

Міністерство освіти і науки України  
Національний технічний університет України  
“Київський політехнічний інститут ім. Ігоря Сікорського”  
Фізико-технічний інститут

**Лабораторна робота № 3**  
з предмету «Криптографія»  
«Криптоаналіз афінної біграмної підстановки»

**Виконали:**

Студенти 3 курсу,

ФТІ, групи ФБ-74

Люшняк Катерина, Харченко Владислав

**Мета роботи:**

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

**Порядок виконання роботи:**

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.

П'ять найчастіших біграм в ШТ	П'ять найчастіших біграм в російській мові
ШЭ	СТ
ЬЭ	НО
ЧП	ТО
ИИ	НА
ПЭ	ЕН

В результаті роботи програми ми знаходили багато пар ключів. Для того щоб знайти відкритий текст ми підставляли кожну пару у функцію `decrypt()` та перевіряли отриманий текст. Звісно не кожна пара ключів нас задовольняла, тому багато де при розшифровці ми отримували не відкритий текст, а набір символів, який не має сенсу. Що знайти саме ту пару ключів ми перевіряли отриманий текст на наявність в ньому символів, які не можуть зустрічатись в мові, а саме ми використовували: **аь, оь, ьь, йй**. Саме ці біграми дозволили нам віднайти справді відкритий текст та відкинути варіанти, які нас не задовольняють.

Для дешифрування було знайдено **a** та **b**, які дорівнювали **144 та 89**.

## Шифровний текст.

пэчпнергегчэжжкойэбгурывсбиобьэбддбнбшбфужэжжцююпюяфхыкщпржэуюжшпуэймджыжггэирчалмхбоыхышбкэмыащбьепипмгубивжвгз  
ждмойсюшэшэззэаивагхдщпрыхэшишпхлхкхблсдлгспзпбмбчщненьхэбозьыхыксбжагуытфчэээичкчххэбдббсюшэябюфээжисслсжпцязе  
жфьюпмьчещпудскыякэзьыхыккыоыяббытжцююпюяууупжжхлфлюююгапирчалмхбфждмойдгоыхышбщгжчиимнэухщшэвифоюягаещгоэмуачс  
ээохзшэгуэпирцбйсчяхбтфмнцгьихбьбьвимэцсшьщящпнгвфсэирачьгыйпоидуюлбуыгдсшьщявихбупукпэтгхгчпжигусциэшйюоцжюытфттязщпо  
ээемыягхбченгегкичищпссцжгсцжэоцпюжжпагккыучыхбчзшйпцюящгзэпгпцьфийуэзгшэвфүэргегяещгбшэлыубжыббсэпсцжэобыбблыротж  
чюямразежэоьэхгцьоэьэычпаглеыгхдчэушсбртбечкщпчцьбаейийюшэьэхэюэяэьждмбдрыдгйфупщпщпэыйсфьюгоэьийгцгмбтрюозсесесчгрт  
юбрпиротртпэндэьрбежыячцькогпугпирчсубюытфогзззчиимещгуюткээфхмяуиисэкшидыбнгньаеюпюящищпчялкжэжжкойэбщкыучыхбймхоц  
жюыизпэчпнейбьэтгсыиэгутсубоншплктквиирвацяднийюпмьмиуьвимэжххоэаьрырэщглдцэщэбщбщыдэледпрыббшэртщэифькиэкжжкой  
мбгутсцжйсцкэбздэбьбзооэзэаьчббжхофьогбйсукохчптбюкщпржнвизгсцяежжчнчкщпржигогргйфщыхбмбщукщпгхмяеюыкчиихоапыои  
рмыаьхыыщвидбиямнагнгсзтфяеиихоитфлержщэомфнцэгзньаефьфьэошьбдгркснефрржыурдщыиэнищпссцжардятыучыхбфбоьчэшйиэфь  
хылытфсзусямдшпткрьцюшэоьчэшйиэшэбуэеыйжфьшэусфьоэгупнпжткогидшйшонечаяииюпохебсжитуэшидэшеюяусчямдшьдуюяфоюя  
шпмьорпюсдебсигсубдпсэбсубонмеймщпудскпжхофьфинечпегхгнхшэлыубжыббхбуэеыбрдяэгйеызмпжгувишэббймщыиэпэтьобежсеюя  
щпмбыйфиниэсынмкщпржигмычэлымбчщкбтыхязчыяагхдьеюецятэфирццямяемещпэдэаеагчщжэурдяежкбэеоишжщпбчпойкксщфьэх  
кшйнсфьхыаяииоыоиииссэсчяачииагэддгмбхгнийууэвсюгзпэувилсдпгсчящцыляеохежжчхбвюскхопэнирццяуьлкыучыхбхсчхрдяежибпусчяо  
лфегомецяфьоооэыиыюыиэзылфссубшймбсэнімжббгойсэнийюямоыяцлхообфямесэцжубьежфьгжибыяфьспнеемтдсоиисдгщгизииуыгжыгхб  
щкщпржыгдэудэаегфирццяфеохрйфжфьшэьемоылыяоэуюещцосэсчяачииагусчямддгюфежэоцзсзюонечьямеачзббжиогегбидеыгниоххя  
зшйцэжймоыуцшэмысэыапсемулсубнгзьфбысукижбпееохскеэзсдчымбщптбвфрйэмысийухаачрийщфьюопжчдгнийуьэмбэбхгсбуюпт  
кзбхгсбубежжжиыурысоьхсыгэзсдмяиичздэежнеачфыцьяиэиоххщпгэбепцжьньнедуюмткртхгбгбчпмычпфхщцыкизуйпэрэохзыдбыйцссм  
еиэнжхоскщлсчярыдгюфьпщпщпчптсшпюящиьхэцэебдрлхтэидгхыфохьхышэийуежцонечьямеаагрядыийвспэчпйусеьыяйунгйхд  
рйлытфпгйсуккбтфсзобепубгэлтфээфясефямесэмкыпгфжйыщбщдшэуэыиужобжиьежхлсецшэорюкюодмрцгьюобпьмбюююгмбупжэзс  
дчпыпшэшэвфүэьшэхдупвихоирдянефнцюпвбхэуцуюпохьепжбойщпцпэпкглфүэдсбирйжчюяобежмнцюяукэуэйимрюооегизэдупцюяксиэ  
ьбшэрывьюггдапцэпэгхдэоиисэхдгхгдгмдшэжкэурюшэежмнцюянегэиэздчппжцясзшйтфдгщгмбзгрдщытфйриряганцоэюяходушпюэлеыг  
ярмбюыплгунгогаирццямеьыюяфьшэвяпсцююгтбвфйтыоэезситкэучплыйсчямьббьбэьтгнбрыббкэебфьбщпшйлыяьээгжющфьюопжфбвжш  
щмннийфлмнуэщывофжнеэшэвсубкнсубрыхэзсдятабфвдгшвмиуобчпеглядпгспэтббикжщпржхэзгвгзшйиэфелмэблеишзрйчыкзфйрдя  
хщыьпжыушэвфүэьшэхдупйюшэшйнслзрйрящцжлкткежмлыеьэныжучзчпузакждлеишхзбьшэхдупнелеишзоынусэгшйиэюыиэхимео  
хскдмшпсцшэвсифьэвфхэлыалшьгсубрытыхбгущпюмытфежнезыенщцшьюежнезыепдзэрфжцяобиэсынбгбфкпсчюбуэшждьэвфскмнчы

сэшжфьшэусэухбцдгшвмицшпэушцшэвиуцсжнйпоииеечптсрюгхбечьпэуьогнкфьтгхбпезнббчпмыжигусцйсмьтбтфсэйсцжсссешбббсэьгуыя  
мофунюскхопэоыуэшэойорлмчщнеозуюддгзяпсдпарсцкчпжсцлссеезэдгшвмицпчптсцьяоцяолрбфывфкгэвжшгьйкэизтфщпчптсыякэйо  
убтьлдцгежмрмбюыяьликдтьчибишмьхбиыищкбняхсмеиэнжхоиыдергцеьхмьсыбужьяфяржпеещгйфлмсэноячщкбнячесэщфойрыкдзнгфы  
шйеибвфойтрчжяьчэсогухцпэхэряапсцщомежэпаордемыучщпюяциирчжзупсмеиэнжхоскагеаеиюсхпоэоычпузэмбюблырыббжжэосефрю  
псцщощпеыскщпэуыяцлхофугдгцгнйуэиэибялчщфььжюкысэгьээхээсопяямбфеубпэчпнейсукпэтбогавфчпздгуйбуээиэцйээжббпэббвфжйиуи  
бнгнсцоссржачирийшиуэуиджжьюлцяхлчкэугшсвцжмньэхкуйяжирйббыыупспэчэвчмешбббсзщпгягжгосешбжеипзриймуьэбйабпхчэсог  
утыгхкпэчпнеэзнжвшймипзруьзйсымбьэяхщмыесксцкбгшсвцжмьтырытынснопэхифьббыыпбизнескщфьмыцгхбьязйсйнигибуалхыпгпэч  
пнеэебщыяьолвгюмткщпржхттыогрыеыоэфымдубыпидзксбхяюлцязгкибушпюящикбажэорыьэфябошкетзоыээиэчэгэгшсвцжйбвфжиткщпрж  
хюыцьрзуэизэггэгшсвцжьпщпкгчпоыявшпыапапхуцяйцкзгфыкилсфьсдяблхтхусчяхрдяогргйфозфицииобпичкчянтогигушйдичкчянхэофиц  
лиобдоиийшьнеыьгупяапшэхдоытыывфвичиппжцясзозэьгуьэвжчашпифьшэзэдчкткцзажизрдяаяорюгшесзгэгшсвцжфюозьийугдбыббжойч  
жисктхмьтырыфйлыдикиаииисцпэурывьцяхысэьрыхсиээбоышйеычгжулсыяуфжыьскмнрыпииюшэдсиэбзгшйцънецжкгэшиицжцяэуыу  
ескбуэчпптсукчэчпохрипоегикифьэбжойчжисктхмьтырыфйлынсфьсдэюжьгэуэгуэшоэойжецеюяоымящпжиьоэмняепннгйсэдгдсочплмырых  
сщививбаибуфжбозуьэьгпешпткчжфьшэьбдсытжувьскдмжиапчялхвицщвичщнержыяусоаецжсоииагэоэчпржажойчжисксщививикспээбтбт  
пёохгиздгрыуэшэойнъйыбцдпсцщпэгучжувьскдмщентьнщпфбзгоытгегшееммыоытфпэчпнеэхяйыьобгясвуэгбгфырырвситхсицяэалеы  
гхддэиаеиисэхдлсжпшцшэмытырыфйлычеыгниигежкбфляеачэьщфышжбпрычббыэешемьтжувьскдмщетзоэвпржфнвибуояоычпчялкжэщ  
йфифьэбупемоххкткэспэшэьцэыбфимеохгдэьгузгхыбкткыйээцгдэжэджячшпвбмьтырыфйлытфпсцпэуггхдзгымеясызмьтырыфмвжебау  
эгэзгыжмеыясзшыьужойчжисктхуэшэойнълекбббыьукэоащкэалеыгдсубнйнккиймуэоызбцыцьмихомблэрпсцхуэуэныжувьскдмщецюпыхб  
юггэвпысьэнлчяхлцжфьшэеучэыьущпегдибичщнелсцжнйиткисэиэбзгуэшидшыхуэлымбэвчюышйеышйтфдглищптктзудхыхбиыюпьсэхууп  
ыгцгмбмыуесктхсещеюялекбёоинефхшэьпвжитксцшвиуусциэьэнгняенешплкпэтгрияцяоянещкоынсгзтфуэшэойордякэуэизьбээгчщцодуця  
пэчпнефьхывфйрбзгээфясеюоаплкткшйгнлюямыуесктхьмящпжииникбогуэшэойуёоюянюшэзгээфякэхглфозцоюлеуопмьхсцпэушцшэупкб  
рдаемхоюяцовижирйбжцоююпямьбвцфечпшжьгэуэгуэуошлбпнгизжяжэдэньаеиисплмдегьшээммпсцшсцшэозпфхдбмбзгоэпфхдзэьхыс  
ээмдбсиээбкдзгытбщгеыздсфцыщпчцьааеткткыоээабгйлыпплсплэчгжулсыяцбчпциаржпэмрцгцшйизежжифьюпсптхтцггпздпсцпэуыг  
рпбпоыоэыгуэлшпмьоэмнгогмзшйзгшэвфуэргбтджшпбисснэюяшйфыцгобвфжикхоячпюшэгшдбэгэшиициорпэгэщывфдбрыэьчппжцясзшй  
эьчпмеюплкюобимрюогсцотынбсдежцочяюышодушпжфьшэьбдсыпмвжебауэгэсэвизгсдмцялекнубнубюгэяхбобыпядцгбуюялсжпвисцяу  
пйюшэгжувьскдмдэгнъаенецашспэжхмэюгхбчхлчщжэидебфьбэшэхдоычэшйиэнгьитфбгцшэзгэзшиуеьгофсзкигхуыуэхбнгёиизуиткзусцжиа  
пскдмцяыявбрыуччмешбкщпэчпнейиимытбзььждмгэозомвжебауэгэхчяяцбфжпрхлрыпсцотгязьэлпщкиэьэпосбскпсгубппткчячпсэчэс  
очкьэюогцрбвфжинйкгмбжойчжисктхггуыуццжлмизтфббкдэбвфжикжастзэьнжпмпсубпюыхксыеындчжпжфьшэтбнгльуэегихлюяоэмлпбсыг  
еяодгчпчкржцуюдфпюодмэзмымбюфышбцэтфьээдшблфбщыйфыщиюубэкишпыуцыйфыщиюубэкизрдяячииксчяуэозгэчэзпржыучяцотзг  
элэглфрымигурьыоуэшэпэпоукшэйчиныясзусчяолоэоукшэубмбщпшгэупвирбтгцегжьяеыякэммпсцшсцшэзгэогнсчжоэуегкзцгхбфшймызаш  
цшпмьяээиэчшчиохоэщбюгуелмнгтыдэщэдсубыдбыюуэвсчямдфжусэчпооукшэмыфоюяцяуьюэшыйийеужэотгшэнлбпуктгсошщыьпжск  
букэжббгмыббпэчпнеоычбкднсеыцкмбпиятыдэщэрямеидвкыьдгжыббпсцлюиябвфжийууоцжувьрычйлыяьгссцэзщбуоссэзэжастзьэрдэбуы  
ялбучэсогупгусэогдгхгыймегекбипжольгээпоцящкбубучяхзбуфжфьшэвпючнгжовьлкткнеуычяхбхсцжщпнепжсецяшьоэхбусукжибпохуэьц  
тгртегекщпржотчпзуеычбюбшэнкхоукшэмызчордясцяоянещкизтфгшсвцжнещыйфыщиюубэкиксчяоыртрюяукжтзэгэнкмеуэхпсцйгжиксцэицс  
сдбйгибнгёиуысцжэозгхдфйихлфжужокеыыкгузчвгчэзпржйсцяэтыыбвгпэчпнеибвфжийуэьгжчцирийуеььюяйусефьеясвбичзббмниншпэуоэж  
ясеуэшишпсбфыеуьрыуэуеьыюягуьущзюфскдмцяпэчпнемеюшэлглыапоржцлюпткюпцапаимнгэпжжхтоынздгытээдбогщыйфхшиюубцэк  
ичсеытфиилмкскрцрытфщпдгэымбгэиэьбпэчпнеибвфжийуьэйсэлыажинхэбшчякууоортэхбзоыидсыяьюжэусэчпубпжвбшгымннерйээфям  
рсцжгуиюпфуюкпэссеытфмэхбьэжмрдяемксцжщржцомдупирчсжмэнгтфсзэеуцяиилкэушдеыэцккииксчяэжггэдгюфдэуиохлечцуэыикс  
ышэкзбнйгигбнгмбгжкэжббгмьхщмычерыгпцбхбтыупвионщпюягдчптсрюмьоэгуьышэщыйфыщиюубэкиюдчптсыяимеегкзлеотюрмдупирл  
дэьгжорюпугуэтгчпембимеььчбймиошэюмбимеььуэйжфьшэтбывабьяэээгфнямеидвкпсубзгфлчщнежтчаивявбуукпэрбоынгмбэдцэссеытфу  
емыязэубисэдсцйгмызачыакэглфчэчпцяюфьмдгдаецжыбдгиохоздеьэоёеысукоймбьээсэпофьхымббыээлыыцкьэнжорувпсчятдйхкфжэ  
усбьэежфьсещыйфзщиюубэкипржпанемшхуэжешчпчяябмбюфукчявигзплсегйярщцяфхдбчпхсэдэоздсеышэяцшэшйирзбмьтфежюьяьфии  
гиднккшэьэуиачбьэекеыцйлыюгкеишгэкшцшэшйзгшйизгйпэплсейьэымбимеэлсецяуксэупироизояукшэирщыьблыяупнхясвггузчрщэ  
шйвизгежфькдцэрчпмеспвггэозэубеыщыйфыщиюубэкипжирүшэьычпмбозаяфртзюфвиюпткйсюпцэпэфьэхяорььдэниохсдбзгвфгзщыйф  
ыщиюубэкиэаечццягшсвцжовьчэчэзпржтсубхязчюпмьчешгээцгьржпвбвигтязьэююягуэуобиссбмбидмдегтытфчпбиапчпкбинешйишэв  
фуэгжсецзрдяшпчтзжнпмоыцшзэвфгшйизегшбтфуэотбгэьчмбзгюжсукыгбэыуенпжүецофрдячпчялхльтфчпкбинесэгоэвсубд  
згордясжэжгеыбшьхыалжичпздэбдбтфлеохчпкткиймудияфнскржщпчбббзгдэьгудбчпйужиссжзббидхгкупжвбшгыжмннерйэьмэжбгой  
рытыиэюфнгнъаеюпюяшиирдясеьпщпдхгцертляиищещыйфзщиюубэкиюоачапмэжбгойуэшэойрбнжцяймксцжщржцоуэжерыгпбьуэпэдж  
фьяяобнжсбргегжячкыээлыидьэгцжиюзюфриягхдоычппэиитпннчасебилзтыщыйфхшгыжмннесэхупжлзшгыжмннеоытбешцззукидгцниохх  
ыуэбрюгпжафхгдупсеохээиэнгфькчзеыпцуьтфгурыпишьхымыеынюфвиуюжщешпбюшэгэчткхбсцуеосэпэггеыежкчячэльвисэнотбгхбшь  
чыялчщембифххдуюиэокзрдяшпчялкжзуиуьзнпжпрдяряолюещггэсэмымуэлсешпуггэгзыьрглымбпсцшпэупрдяржэлиисцшэвизрюоаьэсцж  
эосэтгсйтфбыуэыкчячхдпэчпнеэбдбдбэозньхырыхбэыйсекичщржэутслспэибупжжтшгыжмннекдмымуэлшпоомеозеоефрлмбыуымыскдмц  
яеозыьэдьйцяыялкткдлпнещгупгы

**Відкритий текст:**

ростовпередоткрытиемкомпанииполучилписьмоотродителейвкоторомкраткоизвещаяегооблезниаташииоразрывескняземандреемразры  
взтотобсянлиемуотказомнаташиониопятъпросилиеговыитвотставкуиприехатьдомойникалайполучивэтописьмоинепопытасяпроситьсаво  
тпускилиотставкуанарисалродителямчтооченьжалеетоблезнииразрывенаташисеегенихомичтоонсделаетвсевозможноедлятогочтобыиспо  
лнитихжеланиесонеонписалотдельнооббожаемыйдругдушимоейписалоничтокромечестинемоглобыудержатьменяотвозвращениявдеревн  
юнотеперьпередоткрытиемкомпаниябысчелсебябесчестнымнотолькопередвсемитоварищамиинопредсамимсобоюежелибыяпредпочелс  
воестачиесвоемодолгуилилюбоикотечствунотэтопоследняразлукаверьхотототчаспоследнейнежелиабудужививселеннойбоябпродувсеипр  
илечуктебчтобыприжатьтебяуженавсегдакмоейпламеннойгрудидействительнотолькооткрытиекампаниизадержалоростоваипомешалоэму  
приехатькакнобещалиженитьсясанасеотрадненскаяосеньсохотойизимасосвяткамиилюбобвыюсониткрылиемуперспективутихихдворянск  
ихрадостейиспокойствиякоторыхоннезналпреждеикоторыетеперьманилегоксебеславнаяженадетидобраястаягончихлихидесятъдвадц

тьсворборзыххозяйствососедислужбаповыборамдумалоннотеперьбылакампанияинадобылооставатьсяявполкуатаккакэтонадобылотоникол  
йростовпосвоемухарактерубылдоволенитойжизньюкоторуюонвелвполкуисумелсделатьсебезужизньприятноюприехавизотпускардостнов  
стреченныйтоварищаминиколайбылпосылалзаремонтомизмалороссиипривелотличныхлошадейкоторыеерадовалиегоизслужилиемупохва  
лыотначальствавотсутствиегоонбылпроизведенвротмистрийкогдаполкбылпоставленнавоенноеположениеисувеличеннымкомплектмоноп  
ятьполучилсвойпрежнийэскадронначаласькампанияполкбылдвинутвпольшувывадалосьдвойноежалованьеприбылиновыеофицерыновыеел  
юдилошадииглавноераспространилосьтовозбужденновеселоенастроениекотороесопутствуетначалувойныириостовсознаваясвоевыгодноепо  
ложениевполкувесьпредалсяудовольствиямиинтересамвоеннойслужбыхотяизналчтораноилипозднопридетсяихпокинутьвойскаотступалиот  
вильныпоразнымсложнымгосударственнымполитическимитактическимпричинамкаждыйшаготступлениясопровождалсясложнойигройинте  
ресовумозаключенийистрастейглавноштабедлягусаржепавлоградскогополкавесьэтототступательныйпоходвлучшуюопорулетасдостаточны  
мпродовольствиембылсамымпростымвеселымделомуныватьбеспокоитьсяинтриговатьмоглиглавнойквартиреавглубокойармииинеспра  
шивалисебякудазачемидутеслижалеличтоотступаюттолькопотомучтонадобыловыходитьизобжитойквартирыотхорошенькойпаньежели  
иприходилокомунибудьголовучтоделаплохитокакследуетхорошемувоенномуучеловекутокомуэтотприходилоловуларястеласьвеселине  
думатьообщемходеделадуматьосвоемближайшемделеначалавеселостоялиподвильнызаводязнакомствасполскимипомещикамиожжи  
даяотбываеясмотрягосударяидругихвысшихкомандировпотомпришелприказотступитьксвенцанамиистреблятьпровианткоторыйнельзябыл  
оувезиственцаныпамятныбылигусарамтолькопотомучтоэтобылпьяныйлагерькакпрозвалавсяармиястоянкуусвенцанипотомучтовсвенцанам  
ногобыложалобнавойсказаточтоонииспользовавшисьприказаниемотбиратьпровиантчислепровиантазабиралилошадейизкипажиковры  
упольскихпановростовпомнилсвенцаныпотомучтоонпервыйденьвступлениявэтоместечкосменилвахмистраинемогсправитьсясперепившим  
исявсемилюдьмиэскадронакоторыебезеговедомаувезилипатьбочекстарогопиаотсвенцанотступалидальшеидальшедодриссыиопятьотступи  
лиотдриссыужеприближаяськрусскимграницамгоиюляпавлоградцамвпервыйразпришлосьбытьвсерьезномделеогоиюлявночьнананунеделаб  
ыласильнаябурясдождемигрозоюлетогодавообщебылозамечательнобурямипавлоградскиедваэскадронастоялибывакамисредивыбитогодо  
ласкотмилошадьмиужевыколотосившегосяржаногополядождилиливмириостовспокровительствуемымимолодымиофицерамиильнымсиде  
лподогороженнымнаскороуюркушалашикомофицерихполкасдлиннымисамипродолжавшимисяотщекздившийвштабизастигнутыйдожде  
мзашелкростовуюграфизштабаслышалиподвигаевскогуюофицеррассказалподробностиалтановскогоосраженияслышанныеимвштаберостов  
пожимаясьшеейзакоторуюзатекаловодакурилтрубкуислушалневнимательноизредкапоглядываянамолодогоофицераильнакоторыйжалсяо  
колонеогофицерэтотшестнадцатилетниймальчикнедавноступившийвполкбылтеперьвотношениикиколаютемчембылиниколайвотношении  
икденисовусемьлетомуназадильинстаралсявовсемподражатьростовуикаженщинабылвлюбленнегоофицерсдвойнымисамиздржинский  
рассказывалнапыщенноотомкаксалтановскаяплотинабылафермопиламирусскихкакнаэтойплотинебылсовершенгенераломраевскимпоступо  
кдстойныйдревностииздржинскийрассказывалпоступокраевскогокоторыйвывелнаплотинусвоихдвухсыновейподстрашныйогоньиснимиряд  
омпошелватакуростовслучалрассказинетолькоконичегоноговорилподтверждениевосторгаздржинскогоонапротививиделчеловекакоторые  
йстыдилсаятогочтоемуиуассказываютахотяиненамеренвозражатьростовпослеаустерлицкойигодакампанийзналпосвоемуособенномуопытучт  
орассказываваявоенныепроисшествиявсегдавруткакасамонвралрассказываваявотрыхонимелнастолькоопытностичтозналкаквсеисходитна  
войнесовсемнекакмыможемвоображатьрассказыватьпотомуемуненравилсаярассказздржинскогооненравилсаясамздржинскийкоторый  
своимиусамиотщекпосвоейпривычкинеизконагбаснадлицомтогокомуонрассказывалитеснилеготвесномшалашеростовмолчасмотрелнан  
еговопервыхнаплотинекоторуюатаковалидолжнабылабытьвернотакаяпутаницатеснотачтоежелираевскийивывелсвоихсыновейтоэтонинач  
огонемоглоподействоватькромекакчеловекнадесятькоторыеебылиоколосамогоегодумалростовостальныеиенемогливидетькакискемшелраев  
скийпоплотиненеотекоторыевиделиэтонемоглиоченьвоодушевитьсяпотомучтоимбылозаделодонезныхродительскихчувствраевскогого  
датутделошлоособенношкурепотомоттогочтовозымутлиневозымутсалтановскуюплотинунезависеласудьбаотеческанамописываю  
тэтопрофермопилыисталобтызачемжебылопринеситакуюжертвуипотомзачемтутнавойнемешатьсвоихдетейбынетолькопетюбратанепов  
елбыдажеиильнадажеэтогочужомненодоброгомальчикапостаралсябыпоставитькуданибудьподзащитупродолжалдуматьростовслушаяз  
ржинскогонооннесказалсвоихмыслейониэтогожеимелопытонналчтоэтотрассказодействовалкпрославлениюнашегооружияипотомуна  
былоделатывидчтонесомневашьсявнемтакониделалоднакомочинетсказалильинзамечавшийчторостовуненравитсяразговорздржинскогоич  
улкириубашкаиподменяподтеклопойдуискатьприютатакжесядождикполегчеильинвышелиздржинскийуехалчерезятьминутильиншлапаяпо  
грязиприбежалкшалашууарростовидемскореенашелвоттутаговдвистикорчмаужтадазабралисьнашихотьпосушимсямарьягенриховнатамм  
арьягенриховнабылаженаполковогодокторамолодаяхорошенькаянемканакоторойдокторженилсявпольшедокторилиоттогочтонеимелсредс  
твилиоттогочтонеимелпервоевремяженитьбыразлучатьсмолодойженейвозилеевездезасобойпригусарскомполкуиревностьдокторасдела  
ласьобычнымпредметомшуткимеждугусарскимиофицерамиростовнакинулплащцкинулзасобойлаврошкусещамипошелслиялинымгдерас  
катыаясьпогрязигдепрямшлепаяподухавшимдождемвтемнотевечераизредканарушаемойдалекимимолниямириостовтыгдездеськакова  
молнияпереговаривалисьонивпокинутойкорчмепередкотоуюстоялакибиточкадоктораужебылочеловекпятьофицеровмарьягенриховнапол  
наябелокураянемочкавкофточкеиночномчепчикеиделавпереднемуглунаширокойлавкемужеедокторспалпозадиееростовсильнымвстрече  
нныевеселымивосклиданиямихотомвошливкомнатуйдауваскакоевесельесмеялсясказалростовавычтозеваетхорошитакитечетснихгостин  
уюнашунезамочитемарьягенриховныплатьенезапачкатыотвечалиголосаростовсильнымппоспешилинайтиуголокгдебыониенарушаяскромн  
остимарьягенриховнымоглибыпеременитьмокроеплатьеонипошлибылозаперегородкучтобыперодетьсяноваленькомчуланчикенаполняя  
еговесьоднойсвечкойнапустомаящикисиделитриофицераграивкартинеизначтонехотелиуступитьсвоемостомарьягенриховнауступиланаврем  
ясвоюобкучтобыупотребитьееместозанавескиизаэтоизанавескойростовиильнспомощьюлаврушкипринесшеговкосьнялимокроенадел  
исухоеплатьеvразломаннойпечкеразложилиогоньдосталидоскуиутвердивеенадвухседлахпокрылипопонойдосталисамоварчикпогребеципо  
лбутылкиромуипопросивмарьягенриховнубытьхозяйкойвсестопилисьоколонеектопредлагалейчистыйносовойплатокчтобыобтиратьпре  
стныеручкиктоподножкиподкладывалейвенгеркучтобынебылосыроктоплащомзанавешивалокночтобынедулоктообмахивалмухслицаеему  
жачтобыоннепроснулсяоставитьегоговориламарьягенриховнаробкоисчастливоулыбаясьонитакспитхорошопослебессоннойночинельзямарьг  
енриховнаотвечалофицернадодокторуприслужитьсявсеможетбытьионменяпожалуеткогдапогулируюкурезатьстанетстакановбылотолькотри  
водабылатакаягрязнаячтонельзябылорешитькогдакрепикилинекрепокчайивсамовареводыбылотольконашестьстакановнотемприятнеебыло  
поочередистаршинствуполучитьсвойстаканизпухлыхскороткиминесовсемчистыминогтямиручекмарьягенриховнывсеофицерыказалосьдей  
ствительныбылизтотвечервлюбенымарьягенриховнудажетеофицерыкоторыееигралазаперегородкуквартирыскоробросилигруппперешли  
ксамоваруподчиняясьобщемунастроениюухаживаянызамарьейгенриховноймарьягенриховнавидясебяокруженнойтакойблестящейичувств  
молодежьуюсияласчастьемкакнистараласьонаскрыватьэтогоикакниочевидноробелаприкаждомсонномдвижениииспавшегозанеймужаложаб

ылатолькооднасахарубылобольшевсегоноразмешиватьегонеуспевалиипотомубылорешеночтоонабудетпоочередномешатьсахаркаждомуро  
стовполучивсвойстаканиподливнегоромупопросилмарьюгенриховнуразмешатьдаведьвыбезсахарасказалаонавсеулыбаяськакбудтовсечто

Код

```
package com.gmail.xapchenko2000;
```

```
import java.io.BufferedReader;
```

```
import java.io.IOException;
```

```
import java.io.*;
```

```
import java.util.*;
```

```
public class Main {
```

```
    public static void main(String[] args) {
```

```
        // System.out.println(solveTheEquation(961, 142, 837)); //ax ≡ b (mod n)
```

```
        String justString = readFile("C:/Users/xapch/Desktop/crypt3/text.txt");
```

```
        String russianAlph = readFile("C:/Users/xapch/Desktop/russianAlph.txt");
```

```
        String clear = clearWithOutSpaces(justString);
```

```
        String clearAlph = clearWithOutSpaces(russianAlph);
```

```
        int allLetters = clear.length();
```

```
        printAlph(clearAlph);
```

```
        //bigram(clear,allLetters); //find 5 most popular
```

```
        mainFun(clearAlph, clear);
```

```
    }
```

```
    public static String readFile(String path) {
```

```
        String str = "";
```

```
        try {
```

```
            FileInputStream file = new FileInputStream(path);
```

```
            DataInputStream dis = new DataInputStream(file);
```

```
            BufferedReader br = new BufferedReader(new InputStreamReader(dis));
```

```
            String Contents = "";
```

```
            while ((Contents = br.readLine()) != null) {
```

```
                str += Contents;
```

```

    }

    } catch (IOException e1) {

        System.out.println(e1);

    }

    return str;
}

public static void printAlph(String alphabet) {

    char[] alphabetArray = alphabet.toCharArray();

    for (int i = 0; i < alphabetArray.length; i++) {

        System.out.println(alphabetArray[i] + " " + i);

    }

}

public static float bigram(String clear, int allLetters) {

    char[] charArray = clear.toCharArray();

    Map<String, Float> biCounter = new HashMap<String, Float>();

    for (int i = 0; i < clear.length() - 1; ++i) {

        char s = charArray[i];

        char sOne = charArray[i + 1];

        String bi = String.valueOf(s) + sOne;

        if (biCounter.containsKey(bi)) {

            biCounter.put(bi, biCounter.get(bi) + 1);

        } else {

            biCounter.put(bi, (float) 1.0);

            i++;

        }

    }

```

```
}
```

```
biCounter.entrySet().stream()  
    .sorted(Map.Entry.<String, Float>comparingByValue().reversed())  
    .forEach(System.out::println);
```

```
System.out.println("=====");
```

```
return 0;
```

```
}
```

```
public static String clearWithOutSpaces(String str) {
```

```
    String newStr = str.toLowerCase();
```

```
    String clear = newStr.replaceAll("[^a-zA-Z]", "");
```

```
    return clear;
```

```
}
```

```
public static int gcd(int a, int b) {
```

```
    int c;
```

```
    while (b != 0) {
```

```
        c = a % b;
```

```
        a = b;
```

```
        b = c;
```

```
    }
```

```
    return a;
```

```
}
```

```
public static int howManyTimesAWillDivB(int a, int b) {
```

```
    int len = 0;
```

```
    int c;
```

```
    while (b != 0) {
```

```
        len++;
```

```
        c = a % b;
```

```
        a = b;
```

```
        b = c;
```



```
}  
  
return len;  
  
}
```

```
public static int getOppositeElement(int a, int b) {  
  
    int oppositeElement = 0;  
  
    int copyA = a;  
  
    int c;  
  
    int remainder;//остаток от деления  
  
    int i = -1;//номер элемеента в массиве  
  
    int lenOfTheArray = howManyTimesAWillDivB(a, b);  
  
    int[] arrOne = new int[lenOfTheArray];//массив остатч  
  
    int[] arrTwo = new int[lenOfTheArray];// массив после операций, где предпслений эелемент будет обратным  
  
  
  
    if (b == 1) return 1;  
  
    if (gcd(a, b) != 1) {  
  
        //System.out.println("Try one more time.\nNumbers are not mutually simple.");  
  
    } else {  
  
        while (b != 0) {  
  
            i++;  
  
            remainder = a / b;  
  
            arrOne[i] = remainder;//записываем в массив остаток от деления  
  
            c = a % b;  
  
            a = b;  
  
            b = c;  
  
        }  
  
        for (int j = 0; j < arrOne.length; j++) {  
  
            arrOne[j] = arrOne[j] - arrOne[j] * 2;  
  
        }  
  
  
  
        arrTwo[0] = arrOne[0];  
  
        arrTwo[1] = arrOne[1] * arrTwo[0] + 1;  
  
        for (int j = 2; j < arrTwo.length; j++) {  
  
            arrTwo[j] = arrOne[j] * arrTwo[j - 1] + arrTwo[j - 2];  
  
        }  
  
    }  
  
}
```

```

    }

    oppositeElement = arrTwo[lenOfTheArray - 2];

    if (oppositeElement < 0) {

        oppositeElement += copyA;

    }

}

return oppositeElement;

}

public static int solveTheEquation(int n, int a, int b) { //  $ax \equiv b \pmod{n}$ 

    int result = 0;

    int cN = n;

    int opposite = getOppositeElement(n, a);

    int gcd = gcd(a, n);

    if (gcd == 1) {

        result = (opposite * b) % n;

    } else if (b % gcd != 0) {

        System.out.println("Wrong!");

    } else {

        opposite = solveTheEquation(n / gcd, a / gcd, b / gcd);

        n /= gcd;

        int k = n;

        int[] arr = new int[gcd];

        for (int i = 0; i < arr.length; i++) {

            arr[i] = k * i + (opposite) % cN;

        }

        for (int i = 0; i < arr.length; i++) {

            System.out.println(arr[i]);

        }

    }

    return result;

}

```

```

public static int mainFun(String alphabet, String userText) {

    int a = 0;

    int s = 0;

    int[] arrCipher = {772, 834, 728, 256, 493};

    int[] arrOpen = {545, 417, 572, 403, 168};

    char[] alphabetArray = alphabet.toCharArray();

    char[] userTextArray = userText.toCharArray();

    int count = 0;


    String openText;


    while (s != 5) {

        int k = 0;

        while ((k != 5)) {

            int i = 0;

            if (s == k) {

                if (k == 4) break;

                else k++;

            }

            while (i != 5) {

                int j = 0;

                while ((j != 5)) {

                    if (i == j) {

                        if (j == 4) break;

                        else j++;

                    }

                }

                count++;

                int dy = getOppositeElement(961, (arrCipher[s]) - arrCipher[k]);

                int dx = arrOpen[i] - arrOpen[j];

                if (dx < 0) dx += 961;

                if (dy < 0) dy += 961;

```

```

        System.out.println("The pair of cipher text = " + alphabetArray[arrCipher[s] / 31] + "" + alphabetArray[arrCipher[s] % 31] + " " +
alphabetArray[arrCipher[k] / 31] + "" + alphabetArray[arrCipher[k] % 31]);

```

```

        System.out.println("The pair of open text = " + alphabetArray[arrOpen[i] / 31] + "" + alphabetArray[arrOpen[i] % 31] + " " +
alphabetArray[arrOpen[j] / 31] + "" + alphabetArray[arrOpen[j] % 31]);

```

```

        a = (dx * dy) % 961;

        j++;

        if (a < 0) a += 961;

        if (a > 1) {

            int b = (arrCipher[s] - getOppositeElement(961, a) * arrOpen[i]) % 961;

            if (b < 0) b += 961;

            System.out.println("a = " + getOppositeElement(961, a));

            System.out.println("b = " + b);

            openText = decrypt(alphabet, userText, a, b);

            findImpossibleBigram(openText);

            if (ifOpenTextIsCorrect(openText)) {

                System.out.println(openText);

                System.out.println("a = " + getOppositeElement(961, a));

                System.out.println("b = " + b);

            }

            if (ifOpenTextIsCorrect(openText)) return 0;

        }

        i++;

    }

    k++;

}

s++;

}

return a;

```

```

public static String decrypt(String alphabet, String userText, int a, int b) {

```

```

    char[] alphabetArray = alphabet.toCharArray();

```

```

char[] userTextArray = userText.toCharArray();

int Xi;

int Yi;

String openText = "";

char s;

char sOne;

int one;

int two;

int oneOpen;

int twoOpen;

for (int i = 0; i < userTextArray.length - 1; i++) {

    one = findIndex(userTextArray[i], alphabet);

    two = findIndex(userTextArray[i + 1], alphabet);

    Yi = one * 31 + two;

    Xi = (a * (Yi - b)) % 961;

    if (Xi < 0) Xi += 961;

    oneOpen = Xi / 31;

    twoOpen = Xi % 31;

    s = alphabetArray[oneOpen];

    sOne = alphabetArray[twoOpen];

    StringBuilder sb = new StringBuilder().append(s).append(sOne);

    String bi = sb.toString();

    openText += bi;

    i++;

}

//System.out.println(openText);

return openText;

}

```

```

public static int findIndex(char a, String alphabet) {

    int i;

    char[] alphabetArray = alphabet.toCharArray();

    for (i = 0; i < alphabetArray.length; i++) {

        if (a == alphabetArray[i]) {

            return i;

        }

    }

    return i;

}

public static void findImpossibleBigram(String openText) {

    String[] arrOfImpossible = {"оь", "ьь", "йй", "аб"};

    System.out.println("The text doesn't correct because: ");

    for (int i = 0; i < arrOfImpossible.length; i++) {

        if (openText.contains(arrOfImpossible[i])) {

            System.out.println("Found " + arrOfImpossible[i] + " in the text");

        }

    }

}

public static boolean ifOpenTextIsCorrect(String openText) {

    if (openText.contains("аб") || openText.contains("оь") || openText.contains("ьь") || openText.contains("йй")) {

        return false;

    } else return true;

}

}

```

**Висновок:**

Ми навчились працювати з алгоритмом афінної біграмної підстановки, використали на практиці знання, які отримали в минулому семестрі з дисципліни дискретна математика. Покращили навички роботи з алгоритмами розшифрування та