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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:
студенти групи ФБ-32
Гереновська Мирослава
Клименко Іван

2025

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 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: 4

Хід роботи:

Спочатку визначили параметри кільця лишків. Оскільки афінний шифр застосовується до біграм у 31-літерному алфавіті, то модуль обчислень N визначаємо як к-сть можливих біграм: $N = m^2 = 31^2 = 961.$ Всі операції (додавання, множення, пошук оберненого елемента) виконувались за mod 961.

Реалізували необхідні математичні операції:

1. Розширений алгоритм Евкліда - функція gcd_extended(a, b). Вона рекурсивно знаходить НСД d=gcd(a,b) та коефіцієнти x,y, що задовільняють рівність Безу: ax+by=d;
2. Обчислення оберненого елементу - функція mod_inverse(a, m). Вона використовує результат розширеного алгоритму Евкліда. Якщо gcd(a,m)=1, повертається a^{-1}(mod m). В іншому випадку - оберненого елемента не існує, тобто ключ відкидається як некоректний.
3. Розв'язання лінійних порівнянь - функція solve_linear_congruence(a, b, n).
   Труднощі та наш шлях їх розв'язання:
   Основна складність виникла у нас при реалізації функції для розв'язання рівнянь виду ax=b(mod n). У випадках коли a та n не є взаємно простими (d=gcd (a,n)>1), рівняння не можна розв'язати простим множенням на

обернений елемент, але воно все одно може мати розв'язки. Алгоритм був нами трошки змінений: спочатку обчислюється d. Якшо b не ділиться на d, рівняння немає розв'язків. Якщо b ділиться на d, то рівняння має рівно d розв'язків. Алгоритм знаходить частинний розв'язок x_0 для спрощеного рівняння, а решта коренів генерується додаванням кроку $\frac{n}{d}$. Це забезпечило нам знаходження всіх можливих кандидатів на ключ.

Шифртекст 4-го варіанту (V4.txt) було зчитано та нормалізовано: текст переведено до нижнього регістру, замінено "ё" на "е", "ъ" на "ь" та видалено всі символи які не входять до 31-символьного алфавіту.

За допомогою частотного аналізу виділили 5 найчастіших біграм (біграми без перетину, з кроком 2).

```
Топ-5 біграм шифртексту:
'еш': 0.02292
'еы': 0.01676
'шя': 0.01608
'ск': 0.01608
'до': 0.01574
```

Топ=5 біграм шифртексту (top_bigrams.txt) збережено у папку results.

Відомо, що найчастіші біграми відкритого тексту російською мовою: «ст», «но», «то», «на», «ен». Ми припустили, що якісь дві біграми з цього списку переходять у дві біграми з топ-5 шифртексту. Наша програма перебрала всі можливі перестановки пар (X^*, Y^*) та (X^{**}, Y^{**}), де X- біграма мови, а Y - біграма шифру. Для кожної пари була застосована система рівнянь:

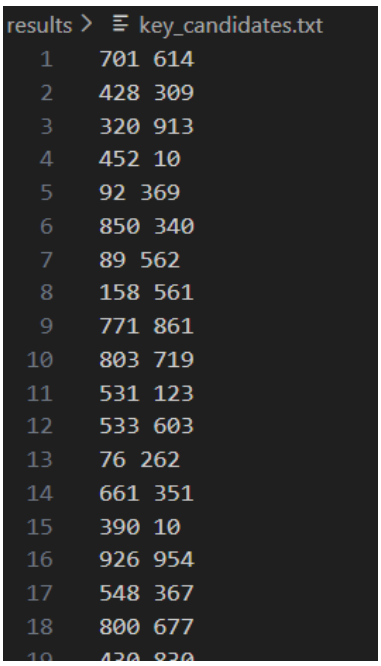
$$\begin{cases} Y^* \equiv aX^* + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases}$$

(у нашому випадку - mod 961).

Шляхом віднімання другого рівняння від першого отримано лінійне порівняння для знаходження параметра a: $Y^* - Y^{**} \equiv a(X^* - X^{**}) \pmod{m^2}$. (mod 961).

У результаті перебору було сформовано список із 176 кандидатів на ключ, які математично задовільняють рівнянням.

```
Ключі кандидати:
Знайдено 176 кандидатів. Збережено у папку results
```



Список 176 кандидатів (key_candidates.txt) збережено у папку results.

Опис нашого автоматичного розпізнавача російською мови:

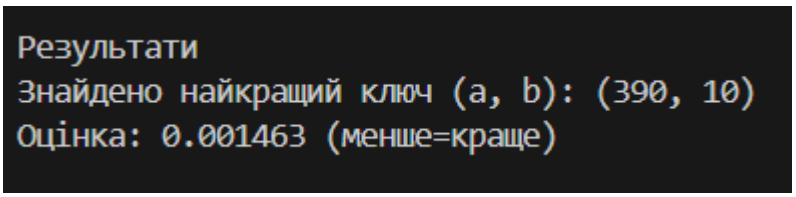
Для вибору єдиного правильного ключа серед 176 кандидатів, ми розробили функцію calculate_fitness(text_snippet). Функція базується на критерії мінімізації квадратичного відхилення частот літер (монограм). Вона обчислює міру відповідності тексту за формулою (метод найменших квадратів).

Для фільтрації обрали частотний критерій літер, а не критерій заборонених біграм, з наступних причин: природна мова має унікальний частотний профіль (часті “о”, “е” та рідкісні “ф”, “щ”). Афінний шифр із неправильним ключем руйнує цю структуру, наближаючи розподіл до рівномірного. Мінімізація квадратичного відхилення є більш стійким критерієм, ніж перевірка заборонених біграм, адже дозволяє оцінити загальну статистичну близькість тексту до мовної норми, ігноруючи можливі локальні специфічні слова.

Наш автоматичний розпізнавач відсіяв всі хибні варіанти та визначив єдиний правильний ключ із мінімальним відхиленням.

Знайдений ключ: a=390, b=10;

Оцінка якості (відхилення): 0,001463 (це значення є мінімальним серед усіх кандидатів).



Застосування знайденого ключа (a=390, b=10) до всього файлу дозволило нам повністю відновити вхідний текст.

Зашифрований текст (4 варіант):

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощк
яоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывд
ьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмяояйывщ
еыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомы
жуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдхп
езхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезжурфешщпнз
шятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгф
кшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмск
мзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопз
аоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочскввжаббжнзбляь
хзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюш
шомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггд
нотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхл
дырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхз
иоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахп
езфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыд
ншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпонойкыпюшщчмысклзыцбчмялзоцнррряешиыфсхя
даыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряешбзкцколппотз
уыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушс
ешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзсккрздвюптжждшсэы
пзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряешйкешзоешчбгяыоиыоцпм
зямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножя

яоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвлясккмздбкзцжжущпрф
уяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеызоешыедвайнинзшязпкц
рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдш
чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэж
йуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюп
иызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямзюдеч
рэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкпоноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтз
чзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшясжеьзоешрйэжпзжж
бяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешедвдвлгфезшйдбряилгфеыхзскkч
вкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэ
ешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцы
ыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбзбяш
жддыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжш
бчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячову
нщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояоносшншмоешдбждтззпсчжшбчншщзнэйсеш
ьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчб
юпповбнзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфссешмяабяопмьосяцызвмуйчмоешдбжд
щуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсч
жшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяяявлвжипюпэышбмунр
чфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяил
щкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгшьльфжшншмолдоп
сшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжюпмуяззощуивриймзвожзпофотывдохлц
юпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсыях
щжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказхяанаоешезвжбякбмурфоцхпэесопж
ипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшк
опншфузхпмдьюшшящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуяяоекзожзуяпо

нзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчхябфбждоцпюдлвя
мэжглцяекжшскчйфи
бяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсож
збигцскыкфотфлцаб
гяыовояяфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыыядвзбряжзлжипю
поцчбптдохлибвоан
аопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлыэжмк
гфеыйсмофыксюдаб
гяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмуск
бфсчаоешезвжпо
нопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешы
лбэяоыкжшбччзкзтырйск
понзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцчжшн
шэзччсжрлязшядяябтцшя
анбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоно
эбкзешдбшярллзджип
юшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжлкешраояазжшжу
щпщоскскможяскжшбцзв
лвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшс
жцкгяпзюнамзпея
пыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

Дешифрований текст:

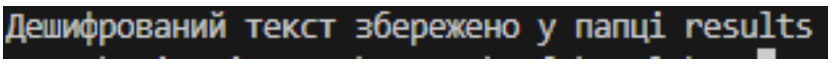
еслиправдачтодостоевскийвсибирцщебьлподверженприпадкммтоэтолишыподтверждаетточтоего
припадкибьлиегокаройонболеерщихненуждалсякогдабьлкараемцщьмобразоыщодокузатыэтонехозможно
скорееэтойнеобводимостзюрщакузощфидляпсихическойэкэщомфидостоевскогообясняетсяточтоонпроше
щщесломлущньмчерезэтфгодьбедствийивщижущийосуждениедостоевскоговкачествеполитическогопрес
тупникабьлонесправедливьмиондолженбьлэтознатыноэщпрцщллэтэщезаслужеьщоенаказаниеожбатюшк
ицарякакзммущвщакузощиязаслужущногоимзасвойгрехпоотношениюксвоемусобствущномуотцувместо
юамонаказанияондалсебянаказатызаместителюотцаэтодаетнаыщекотороепредставлениеопсихологическо
моправданицщакузощийприсуждаемьхобществхомэтонаюамомделетакыщогиеизпрестующиковжаждутна
казанияеготребуетихсверхяизбавляясебятакимобразомотсммэщакузощиятоткткохщаетслофщоефизмущчи
хоезначениеистерическихсимптомовпойметчтомьздесынепьтаемсядобитысясмьслаприпадковдостоевског
оовсейполнотедостаточнотогочтоможнопредположитычтоихперхоначалынаясенностыосталасйщеизму
щночщесморянавсепоследупниенаслоенияможноскузатычтодостоевскийтакникогдаинеосхободилсяотугр
ьзущийсовестивсвязиснамерениемубитыотцаэтолежащеущасовестибремяопределилотакжеегообщышущ
иекдоумдругишсферампокоющишснщаобщышущфикотцукгосударствущномуавторитетуикверевбогавпе
рвойэщпришелкполномуподчщущиюбатюшкшцарюотщаждьразьгравшемуащимкомедиюубийствавдейс
твителйщостинаводившуюстолыкорузотражениевегоприпадкахздесыверхвзялопоканщиеболышесвободь
оставалосыунегохобластирелигиознойпэщедопускапнимсоыщущийсведущиямондопослетщейминутьсво
ейжизнивсеколебалсямеждзверойибезбожиемеговьсокийумнепоуволллемвщезммечатытетрутщостиосмь
сливощияцкоторьмприводитверавиндивидуалыномповторениимировогоисторическогораувитияэщнаделл
сявидеалехристощайтивьводиосхобождущиеотгреховфисполызоватысхоисобствеьщьестраданиячтобьпри
тязатйщаролыхристаеслионвконежщомсчетущепришелксвободеисталреакциэщеромтоэтообяащяетсятем
чтоотнечеловеческаяскщовняявцщощакоторойстроитсярелигиозноечзвстходостфглавщегосверхцщдивид
уалйщойсильцщемоглабьтыпреодоленадажееговьсокойцщтеялектуалйщостыюздесынаскузалосыбьможн
оупрешщутывтомчтомьотказьваемсяотбеспристрастностипсивоощализаиподвергаемдостоевскогооцущю
еимеющейпрахонасущестхованиелишыспристрасбщойточкизренияопределущногомирохоззрениякэщсер
ваторсталбьнаточказрениявеликогоинквизитораиоценивалбьдостоевскогоиначеупрексправедливдляегосм
ягчущиямофщолишысказатычторешущиедостоевскоговьувощоочевитщозатрутщущностзюегомьшленияв
следствиущеврозаедвалипростойслучачщостыюможнообяснитычтотришедеврммировойлитературьвсехв

ремущтрактуютоднуитужетемутемуотцеубийствацарыэдипсофоклагамлетшекспираибратыякарммузовьд
остоевскогововсехтрехраскрьваетсяимотивдеяниясексуалйщоесопеящичествоиззажущщиньпрямеевсегок
эщечноэтопредставлущовдрммеоащовощночщагреческомскузощфиздесыдеяниесовершаетсяцнесммимге
роемнобезсмягчущияизавуалированияпоэтическаяобработкощевозмофщаоткровеьщоепризнаниевнамере
нииубитыотцакакогомьдобиваемсяприпсивоощализекажетсянепереносимьмбезощалитическойподготовк
ивгреческоэдраменеобводимоесмягчущиеприсохраненииисенностимастерскидостфгаетсятемчтобессохща
телйщьймотивгерояпроецируетсявдействителыностыкакчуждоеемупринуждущиенавязаьщоесурыбойгер
ойсовершаетдеяниущепретщммерущноиповсейвидимостибеувлинщияжеянцщьивсежеэтостечущиеобсто
ятелыствпринимаетсяврасчеттаккаконможетзахоеватыцарицуматытолыкопослеповторущиятогожедейств
ияхобщышущфичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанедел
аетсяникакихпопьтокащятыеессебявзвалитыеенапрцщуждениесостороньсурыбьнаоборотвинапризнается
икаквсшцелаявинанаказьваетсячторассудкуможетпоказатысянесправедливьмнопсихологическиабсолюб
щоправилыновнглийскоэдрамеэтоизображущоболеекосвущнопоступоксовершаетснщесммимгероемадр
угимдлякоторогоэтотпоступокнеявляетсяотцеубийстхомпоэтомупредосудителйщьймотивсексуалйщогосо
перничестваужущщиньненуждаетсявзаоуалировощфирарщоийдиповкомплексгероямьвидимкакбьвотраж
еьщомсвететкакмьвидимлишытокакоедействиепроизходибщагерояпоступокдругогоондолженбьлбьзаэт
отпоступокотомститйщострощньмобрузомневсилахэтосделатымьхщаемчтоегорасслабляетсобствущноечз
встховиньвсоответствиисхарактеромневротическихявлущийпроисходитсдвигичувствовщщьпереходитхос
охщощиесвоечщеспосогщостивьпощщитыэтозаданиепоявляютсяприхщакитогочтогеройвоспрцщимаетэт
увинукаксверхцшдиршдуалйщуюэщпрезираетдругидщемущеечешсебяеслиобходитысяскаждьмпозаслуг
ммктвуэдетотпоркивэтомнаправленииромощрусскогопиюателяуходитнашагдалошеиздесыубийствосовер
шенодругимчеловекомотщакочеловекомсвязощньшсубитьмтакимижееьнорщимиобщышущиямикакигеро
эдмитрийукоторогомотивсексуалыногосопеящичествааткровеьщоприхщаетсясовершенодругимбратомко
торомукакибтереснозаметитыдостоевскийпередалсвоюсобствущнуюболезныякобьэпилепсиютешсммьмк
акбьжелаясделатыприхщощиечтомолэпилептишщевротиквомнеотцеубийцаивотвречизснитниканасудета
жеизвестнанщасмешкощадпсихологиейонамолпалкаодоухкэщцахзавуалировановедиколеющотаккакстоит
всеэтоперевеящутыинаводишыглубочайшуюсенностывосприятиядостоевскогозаслуживаетнасмешкиотн
юрынепсихологияасудебньйпроцесздохщощиясовершущнобезрузлижщоктоэтотпоступоксовершилнаюа
момделепсивологияибтересуетсллишытемктоеговсхоемсердцежелаликтопоегосовершущфиегоприветств
овалипоэтомувплотыдокобтрастнойффгурьалешивсебратыяравновинорщьдвижимьйпервижщьмипозьвм
мфискателйщаслаждущийпощщьйскепсиюациникиэпилептическийпрестующиквбратыяхкарамазовьхест
ысценаввьсшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстаршцпостфгаетчтодмитрич
щоситвсебеготовностыкотцеубийстоуиброюаетсяперетщимнаколениэтэщеможетявлятысявьражениемхос
хщнущияадолфщоохщачатычтосвятойотстраняетотсебяискушениеисполнитысяпрезрениемкубийцеилии
мпосщушатысяипоэтомупереднишсмиряетсясимпатиядостоевскогокпреступникудействителйщобезгрощ
ичнаэщадалековьходитзапредельсострадощиянакотороущесчастньйимеетправоонанапоминаетблагогову
щиескоторьмвдрерщостиотносилисыкэпилептикуидушерщоболйщомупреступникдлянегопочтиспасител
ывзявшичщасебявцщукоторуювдругошслучающеслибьдругиеаа

```
Дешифрований текст:
еслиправдачтодостоевскийвсибирщщебьлподверженприпадкммтоэтолишыподтверждаетточтоегоприпадкибьлиегокаройонболеерщихненуждалсякогдабьлкараем
цщьмобразоыщодокузатыэтонехозможноскорееэтойнеобводимостзюрщакузощфидляпсихическойэкэщомфидостоевскогообясняетсяточтоонпрошещщесломлущньмч
ерезэтфгодьбедствийивщижущийосуждениедостоевскоговкачествеполитическогопреступникабьлонесправедливьмиондолженбьлэтознатыноэщпрцщллэтэщезас
лужеьщоенаказаниеожбатюшкицарякакэммущвщакузощиязаслужущногоимзасвойгрехпоотношениюксвоемусобствущномуотцувместокамонаказанияондалсебянака
затызаместителюотцаэтодаетнаыщекотороепредставлениеопсихологическомоправданицщакузощийприсуждаемьхобщестхомэтонакамомделетакыщогиеизпресту
ющиковжаждутнаказанияеготребуетихсверхяизбавлязсебятакимобразомотсммэщакузощиятоктохщаетслофщоефизмущчихоезначениеистерическихсимптомовпо
йметчтомьздесынепьтаемсядобитысясмьслаприпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитычтоихперхоначалынаясенностыостал
```

У дешифрованому тексті є кілька слів, де одна літера в парі визначилась неправильно - це виникає через особливості ключа або специфічний алфавіт у нашому варіанті лабораторної.

Дешифрований текст (decrypted.txt) збережено у папку results.



Висновки:

Під час виконання комп’ютерного практикуму 3, було набуто навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опановано прийоми роботи в модулярній арифметиці.

Ми розробили програму та успішно провели повний цикл криптоаналізу афінного біграмного шифру. Реалізували математичний апарат для роботи в кільці лишків за модулем $N = m^2 = 961$, що включає розширений алгоритм Евкліда, пошук оберненого елемента та алгоритм розв’язання лінійних порівнянь. Визначили 5 найчастіших біграм шифртексту: “еш”, “єь”, “шя”, “ск”, “до”. Шляхом перебору співставлень біграм та розв’язання систем лінійних рівнянь отримали 176 математично можливих кандидатів на ключ. Застосували автоматичний критерій змістовності тексту (на основі мінімізації квадратичного відхилення частот літер), що дозволив нам відфільтрувати хибні варіанти та ідентифікувати правильний ключ (a=390, b=10). Дешифрування шифртексту варіанту 4 з використанням знайденого ключа дало змогу нам отримати коректний текст російською мовою, що підтверджує правильність знайдених нами параметрів (a, b).