ба , уф)	(пм , ыщ)	(ео , йф)	(сэ , ро)	(ео , ющ)	
(оц , ищ)	(ук , та)	(сд , кф)	(ях , еэ)	(мг , ра)	
(йж , фэ)	(цк , иа)	(од , кф)	(га , ьи)	(ун , чш)	
(жз , ыт)	(ео , йф)	(вс , вф)	(эд , иф)	(цн , эш)	
(яа , уф)	(вэ , со)	(вэ , со)	(ст , рх)	(щс , фж)	
(нц , ищ)	(лх , юэ)	(от , нх)	(ых , пэ)	(чн , оь)	
(иж , еэ)	(га , ьи)	(лт , их)	(эа , ьи)	(ян , чь)	
(чр , шф)	(сд , кф)	(эо , ои)	(щд , иф)	(нм , ми)	
(рй , хф)	(от , нх)	(ош , щы)	(от , лх)	(эш , юб)	
(сй , хф)	(их , иэ)	(пш , ьы)	(вс , зи)	(зт , цз)	
(щп , оф)	(эа , ьи)	(нп , ещ)	(вы , жи)	(за , кщ)	
(юб , уз)		(яр , пщ)	(еы , жи)	(фя , ии)	

## Шифротекст:

ккцлпжтвкофаоопкррнхбхньшсрдфгжцзляжахеунелцвдсмунэкшшжмпеунзмдвелбмьярьфвсщпктсыщмьбхенк  
фкцвэвиюфудмптпккямимьящшцздмввгкгмдсрцикопоюрббебыткнкбэюенвскылмщевдчзвжюасфтмнцмаймибикуулуб  
лхывмнцмаймибикумффушпсебьяпждлщчмьяюмхщшвкпкмэвдлмшакаякцжжфюычгкмтмкоендбмлмшцзэяцпоеэвс  
лносчцэаалмюбмачупеопэщхецдйщызмфылнвшлклохлямфярсфпмфилшабсызэюиэычшэваеиэьнуызыьэвгвюпохлям  
фяркбодмпмохеушмдшзубьяекбуньыхщяьинвнхкбэьыбфкцбемозэйфыщюибыткьязэцщжмтвдфевзбляюмхыдхыдия  
кйфсггящцошфыелшквкгнгмажнвуфибьяшяовнхбшдокфшушквквсдылаьрцэбмлчзэяцбфсахщепцвелквсдновыцдцлаа  
бсалытккливюиуябссмнвцьяслщтвкфклячфояиэтссмнщлкйфчжжлщцебыфкющяктейюпеизмпкыфепабжнвшконелющсы  
фкгххебешцкцугсыэквыуюпеикбжхыклалшиоехноеузбсгяикткнхвцклнщпксцпеясокцдткбфузчэоегяшшвкхххноирцэясам  
дчювцждлцлскцшшккыпкьюаххнпыдэуебсыокцсмювщцжмароытпажпккалтзэшузсыцвиоитцжфикютельчвцыяьюпохчжгяшщ  
дмьядфоасдлцнфпеудалывбпэюфшдлсущьсьбхьцэюерлохххщехжоаьняюмхыщичиелшквкгнгузбтмнюсыфкюпляоаиа  
бсалхнюиаацпоьсжунюеичмлнпэюфшдлслюпкыллэвяаьщэмлмыщткелнвклякцкхычкьясмюооктсрцэяюхяричомпхнвзу  
ыхнюаачеопщлпоиякоцкщввгкфклясжявфшашчклэвчдыхнмдчкьясмюогсыщдликшвшеапймюаефмшквкчкпщлдрщж  
мсмгялкцшолзвржймибикуосммюпобыткнкбэюефывуикшошущытквзмщпкщфюьлнцсфвыщцзвслгвшеоппмюкаегмы  
шткцийкфвиоицфыелжяюфнщоашквкгнчмьыхжжхичбвмщдмквивфыщиикнвьюацяэювзцаыалцкокийкфвдмдсрцтлпкка  
рбикьяэщьсбпеиэюхибенелщцыюепоьюеудювовшыааианщвкпкщяхэвлпкотрыклюшмдглфвмщдмвзилтфчжфкпкыцгцц  
юювьырцвзщлфышиикбсчэцдмщрефпэялнвзвпдоьюеичмлмцаыылэвоипвюкюшжмыщпыуисжунжцпоаьолягжшфймья  
юдсявгцццюювпагымытпчкчфьшхьеыэмцэвюшжмшрфывкмцэвюшжмшрфывэкпвийеопофвцймьянщбфбсыщцвовбцгц  
цюювклшккрыдиовюовювппкырыьянвошвзжжгяждкпгвюешжнвяпаешововгвнвзвжвсфышпкльлзпасчфкфшсчэкпвздбфчез  
ьймэпофьнвенщвзжхкьнфьыуткидивоепхьюцрщбфбссмэсчэцдоешнщбфхшзэвошцьющцгяьпщлмьяпкфвиовкэвлщвк  
ребышквкчквцюьфевзбылрфчжмычэюиктрделцдрднвзжвтквэгвуясмуцгццюювьидивсвлшкххонткхыжвалшксдклшдх  
иохчжхьхегябюжашцзвьыуеушпкаахыьялбыткуывыалсщвлскчуывцпбсэвольэухущювовбцгццюювкцишкнхьюицм  
юендывылфысфгймьяюегяшщэщквцпьюадфсепсшаамьыбгяшщюянкьячкпкбфицьщцщкфкововосклепцэвцывэхмы  
шзвсцаымбсшбыткзорцяпхьсдчкьясмкыглпкшкфшгяпыеышцзвххярляздяйфышгяясоеюлулихчжймнвзуюхыьбс  
ыррьэзюивсмкылювийеыштсюеаабсюктэыйвиоинсфймьяцэвжчымцнвшкофшсоадгьяареклоыйежагяюфбсышцзвикслэиц  
эохчжхьуэдчвхсшжфьыеицмьяпчкбфйммямхжхсфсцэяэлявыбвзфышцвкрхдфцрцчмячфпхцдюикжмлшэуэпасфбжфмо  
анвньсмицгццююловэвиэбьадфврэдчккьтмвршдщцушнфхвзпнлмнщтеврфыпшвкюепкыликэхызнфхывфычкфкпкахй  
мпьяхьюпоанщзвсцзвгнзсэвяжнваскстешхчфксэмеыщюииннвтквкчкфлмщреякткмцгянлгпендмпьсцаымбсшбыткмы  
цвиоишанщрдюовльщивлцкышвыпыйнтфиареврьэсддилелцзшыовелнвбмлхммфюепемхыоткьхгяьткыырывэдхышцзв  
ыпеиксдаачьжйлэвмпэвсллюызздэицгмьолякчичишнвсэнаьсжнвмччьеицздийшоясчюанфцдэлщкйфсчткпымылюсчювь  
люеслэьрездюкжвмывшщфрбювелляышгвалуфгйяьэехешфблйолявлыьоляклипрцгюпеажнвлюаржмюфщкьолякчибжжх  
юефммохьпкбдвхиххщвкпкгхлямфюоюеьэзэфчжзэвнпсмрцеэпэвслмщреушвцрышлмьяюдошцзуслясмсабсчэцдмщодй  
нпвошщпрцрыфкьяэрыфкювхыьцяеюфьядфеуенденкыэцырылюарсжкцэапеоышадфчшахиуимыьбхьнвмбфякы  
ыюыоикзвыбсжибифгмглтхжхсгэяьйиоицпмоьшкявпктцвызкпвьлиаунищзвгндрьесьшасзсжбммфжвфкаеушцвкткявщи  
уыпкбдвхнщкврьшфсьарьякыэшешяруфгйжамямхекюшэшеврсжщкьяэвьунукстепухфгйткьядфеикгпщльнэхгмапьяь  
ыкышцксквкщюфузсэцдшдфздьоляклчирровеювикэхбжжххщяьбжфпяьткмдшднххярбмаыфкичмлгкфккыцплшиевлцк  
ышхноеааикехохэвпыикжмьэзлсженеьчжчыфкткмыеегяыашьярышцвзпеикьнщфыалокцдззвшеврлюызздялэунвпыкб  
лхывмсцкыэыйхжхлямфбсышцзэвалгдчэюиадщквщсмыэцднелшыовелюышадфшдьячктмглшилщпкпасцпжаюпбсчэенф  
воешздфяеушшквкгнгклярьеыцгюймидлдопоепаэтэспщлпоиякюфушцткюкцыквлцфоибявнпщлпоиякфкэзэссммфчышыф  
эяюыалцтккмьцвиюкышквчкфесмсциккбякиххнюкушпеплыжхьнщзлышцзвикслюкшитковылуфгйхьлуитвкхнмщзвлэмпы  
шкизмфрцгмцышщкдхфпляблнэкшкдхюьчвлуыавзбыдтеушцзвшивлфвикаехечеушцзвшивлфвикаешпрцелцлфвтисдбкткв  
кспцововссэвкюаюьмхнкаяэпцрнмюфюузвцхьяящиущыэввсцшцжаохчжхьнвяушечтмхесмнвэюэюовглвовссэволзэв  
длмщбхпыхыцднвзвицлцияеышдслымщсфыщяюехцаапешмыоееклмпэячкелшишсаалйвчкьнжщфезикушзвалл  
яыбвмщцаагечезэшищцкьявонекскрцкщцпдэлхшыгядылаьтэиципыххжхюецшмьяушццовавсэвщцловасзэцасаблюы  
япмфихжхьыылслюицэюапыюьсмшкхепхюбюшсмынвкьгцсмюхпавьеооашяюьпмшюэпляоампэвлфвссэвкяжхкмеышкб  
юебжнвшячцнщзвиоизвцяюешксжидщепчовшконащхьяршфсьярэвмцтмкцчысшуссммфьяпыхьжнвмшааьсрцмяздфяеф  
омфйюаьмцмяквнвшкыьквювшкфвювхяецпэщгямхжхнхыкеэщнлыжймдфлцщльжзжфеэикапоайечьяэщцкккыкыюх  
жхтмгяшщзвалляшреллвьяэвьыьйиоидияящмшдфызрышвпышцкздыйуныьеуцдвяжхбсоаюьрцывткэщцвовиоткэщцвовиоткня  
мфяуфгйслылгэкйврымшкшкфшьяушйжххюхмфмфлшщцаапешпплохгяшщцвововоикжммфсштмэяткйиндлхрлщкьяй  
мязэвпвлышхчежавцкловшквкэкетмсмпытфтсхьрльнсьмьяжжелцвявкляшкпгкцаапешышцкфкпкцлмдньюоймошикэвмцй  
ймглвшдмдлскзмажиддыфкццткюмфмхебыуеузьюьсыномфоямьякыесюеюлскшежхюкклгсюьсмпщлпныгюхцэпаюобвтк  
уфажьяцэпвицлднвнпкщийегяхалсфйюопзвюкчпсэгкнвчэщкюшшкгтсмпвьсэвяжщцфмьяюфэяшцднлххщалыюалякын  
пофвцэкккмявщиткесыкыонэхблыгцвгцюфйвмждлызвлпщхлмнвцовгваэкпвищпийнжмщцуюшбщцткпкяхцпрцх  
учнчмпьялэаречезэшищцкьявонекскрцкщцпдэлхшыгядылаьтэиципыххжхюецшмьяушццовавсэвщцловасзэцасаблюы  
лащфыгкэзышесаткюмфмхебыдхлямфаынькбьяэпщлщезжоафкнвткпкяхкцаымбсшбыкбпеопмфюххувчльыххьрлбжов  
юшмофкюэкүмяшрцдвссюышцвяклйнвкпвляьярвксфюеллфышииквкйхарфкюкацхьясхчжхыщыефпювьэвмнщыьнщын  
скылалыжхьнщзлнмушхьявршкяпоьопщлньюймглшиьнохюьмхышахчьяюьбуфгйбыфкьякыэшешярызвцяьэщцшкф  
кфшбыэвюзяэщыицвьяьзлрцнвккщижвяфгмгжвакэкэшысбсфмшышцзвгкцхыюяшщгцждцвмшущюиьзлткыньнушц  
мщкщиткрылделгкуфгйзлсфйтквкцзвзубыьшнсеыдичичювдивчхьяркрпвуявсоеушцлфвалшиьыкыалфвалшииквзудявчза  
лшипыхыммщюцдалнвеечэщявзэпэвслюибммфздрхлямфярровбдзвмшбаюьрцяршкэышиуфгйвкцывжщквечьбжаэятм  
юшпкррждлызвпвлышхзкгхгнрыблщкьяхышйткюинновыхщлйечьпыхышжхзвпбхлямфвьрньняцпьяовэпгюздуфгйвжшфб  
сцдалжфюеяэзвпвлышхчеушцзвшивлфвикаеушрлльяхьткпеагяюйтсэволпыхышщгкбфпьяехетссмшсфсювувтквбьяэвзмч  
ыфжюдмсюеаексмепкесфгаллмщбхххщадцямлялпксюпфцклевеллхналгвзгыхьяшцзэхэдичичювдивчхьяэсвмке  
ьречызэаефпэвпклемсцхелюиэзшквкгнгчмсхгяфймйглелцэьчжаэщцкбфпнвуфгйзлтккедмжвуххдювфнфврысдяпофвцн  
вшфьссьямфюеьзюфтсбжжхщлбвюкжяжхпафкюэкпшвксклевзбышщвкыуяшцюкпкьяеаьдцысдюлфышииксфышьяьшщд  
ыфкнвждтдюпышцуюоввмапхщдлюшцзвжхткнвсфймрыкылухуфгйсьэволпыхымьяшцуюовалбжэпгюляехьмнкрщуюдсдя  
валпкяхжхлямфврээххэпофгмхьтмьяэшидлулсщшкшктпрцюхжхтмхьрывыблтхквкщжарэпгюлюыхлямфярюешцк

[illegible]

[illegible]

одылабкчшиювщажапемхжабсгвуенщювовуюиуянкаябсщшвкэквээыкегязэеаабсчъпзмяюивциахьюеыгкгдлявыбвиюинсы  
выиессчфвцхецдльпзмрвкбнввыиеаынеррфзкцхшбвьяалвылшааюхжхярклшдхиздйьярочалткцыхяпкфвиюибмлпшлмьяпк  
ээюштсаявкгдкфзгвшвбмлрфрцунесммфьяюеввсщузпезпщлшовфнфвиюибмаысдкдюшжмбэыгкгдвбпьиэичьйщюешящ  
шлмьяпкгкнцьябесыгтмюгмпыфккыбаперепхювцрьгтмохъраыщэмьсэволвэыпкйкьесмчэгвнпаэвэсммфекцыклоиэыэ  
шуфхщюнавяебявокищъвзрыклааслмыгвсфбжнвлюшккциуыфктзюэзотсыщъсбпеиэхызцхшппкаиикелэымшщиявшеяр  
экьюкнвщпкыювгвпыдэоввкыкыгекъхегммфбвиюиысфсцнфгяшцбхэкыбвьявзсжсфъшяеркьяхеймалфвтыпечжфмяэсы  
нпазэлгвфзюбсыюштсрцвзэвсэволэоввкэщюфылгвшинвэктчщияитзвэыкеаэоыиесгвовппрыээшелущзбгыжхчфляювз  
ыцвзэвзипкыявшевзгвфкыивеушщпкпайшсрцэяпъбамяжхвыиеноеблкапеиклщжанкжмюфцыклааыпзрынвепхюбэщяюеп  
ьюжфзбьюетмоысдсфхцдюисыклшкгвццрбтмхъжфрцунащпквщчкшкспхщювляцыклщвийетжевлщкыппюушпешевзбъаыфлш  
игкбжщливрхлямфоаюефлвкшвкюекбвщймикхнхноефпеятмчклщшчвбпыгзбеляжлявшесмфыгъайъпагяпеякжхгнгвшитсм  
фхесшвковьяймчээтснктърбмяшщпкукфымщцкнвбгвшдидшыфкфкявнвзвжхнгвзвыогмичьпеймбмаыфкцыклщвзыбн  
дмпохаынвуйаричкклиэлзвыбгмыщсфрлпштмжхсмпывицыщыэжббжкликрхюейоыжмюфвкфкхыцэывэщыхэщклуехе  
сынвлюлнвалнвскылюиелцдннуфхщдлсфлятмшквкчкукнвыгкеьцзмфляшщтыцбхъшкхнюкввгкнщузгбхъшкхнюкщянкнвз  
выцдфоаклкъбхбсэпчкчвявгвюшущясмкыэяпчкщкббпебшквкчкфккоесшлмьяпкфвгвпыдэяюышщткэкъеяримлюитзояы  
пзпаяртцоаюфшщкнжзбьюегмнщпэпщлсьэщйэгхрлчфоаопдфицикуэкыкепчкхыквбншжмпеунулюхушунбпажшфймр  
ыкльщышщпцррщпкчкынтхчкхынвюшмонвмыннвесмюогъяюбэузбьюеыштснкэышебснкжежапесмфмпчшыфкбмюяль  
мэынмэякышеоадлуфицхщикдамфажгмяфшкгкньопчэзгаэкосйкеаатмнмсжеоаллуеаабмэяпешшхчкдюшжсмхушщпл  
якыбешщюиовшкфклшдхиажнвхыкфвкльтвкфкофаапеув

## Розшифрований текст:

князь андрей приехал в главную квартиру армии в конце июня войска первой армии той при которой находился государь бы  
ли расположены в укреплённом лагере у дриисы в ойске в той армии отступали стремясь соединиться с первой армией от  
которой как говорили они были отрезаны большими силами французов все были недовольны общим ходом военных дел в  
русской армии но о безопасности наших в русских губерниях никто не думал никто не предполагал чтобы война могла бы  
ить перенесена далее западных польских губерний князь андрей нашёл баркляда то ли кто которому он был назначен на бе  
регу дриисы так как не было ни одного большого села или местечка в окрестностях лагеря то все огромное количество генера  
лов и придворных бывших при армии располагались в окружности десяти верст получившим домам деревень по сю и по ту сто  
рону реки баркляда то ли стояла в четырёх верстах от государя он сухо и холодно принял болконского и сказал своим немцам  
ким в выговоре что он доложит немскому государю для определения ему назначения а покамест просите господа приёмыш  
а беанатоя курагина которого князь андрей надеялся найти в армии не было здесь он был в петербурге и это известие было по  
риятно болконскому интерес центра производящейся огромной войной занял князь андрей и он рад был на некоторое врем  
я освободиться от раздражения которое производила немцы курагин в продолжение первых четырёх дней вое врем  
я которых он не был никуда требовать князь андрей бездиль весь укреплённый лагерь и помощь своих знаний и разговор  
ов с сведущими людьми старался составить себе неопределённое понятие о вопросе отом выгоде или невыгоде этого ла  
герь остался нерешённым для князя андрея он уже успел вывести из своего военного опыта убеждение что в военном дел  
е ничего незначитса мые глубоко мысленно обдуманные планы как он видел это в аустерлицком походе что все зависит от то  
го как отведать не ожидаемые и немощные быть предвиденными действиями неприятеля что все зависит от того как кем  
едется в сёдело для того чтобы уяснить себе этот последний вопрос князь андрей пользуясь своим положением из знакомств  
а мистарлся вникнуть в характер управления армией и лиц партий участвовавших в нём и вывел для себя следующее поня  
тие о положении дел когда ес государь был в вильне армия была разделена на три армии находилась под начальством б  
аркляда то ли под начальством багратиона под начальством торма сова государь находился при первой армии и не вк  
ачестве главнокомандующего в приказе не было сказано что государь будет командовать сказано только что государь бу  
дт при армии и кроме того при государе лично не было штаба главнокомандующего а был штаб императорской главной кварти  
ры при нём был начальник императорского штаба генерал квартирмейстер князь волконский генералы флигель адютанты  
дипломатические чиновники и большое количество иностранных вое не было штаба армии кроме того бездолжности при го  
сударе находились аракеев бывший военный министр граф бенигсен починустарший из генералов великий князь цесаре  
вич константин павлович граф румянцев канцлер штейн бывший прусский министр армфельд шведский генерал пульг  
ла вный составитель плана кампании генерал адютант паулучи сардинский выходец вольцогеним многие другие хотя эти лица  
и находились без военных должностей при армии но по своему положению имели влияние и часто корпусный начальник  
даже главнокомандующий не знал качества человека спрашивали совета у него и другие об этом великий князь или а  
ракеев или князь волконский и не знал того или лица или от государя истекает такое приказание в форме совета и нужной  
ли не нужно исполнять его но это была внешняя обстановка существенный же смысл присутствия государя в этих лицах  
при дворной точки зрения присутствия государя в сёделах при дворных всем была сенон был следующий государь не при  
мал нас беззвания главнокомандующего но распоряжался всеми армиями людьми окружавшие его были его помощники а  
ракеев был верный исполнитель порядка и телохранитель государя бенигсен был помещик вilenской губернии  
и который как будто делал края в сущности был хороший генерал полезный для совета и для того чтобы иметь его всегда  
готовен а смену баркляда великий князь был тут потому что это было ему угодно бывший министр штейн был тут потому что он  
был полезен для совета и потому что император alexander высочайше оценил его качества армфельд был злой и ненавист  
ник наполеона и генерал уверенный в себе что он имел всегда влияния на alexandra паулучи был тут потому что он был смел  
и решителен в речах генерал адютанты были тут потому что они везде были где государь и наконец главноуправляющий  
о мучто он составил план войны против наполеона и заставил alexandra поверить в целесообразность этого плана и руково  
дил всем делом войны при пуле был вольцоген передававший мысли пуля в более доступной форме чем сама пульз резк

ийсамоуверенныйдопрезренияковсемукабинетныйтеоретиккромеэтихоименованныхлицрусскихииностранныхвособенностииностранцевкоторыеессмелостьюсвоейственнойлюдымдеятелиностисредичужойсредыкаждыйденьпредлагалиновыенеожиданныемыслибылоещемноголицвторостепенныхнаходившихсяприармиипотомчтотутбылиихпринципалывчислевсехмыслейиголосовэтомогромномбеспокойномблестящемигордоммирекнязьандрейвиделсладующиеболеерезкиеподразделениянаправленийипартийперваяпартиябылапфульиегопоследователиеоретикивыныверящиевточтоестьнаукавойныичтоэтойнаукеестьсвоинеизменныезаконызаконьоблическогодвиженияобходитпфульипоследователиеготребовалиотступлениявглубьстраныотступленияпоточнымзаконампредписаннымнимитеориейвойныивовсякомотступленииотэтойтеориивиделитольковарварствообразованиеиизлонамеренностькэтойпартиипринадлежалинемецкиепринципыольгогенвинцингероидругиепреимущественнонемцывтораяпартиябылапротивуположнаяпервойкакивсегдабываетприоднойкрайностибылипредставителидругойкрайностилюдиэтойпартиибылитекоторыеещесильнытребовалинаступлениявпольшуйсвободыотвсякихпередсоставленныхплановкрометогочтопредставителиэтойпартиибылипредставителисмелыхдействийонивместестемибылипредставителяминациональностивследствиечегостановилисьещеодностороннеевспореэтибылирусскиебагратионачинавшийвозвышатьсяермоловидругиеэтовремябылараспространенаизвестнаяшуткаермоловабудтобыпросившегогосударяободноймилостипроизводстваеговнемцылюдиэтойпартииговориливспоминаясуворовачтонадонедуматьненакалыватыголкамикартуадатьсябитьнеприятеляневпускатьеговроссиюинедаватьуныватьвойскупкретнейпартиикоторойболеевсегоимелдовериягосударьпринадлежалипридворныеделателисделокмеждуобоиминаправлениямилиудитойпартиибольшаячастьюневоенныеикоторойпринадлежалакакчеевдумалииговориличтоговорятобыкновеннолюдинеимеющиеубежденийножелающиеказатьсязатаковыхониговориличтобезсомнениявойнаособенностиакимгениемкакбонапартеегоопятьназывалибонапартетребуетглубокомысленнейшихсоображенийглубокогознаниянаукиивэтомделепфульгиеналенновместестемнельзянепризнатьтогочтотеоретикичастоодносторонниипотомуненадовольнедоверятьимнадоприслушиватьсяяктомучтоговорятпротивникипфуляиктомучтоговорятлюдипрактическиеопытныеввоенномделеиизовсеговзятьсясреднеелюдиэтойпартиинастоялинатомчтобыудержавдрисскийлагерьпопланупфуляизменитьдвижениядругихармийхотяэтимобразомдействийнедостигаласьнитанидругаяцельнолюдямэтойпартииказалосьтаклучшечетвертоенаправлениебылонаправлениекоторогосамымвиднымпредставителембылвеликийкнязьнаследникцаревичнемогшийзабытьсвоегоаустерлицкогоразочарованиягдеонкакнасмотрвьехалпередгвардиейувкаскеиколетерассчитываямолодецкираздавитьфранцузовипопаввнеожиданновпервуюлиниюнасилуушелвобщемсмятениилюдиэтойпартииимеливсвоихсужденияхикачествоинедостатокискренностионибоялисьнаполеонавиделивнемсилувсебесслабостьипрямовысказывалиэтоониговорилиничегокромегорясрамаипогибелиизвсегоэтогоневыйдетвотмыоставиливильнуоставиливитебскоставимидриссуоднотонамостаесяумногосделатьэтозаклчитьмирикакомжнокореепоканевыгналинасизпетербургавоззрениеэтоосильнораспространенноеввысшихсферахармиинаходилосебепоподдержкуивпетербургеивканцлерерумянцевеподругимгосударственнымпричинамстоявшемтожезамирпятаебылиприверженцыбарклаядетоллинестолькокакчеловекасколькочеловекаминистрайглавнокомандующегоониговориликакойонниестьвсегдатакначиналиноончестныйдельныйчеловекилучшеегонетдайтеемунастоящуювластьпотомучтовойнанеможетидтиуспешнобезединстванаачальствованияионпокажетчтооонможетсделатькаконпоказалсебявфинляндииежелиармиянашаустроенаисильнаиотступиладодриссынепонесшникакихпораженийтомыобязаныэтимтолькобарклаежелитеперьзаменятьбарклаябенигсеномтовсепогибнетпотомучтобенигсенужепоказалсвоюнеспособностьвгодуговорилилюдиэтойпартиишестыебенигсенистыговорилинапротивчтовсетакинебылоникогодельнееиопытнеебенигсенаикакнивертисьвсетакипридешькнемуилиудитойпартиидоказываличтовсенашеотступлениедодриССЫбылопостыднейшеепоражениеибеспрерывныйрядшибокчембольшеналадоушибокговорилионитемлучшепокрайнеймерескореепоймутчтотакнеможетидтиануженнекакойнибудьбарклайчеловеккакбенигсенкоторыйпоказалужесебявмгдуготоромуотдалсправедливостьсамнаполеонитакочеловекзакоторымбыохотнопризнаваливластьитакowejестьтолькоодинбенигсенсдьмыбылилицакоторыевсегдаестьвособенностипримолодыхгосударяхикоторыхособенномногобылоприимператореалександрелицагенераловифлигельадютантовстрастнопреданныегосударюнекакимператорунокакчеловекаобожающиеегоискренноибескорыстнокакегообожалростоввмгдуивидящиевнемнетольковседобродетелиноивсекачествачеловеческиеэтилицахотяивосхищалисьскромностьюгосударяотказывавшегооткомандованиявойскаминоосуждалиэтуизлишнююскромностьижелалитолькооногоинастаивалинатомчтобыобожаемыйгосударьоставивизлишнеенедовериексебеобявилоткрыточтоонстановитсявоглавевойскасоставилбыприсебештабквартируглавнокомандующегоисоветуясьденужносопытнымиитеоретикамиипрактикасамбылелсвоевойскакотрыходноэтодовелобыдовысшегосостоянияивоодушевлениявосьмаясамаябольшаягруппалюдейкотораяповоемуогромномуколичествуотносиласькдругимкаккмусосостоялаизлюдейнежелавшихнимираниявойнынинаступательныхдвиженийниоборонительноголагерянипридриссениигдебытонибылонибарклаянигосударянипфулянибенигсенаножелающихтолькооногоисамогосущественногонаибольшихдлясебявыгодудовольствийвтоймутнойводеперекарещающихсяиперепутывающихсяинтригкоторыекишлиприглавнойквартирегосударяввесьмамногомможнобылоуспетьвтакомчтонемыслимобыбыловдругоевремяодиннежелаятолькопотерятьсвоеговыгодногоположениянычесоглашалсяспфулемзавтраспротивникоегопослезавтраутверждалчтонеимеетникакогомненияобизвестномпредмететолькодлятогочтобыизбежатьответственностиугодитьгосударюдругойжелающийприобрестивыгодыобращалнасебявниманиегосударягромкокричатосамоеначтонаемкнулгосударьнаканунеспорикикричалвсоветеударясебявгрудывывызываянесоглашающихсянадуэльтемпоказываячтоонготовбытьжертвоюобщейпользытретийпростовыпрашивалсебежду двухсоветовотсутствиявраговединовременноописаниезасвоювернуюслужбузнаячтотеперьнекогда



абудетотказатьемучетвертыйнечаянновсепопадалсянаглазagosударюотягченныйработойпятыйдлятогочтобыдостигнутьдавножеланнойцелиобедаугосударяожесточеннодоказывалправотуилинеправотувновьвыступившегомненияидляэтогоприводилболееилименееисильныеисправедливыедоказательствавселюдиэтойпартииловилипубликрестычинывэтомловлениииследилитолькозанаправлениемфлюгерацарскоймилостиитолькочтозамечаличтофлюгеробратилсьаводносторонукаквсеэтотрутневоенаселениеармииначиналодутьвтужесторонутакчтогосударютемтруднеебылоповернутьеговдругуюсрединеопределенностиположенияприугрожающейсерьезнойопасностипридававшейвсемуособеннотревожныйхарактерсредизаговихряинтригсамолубийстолкновенийразличныхвоззренийичувствприразноплеменностивсехэтихлицэтавьсямаясамаябольшаяпартиялюдейнанятыхличнымиинтересамипридавалабольшуюзапутанностьисмутностьобщемуделукакойбыниподнималсявопросажужройэтихтрутнейнеоттрубивещенадпрежнейтемойперелеталнановуюисвоимжужжаниемзаглушализатемнялискренниеспорящиеголосаизвсехэтихпартийвтосамоевремякаккнязьандрейприехалкармиисобраласьещеоднадевятаяпартияначинавшаяподниматьсвойголосэтобылапартиялюдейстарыхразумныхгосударственноопытныхиумевшихнеразделяниодногоизпротиворечащихмненийотвлеченнопосмотретьнавсечтоделалосьприштабеглавнойквартирыиобдуматьсредствавыходуизэтойнеопределенностинерешительностизапутанностиислабостилюдиэтойпартииговорилиидумаличтовседурноепроисходитпреимущественноотприсутствиягосударясвоенымдворомприармиичтовармиюперенесенатанеопределеннаяусловнаяколеблющаясяшаткостьотношенийкотораяудобнапридвореновреднавармиичтогосударюнужноцарствоватьанеуправлятьвойскомчтоединственныйвыходизэтогоположенияестьотездгосударясегодворомизармиичтоодноприсутствиегосударяпарализуетпятдесяттысячвойсканужныхдляобеспеченияеголичнойбезопасностичтосамыйплохойнонезависимыйглавнокомандующийбудетлучшесамоголучшегоносвязанногоприсутствиемивластьюгосударявтосамоевремякаккнязьандрейжилбезделапридريسешиковгосударственныйсекретарьбывшийоднимизглавныхпредставителейэтойпартиинаписалгосударюписьмокотороесогласилисьподписатьбалашевиаракчееввписьмеэтомпользуясьданнымемуотгосударяпозволениемрассуждатьобобщемходеделонпочтительноподпредлогомнеобходимостидлягосударяоо душевитьвойнениародвстолицепредлагалгосударюоставитьвойскоо душевлениегосударемнародавоззваниекнему длязащитыотечестватосамоенасколкоонопроизведенобылоличнымприсутствиемгосударявмосквео душевлениена родакотороебылоглавнойпричинойторжествароссиибылопредставленогосударюипринятоимкакпредлогдляоставленияармииа

## Код програми:

```
package com.company;

import java.io.*;
import java.util.*;
import java.util.stream.Collectors;
import java.util.stream.Stream;
import java.io.FileReader;

public class Main {

    public static void main(String[] args) throws IOException {
        String text = readText("C:\\Users\\katch\\Documents\\кпи\\крипта\\19.txt");
        String cText = text.replaceAll("[^а-я]", "");
        ab(cText);
    }

    static String readText(String path) throws IOException {
        StringBuffer sb = new StringBuffer();
        String res = "";
        try {
            BufferedReader in = new BufferedReader(new FileReader(path));
            String str;
            while ((str = in.readLine()) != null) {
                sb.append(str + " ");
            }
            in.close();
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```

```

        res = sb.toString();
        return res;
    }

    public static int gcd(int a, int b) {
        if (b == 0) return a;
        return gcd(b, a % b);
    }

    public static void bigramm(String str) {
        Map<String, Integer> map = new HashMap<String, Integer>();
        String[] words = str.split("(?!^)");
        for (int i = 0; i < str.length() - 1; i++) {
            String s = words[i];
            String s1 = words[i + 1];
            String s2 = s + s1;
            if (!s2.isEmpty())
                if (map.containsKey(s2)) {
                    map.put(s2, (map.get(s2) + 1));
                } else {
                    map.put(s2, 1);
                }
        }

        Map<String, Integer> top;
        top = map.entrySet().stream()
            .sorted(Map.Entry.comparingByValue(Comparator.reverseOrder()))
            .limit(5)
            .collect(Collectors.toMap(
                Map.Entry::getKey, Map.Entry::getValue, (e1, e2) -> e1, LinkedHashMap::new));
        System.out.println(top);
    }

    public static int inverse(int a, int m) {
        int t = 0;
        int T = 1;
        int r = m;
        int R = a;
        if (gcd(a, m) != 1) return 0;
        else {
            while (R != 0) {
                int q = r / R;

                int newt = t - q * T;
                t = T;
                T = newt;

                int newr = r - q * R;
                r = R;
                R = newr;
            }
        }
        if (t < 0) t += m;
        return t;
    }

    public static int index(char c) {
        String string = "абвгдежзийклмнопрстуфхцчшщъыэюя";
        char[] ch = string.toCharArray();
        for (int i = 0; i < string.length(); i++) {
            if (ch[i] == c) {
                // System.out.println(i);
                return i;
            }
        }
    }

```

```

    }

    }
    return -1;
}

public static char indexNew(int number) {
    String string = "абвгдежзийклмнопрстуфхцчшщъыэюя";

    char[] ch = string.toCharArray();
    for (int i = 0; i < ch.length; i++) {
        if (i == number) {
            System.out.println(ch[i]);
            return ch[i];
        }
    }
    return 0;
}

public static void topBigr() {

    String[] topY = {"уф", "иж", "ьи", "кщ", "хф"};
    for (int i = 0; i < 5; i++) {
        System.out.println(topY[i] + " = " + funcY(topY[i]));
    }
    String[] topX = {"ст", "но", "то", "на", "ен"};
    for (int i = 0; i < 5; i++) {
        System.out.println(topX[i] + " = " + funcY(topX[i]));
    }
}

public static void ab(String criptedText) {
    int[] closeB = {609, 254, 814, 335, 671};
    int[] openB = {545, 417, 572, 403, 168};
    int y = 0, x = 0, a = 0, b = 0, s = 0;
    for (int i = 0; i < 5; i++) {
        for (int j = 0; j < 5; j++) {
            for (int k = 0; k < 5; k++) {
                for (int l = 0; l < 5; l++) {

                    x = inverse((closeB[i] - closeB[j]), 961);
                    y = openB[k] - openB[l];

                    if (x < 0) x += 961;
                    if (y < 0) y += 961;

                    a = (x * y) % 961;

                    b = (closeB[i] - (inverse(a, 961) * openB[k])) % 961;

                    if (a < 0) a += 961;
                    if (b < 0) b += 961;

                    prov(decrypt(criptedText, a, b));
                    String c = String.valueOf(indexNew(a / 31));
                    String c1 = String.valueOf(indexNew(a % 31));
                    String c2 = String.valueOf(indexNew(b / 31));
                    String c3 = String.valueOf(indexNew(b % 31));
                    System.out.println("(" + c + c1 + " , " + c2 + c3 + ")").toString();
                }
            }
        }
    }
    // System.out.println("a = " + a + " " + "b = " + b);
    // System.out.println("-----");
}

```

```

    }
    }
}

static public int funcY(String ab) {
    char[] newAB = ab.toCharArray();
    int a = index(newAB[0]);
    int b = index(newAB[1]);
    int y = a * 31 + b;
//    System.out.println(y);
    return y;
}

public static void prov(String str) {

    boolean isContain = str.contains("кщ");
    if (isContain == true) {
        System.out.println("Невозможное сочитание : кщ");
    }

    boolean isContain1 = str.contains("шя");
    if (isContain1 == true) {
        System.out.println("Невозможное сочитание : шя");
    }

    boolean isContain2 = str.contains("щц");
    if (isContain2 == true) {
        System.out.println("Невозможное сочитание : щц");
    }

    boolean isContain3 = str.contains("вй");
    if (isContain3 == true) {
        System.out.println("Невозможное сочитание : вй");
    }

    boolean isContain4 = str.contains("гю");
    if (isContain4 == true) {
        System.out.println("Невозможное сочитание : гю");
    }

    boolean isContain5 = str.contains("жш");
    if (isContain5 == true) {
        System.out.println("Невозможное сочитание : жш");
    }
    boolean isContain6 = str.contains("aaaaa");
    if (isContain6 == true) {
        System.out.println("Частое повторение : a");
    }
    else if (isContain == false && isContain1 == false && isContain2 == false && isContain3 == false && isContain4
== false && isContain5 == false && isContain6 == false)
        System.out.println("Наш текст");
}

}

```

**Висновок:**

Ми засвоїли методи частотного криптоаналізу на прикладі розшифрування афінного шифру біграмної заміни та опанували прийоми роботи в модулярній арифметиці.