Міністерство освіти і науки України

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота №3

Виконав студент групи ФБ-13

Нійозов Рустам

**Київ 2023**

*Криптоаналіз афінної біграмної підстановки*

**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.

**Хід роботи :**

**4 варіант**

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощк

яоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывд

ьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмяояйывщ

еыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомы

жуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдхп

езхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезжурфешщпнз

шятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгф

кшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмск

мзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопз

аоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбляь

хзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюш

шомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггд

нотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхл

дырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхз

иоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахп

езфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыд

ншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпонойкыпюшщчмысклзыцбчмялзоцнрряешиыфсхя

даыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряешбзкцколппотз

уыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушс

ешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюптжждшсэы

пзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряешйкешзоешчбгяыоиыоцпм

зямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножя

яоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзцжжущпрф

уяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеызоешыедвайнинзшязпкц

рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдш

чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэж

йуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюп

иызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямзюдеч

рэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкпоноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтз

чзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшясжеьзоешрйэжпзжж

бяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешедвдвлгфезшйдбряилгфеыхзсккч

вкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэ

ешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцы

ыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбзбяш

жддыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжш

бчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячову

нщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояоносшншмоешдбждтззпсчжшбчншщзнэйсеш

ьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчб

юпповбнзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфссешмяабяопмьосяцызвмуйчмоешдбжд

щуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсч

жшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяяявлвжипюпэышбмунр

чфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяил

щкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгшьльфжшншмолдоп

сшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжюпмуяззощуиврймзвожзпофотывдохлц

юпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсыях

щжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказхяанаоешезвжбякбмурфоцхпэесопж

ипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшк

опншфузхпмдьюшшящксктллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуяяоекзожзуяпо

нзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчхябфбждоцпюдлвямэжглцяекжшскчйфи

бяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфлцаб

гяыовояяфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыыядвзбряжзлжипюпоцчбптдохлибвоан

аопоьшйкешзокюыврухкнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдаб

гяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаоешезвжпо

нопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйск

понзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшя

анбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшярллзджип

юшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжлкешраояазжшжущпщоскскможяскжшбцзв

лвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпея

пыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

Код реалізований в ( 3.py)

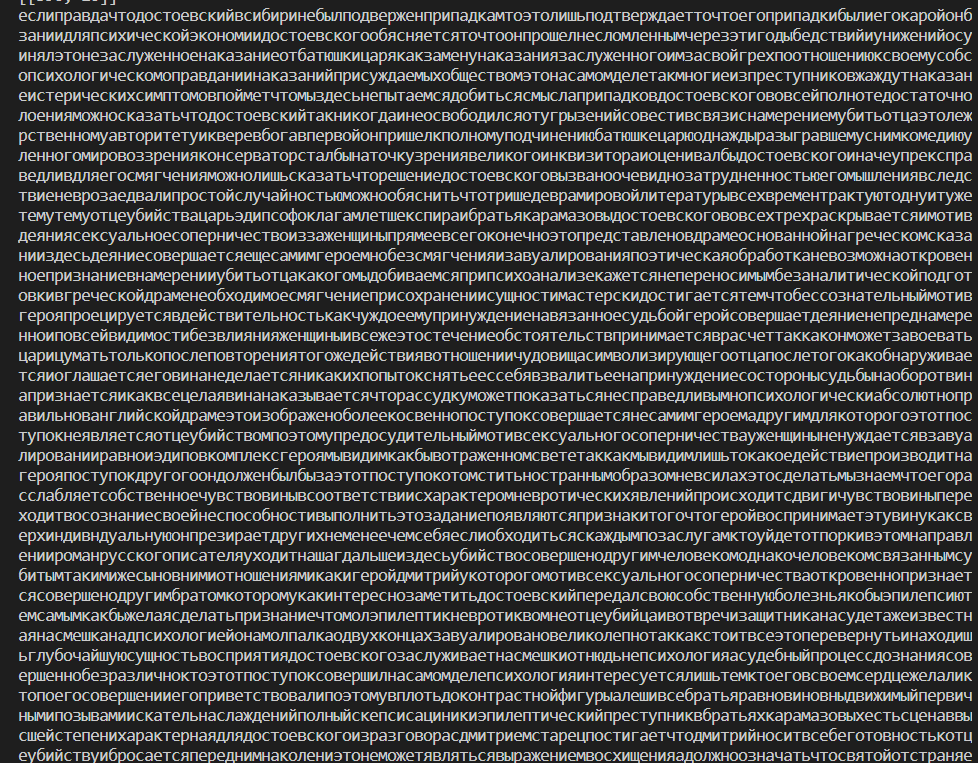
Найчастіші біграми без пробілів:

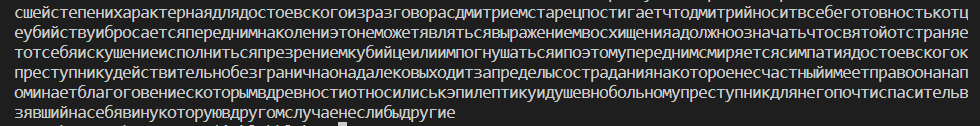


Ключ:



Розшифрований текст:





еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонбзаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиуниженийосуинялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобсопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточнолоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерениемубитьотцаэтолежрственномуавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюшкецарюоднаждыразыгравшемуснимкомедиюуленногомировоззренияконсерваторсталбынаточкузрениявеликогоинквизитораиоценивалбыдостоевскогоиначеупрексправедливдляегосмягченияможнолишьсказатьчторешениедостоевскоговызваноочевиднозатрудненностьюегомышлениявследствиеневрозаедвалипростойслучайностьюможнообяснитьчтотришедеврамировойлитературывсехврементрактуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсегоконечноэтопредставленовдрамеоснованнойнагреческомсказанииздесьдеяниесовершаетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбезаналитическойподготовкивгреческойдраменеобходимоесмягчениеприсохранениисущностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействительностькакчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамеренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторениятогожедействиявотношениичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьеессебявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихологическиабсолютноправильнованглийскойдрамеэтоизображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничествауженщиныненуждаетсявзавуалированииравноиэдиповкомплексгероямывидимкакбывотраженномсвететаккакмывидимлишьтокакоедействиепроизводитнагерояпоступокдругогоондолженбылбызаэтотпоступокотомститьностраннымобразомневсилахэтосделатьмызнаемчтоегорасслабляетсобственноечувствовинывсоответствиисхарактеромневротическихявленийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособностивыполнитьэтозаданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэтомнаправлениироманрусскогописателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитрийукоторогомотивсексуальногосоперничестваоткровеннопризнаетсясовершенодругимбратомкоторомукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийцаивотвречизащитниканасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодвухконцахзавуалировановеликолепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершеннобезразличноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсялишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнаслажденийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввысшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитрийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотороенесчастныйимеетправоонанапоминаетблагоговениескоторымвдревностиотносилиськэпилептикуидушевнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругомслучаенеслибыдругие

**Висновки**: Під час виконання практикуму, навчився створювати та розуміти принцип дії програми автоматичного розпізнавання змістовного тексту, спробував провести криптоаналіз афінного шифру біграмної заміни та знайти вірний ключ, для розшифрування тексту. Набуті навички знадобляться у подальших практикумах та професійні діяльності.