

Лабораторна робота №3
З предмету «Криптографія»

Виконали:

Студентки 3 курсу,

ФТІ, групи ФБ-74

Пудім Єлизавета

Горобець Ангеліна

Варіант 12

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.

Результати роботи:

a = 555,

b = 331

Cipher bigrams ['хк', 'ек', 'вю', 'пн', 'вх']

Original bigrams ['ст', 'но', 'то', 'на', 'ен']

Щоб відібрати саме цю пару ключів, нам треба було відфільтрувати розшифровані тексти, які мали заборонені біграми, тобто ті, які у ВТ зустрілися не можуть. Для цього ми створили функцію з такими забороненими біграмами: ['аь', 'оь', 'уь', 'ыь', 'эь', 'иь', 'еь', 'яь', 'йь', 'ыь', 'ьь', 'йй']

Зашифрований текст:

оклийазогтдхвоэшктжсэллыэежябчехеквюхуашайейллокийбяктейвндкпйзмхшкшэххиккптжпнуафйнрцэкурлюхжыэвхбк
дкшхяиожбтхлцймтдшгхуюклцбьшнцмешврчцьтакугэвжйулнекчвоцмахухкпюкукгхупнфйлрзгдзкохксавхцляплэен
цяккпюлюбйчдгцякбуейяждоохсавхцляххкпюлюптжхквгейчдгцхнцмыжшжхжъэхтшфхййвнхкйеокгхйэоцмахутжджюхбж
яежвбурзежябчехжфлююющчэюхуевхвюйшыьоржлвнкбгхвюдшчжуастхжыэжвашцэежяюэранмафйквхябчжшжккхтхзю
кжябтмюхййвнгцдпгфздьлпнзюекабзюгцщдэтлюзжжэпппгтжмдшрпаьжцеазогтдвхгхьтвуййзмихайгцпндоекачхрмтдшг
екыэвхддппфйкудкшхяйнрыпцюкнфяюапряжфхажсююохкнмздждудбхшхфжяжпрчжтгнкцгцмвкгнъллнышжбгхвюсыпяняконшу
ашяквюезлнлрудвурсюэякеххэыэлабестешцколрзбьууоюкйькрянякурлюмэпжкынлюнлхббщгхьпытжфпыйююейейллхлз
куэщмэьмюебююэряжжжупжйеекфхмуоьнуцпккйегкюкындпфййцпжлнйьэьююирирюрзлкаббжпжихьзщкхэфпыйжуюююо
хкмкпжыэьзчмацюеуюкйькрянябхклзккраирхулнтцпрвюкуцэрххьупртдахууимшхыэалофехжвхжддцънгцмвдххвюку
кьлэбьексрцпядэахуюэзтнрвмззихуечйтшпытэвицкучььдмбдпхукхрпгджусынгамчььоцхуакхжйеххзаппийекдзтддп
багпгдякышгтвунклцмвтхтхкпстихихжыхшхьэвхйькрьчвхэхихуаэьмкэцийфрыизыашлхвюрыаыегтдзякпгжчьяэябжу
исщгэуеэгпймхумбнэцаеблжкосоыюфбыврнийпншбзуумбсмкушбгцххккшппнокшлзапхушжжнжзофлкьпкпгпфунтэрышжнст
вуиохкаюшбирэщвхвюйшрэтфежацлюздэщтжчоebвххцгнбхккыипрехбуэрсьетвудтжпюпнфйтэбаяхклзэклнрзийьжйе
екейейллххэьмюебююэрстгдбьыэцезцмтшьжыэвхежябчеххвцлюлюяжлюмвфншбикьджюзкынтэькчкчвскнббжюиурпвежчх
шнзждкыэгжбюкажунстздиктхлзкхкпншбйрыжожвюфбшжюпобжэкмжмчьюсыякхкаблэчвдьбкзкйевючэшрвнгцпнссшклз
ччещхвикбкпдлножикэбежсэбцггпбгыюашжзуеынбчйчгафйчьбхшбтхвхпущпвынббэфндпшьбжхжтнтэькфндпгдэшнбтп
тжчэююкцеэокежйэятмийэржляждкиовмиржлвнебгхвюдшоцамахупнехуэвхюебуеогдэашэбьсьтмюьфжяжбвлкякбкынэр
кьэьшцфйзмхйэхккпыйжукцгпнфхуфзлюхуойэрзюфзфзшхчэюохкхэжьаехкшжжгпвнзюхкоцихцчдмамуфйюохкпвыэьц
кьэьзотхокогейжуудпююэщчэююокккйегкньсэчэпжйеекбтхбокажулюпнокпудоектхвнвюбжтнещбжуниййчэьщжйблржлвн
цякхкххнрзгдхбтхдхмьывзхуеашпнмбьбвюэумбфбудвурепддгфихонзыежгнииьекдегптдмаппдкпгийзкюпзншбэудткухл
ожфуфзвырзудпмвщдебвюэухуеэщнхуягрижилюкхэьвышкябшряжйрхбськцамахумбтгцпрююпнюкэьтхшрфрззлюэруабк
ехчвмксэьэехедтэтллххмдицофпнвнхбыэлхютшйхклзвняэудебщпфзузюльнфудхбжупнощбхкщюцзтдижезппуэжвхнмма
щддпньнекупийейщлхвйэрфпчгхыэтхокогэагбуэыкокоджепжекупгдньшщещцпгжэьмюебхкчтэтллххддэтэтллххприребтх
екчэьэцеэчькынфйпвийехвшэсзирмбтхыкохцрлнеэхкуншбккмэщжбжяешэбикчвлацюшрякенгцезшххжышцожгпнквх
шэснзюуэззийогвжкмвтыптжбяэсвдхыэгжпвзмэхэсхыэцеджкзгдейтляеиклжэуеокмдыпллюпжджзкимэдкдхмэдхихдд
этэтллххджыонтлэкзхукоцвнгхубищжцпжэяншоохжвтхохтмдпзднлшьокмэенлекфхвжгхихбщзхжышцпгжурешыэцезк

[illegible]

швуаддфклцмвхкбтъниояэфхыхзрофыкчвбмзкяйкцуашктжонтмщбфйирпнчядкьвьюзучькьююшхошекйбпжджеждцщббьбжбк
дкихбкхэлхютцййкххжджекчохфпнтцдпяшеждкфхчькыкоюлмяконхбыхйешвцуисткхэыхфуэугцмэгжскеквьюндпуашмувт
чдпдсвйхпаазофуашрыэьошрмувтфжпнойфхухфпжикашфхшрчжвьюндпуашйуюнтмвкудягвырэмршдзкябшрьпыжндмаекст
шхиэрыкоюлмйфжяжвлкдкгяждкниюилнышьвьюлногююньвлкажхназкухэуетжсшфкгнзнзюгцжьбьжчптгжлйнкфгхжбкжв
либипзщбуфпрыэвьодшшэойчьжапаюэрэкзгрщдлножбвунцмппндокхенгцэрыжтмпнцммафйжуоохкклюбадхалчжашмууфпрщп
пнэрпнякахмэрдишщрвушхбжзконкбхкыбьойчьаагжузаскбкыкинужжжйейвхжйейвбжэьрэрзыкделюдкыкохцзксхькрэ
эухбгдчхчвгджуфбшаэтыкэжтнцмогжузаскбкыкинцмфзыноззынопзчцлнзодэрмждьвхбкыйжэаюствулюыжсээбчплнекенгцэр
ыжюдейвндпуахвхкррвьмохбьяэюхумбехыцлнзэдэширзпнфйстюаашшранагдчвязздофокхкыкдкпнурогзюокжныюфбхдиц
ешвьабчпдпцояяптжмдшргзийеибхшякхжбьжжэкоьогдэафхыкбукцнрннкцбогдэаикхжфхыххмкчэниюилнцщоцзкхегкыкээ
эжякоухбнкмйчэбыбтпшжхжузьлыхихшэкьсэпулнйыьпыждьпнойчыцзиофпвюзкдхсохкчпгдбкензжгндокхаждкййвхоххэ
лхынхбикутбййчцмацютццмюххкхюфнччихмэрбцюогрызкмксэнихйхбпзкугхххлзкбэшддййкэлчщцбхкыкинщбсьыхгзьлых
ихиквьюкиниюифшлхчюшрекгтхщюююпэжнбтптмлюжубаазкуфхзююмихфхмдлюппллофвюткмьеужнньфщпицдпвнцмьеоцкую
пнкрьвндхэзюстофжхвуздащпщпнойчьаьчэьжнпшжжжэцмппнэкдкетуххббьшнебуцанэьмбажпбекдхяктпзуашпнххцбхнп
юхыэбдупекажьюцмихтрпнчягаиргдвхвжвьюцмахушцбфбхкююбкщныюкнпяхкнбихьвскдяжэяпнякбхжнзюекцмппнуцдкхжыэ
икоюлмвхгхюзиййудфййпцюфбжцяждьддллкбкпдьфжшгнфйжхуешэбьизхжвйдошршрьоюхлкцякбкьюззстыэфжпнщбтхекчэ
гббэицмвалмбыафйгдаэрвюхумучйзюкнкндкгэжэмкокежтуяичжашзуиратжуыжсхлхкбьднхвзчцмахуашикоюлмфяхкхк
дкгедтвкоюрзгдэкенуохуйуюнтмщбдптгжнзюиоххшхгэжаюлюцмппнкньотмпнхблэбхлкэбцмхждхжрпнчяжпыйжуучьяэдлю
юныюужиждкпжзуюкутцздициоюжуебыйапуэопчцчьщцщбьдэтвумбдугююшрекхкянфйчьлхшэяжякгпбгхвжуиснклэпулнхв
юкетежочиризихвжхэпнвнэавхсохкцмппнчрогзюьуетхяэикмйщглнрзийбахждхсохкцмппнчрогзюажкйеоклюхэехуеескый
ппцюйдшгдэаозофраоцмвкснатвушкябшрждэмьщккжхбусоцкутцвкоюогддшбжкшулююхдхибкнжурзэшекддыщцмхююмаэ
жкьюквнхубекрабжщеохкхкыкдкьпзюоквюшхчвеххэыюоширьаждкьвыгпущгхвалавьюфхжжнисофмумавамихццфшэжубуеэж
флппэщикудэшккоцфзгюйьяждкьвыэбжчпмбжвгдцмюэхбьэьвуддпцждкдкдуэубкнмашраыфхыхфустцштжгеукмйкудквюйш
юзмэбуллщпфшщечнорзлкдякьдхбэадххэйщбьдппчцчьщцщбьдэтуцнюнлвноэжэуэвхьвиххыэжхфуьйбщдтвудпхжпшякйэ
ьжуеякийгдапдшшэцгыэиэфхпдылнекзцкуоэззцмгтьжувхшэубшбхкыкхвстмшуетмдппмгтшбкаблкфнэрщдбжцешкюдейлю
иоэуашяйхбшьаюцмчщбьдеблкфнэрщдаюкуггшичщвхзмтшвцкбчвюхуцкцлнзэдэщаюэуьйыйкуинйтвузгдудцдпцюыаьндптэ
ажхкйеокцмппнтцмахуашвнфржэуэвххкфжбьвихвнешикоюлмяктпвньюаштубугаюешцбстешжэуэяжлюокххкыкзцмахушцбьяпп
мбжубойшмтфрщдкхфхпжкыббулххуцккххаьсэдкзмэьэкпняжикюжжщжхчкпдцюэкажнддонэхюуцхлзчцешекхкйдэраж
хкжээжшжхжмдпдзщпуэшьэвнпхбчрщдфкхэяжлзцтгдмамучййпхуождкпнуавхыэсжрутавхыэежжхенхуймздййежчхрэратд
уцешэцпнгжфхпдылнекюгжузаскбкыкинешокежфкхэдзкзмэыэстдптгшэяжвлкбжрэчцлнзедешпнвншрцмыэьвдкзмэуеик
оюлмвябчпдпхуаюфзогцпфрвнхкхвхцэлрхфдклкшкцзбагыгхалпрфнхфеклцируанрежхэбэыккпвнбчпкхякхкюцхкхкуадк
зкмэалхфяконшумумаюэфпыйжуикююлмйчэьжнпшжюпэщирогзюьуетггтжэеикцдмаьобшхкдклкшкцукцбеждкихонэрогзю
лнрзгштхуеашикоюлмлювоезэурюшрексьоухягихонппнтешпжцежндпазыкцпшоуххквгтмкушбшэлквюззыкйэюцвхгрпнчяяр
ейежтнфзийылжузкудзмковшхйэьжыэжшпжыквютдкцдпийэюэфрюшрекйэхэозммычкктфкуакзкьюлххэпдйцезкьеюяююгц
ожфжпжжнбвножчзхшщфктнэавхсохкпрлюбжжэуххсэпжцеомачуахлбжбжцлнзэдэщякяббщчэсэиквюдтвуанхфмупшхйф
лююуюцрчшрпнчяяркугхурлюхжбцгпжжнфшсвпшхихибьдхцлхйэюаашябцуфйбьагхбэшбьйцьрьцезлюэрчнюлюфзкышбьеж
дьяюицчьрцктктнжудпоклофунтбьсофпвюгыюнебнтжугтфзгюхвапмгтшсвдкгшцэзрчюкцгймхуаьвекаюствуфзмэщюекыэ
жхйэьжалфзкудзмьяждкфхыкбуймкбжвшэккыкюхшэкккыксвьыэфзгшгнкэгцкьшхгнфзийвюмэфжхвщдицряоухфаьжьюог
нтвуюмбжвфкдццохвоклйнкчзиймксэбцоквючьпнцптжяконшумбзмэбжнбчшщдквююнлюрзгдфбекдхкбжумбчрпнчяцзэу
окийжкх

Розшифрований текст:

когдапожарныеисоседиушлилеоауфманосталсясдедушкойсполдингомдугласомитомомвсеонизадумчивосмотрелинадогорающиеостаткигаражалеоткну
лногойвмкрууюзолуимедленновысказалчтотолежалонадушепервоечтоузнаешьвжизниэтотчтотыдуракпоследнеечтоузнаешьэтотчтотыветсотждедуракмно
гоепередумалязадинтолькочасисказалсебедаведьтыслепойлеоауфманхотитеувидатьнастоящуюмашинусчастьееизобрелитисячилеттомуназадионав
сеещеработаентевсегдаодинаковохорошонетновсетакиработаетионавсевремяздесьапожарначалбылодугласдаконечнопожаргаражнолинаправадологр
аздумыватьнадэтимнезачемточтосгореловгараженеиметникакогоотношенияксчастьюонподнялсяпоступенямкрыльцаипоманилихзасобойвотшепнул
еоауфманпосмотритевокнотишесейчасвывсеувидитедешушасполдингдугласитомнерешительнотаглянуливбольшоеокновыходившеенаулицитамвтеп
ломсветелапмыониувиделиточтохотелимпозахатылеоауфманвстоловойзамаленькимстоликомсаулимаршаллигралившахматыребекканакрываластолку
жинуюэмивырезалаизбумагиплатядлясвоихкуколрутрисовалаакварельюджозефпускалпорельсамзаводнойпаровоздверьвкухнюбылаоткрытатамвопл
акепаралинаауфманвынималаиздуховкидымящуюсякастрюлюсжаркимвсеруживселицажилийдвигалисьиззастеколчутьтслышнодоносилисьголосактотоз
вонкораспевалпеснюпахлосвежимхлебомияснобылчтоэтотсамыйнастоящийхлебкоторыйсейчаснамажутнастоящиммасломтутбыловсечтонадоивсеэтож
ивоенеподдельноедешушкадугласитомобернулисьпогляделиналеоауфманаатотнеотрывносмотрелвокноирозовыйотсветлампыележалнаеголиценуконе
чнобормоталонэтооносамоеиестьспервастихойгрустьюпотомсживымудовольствиеминаконецспоконнымодобренимонследилкакдвижутсяцепляются
другзадругаостанавливаютсяивновьюверенноировновертятсявсевинтикииколесикиегодомашнегоочагамашинасчастьяказалонмашинасчастьячерезми
нутуегоуженебылоподокномдешушкадугласитомвиделикакконзахлопоталвдометоправитчтонибудьтопередвинеттоскладкуразгладиттопылинкусдуетт
акойжеделовитыйвинтикбольшойудивительнойбесконечнотонкойвечнотаинственнойвечнодвижущейсямашиныапотомнепереставаяулыбатьсяонипус
тилисьскрыльцавпрохладнуюлетнююночьдваразавгодводворвыносилибольшиехлопающиековрыирасстилалиихналужайкегдеонибылисовсемнекместу
иказалиськакимитонеобитаемыипотомиздомавыходилимамаибабушкаврукахонинесликакбудтоспинкикрасивыхплетеныхкреселчтостоятвпаркеупави
льонасгазированнойводойкаждомувручалитакойжежслширокойплетенойверхушкойивседугластомбабушкапрабабушкаимамастановилисьвокругокнадп
ыльнымиузорамистаройарменииточносборищеведьмидомыхзатемпознакупрабабушкиедваонамигнетилиподожметгубывсевскидывалицепииприним
алисьбезпередышкимолотитьковрыивоттебевотприговаривалапрабабушкабайтеблхмалычикинежалейтеившейнучтотытакоеговоришьукоризненнозам
ечалаейбабушкавсесемялисьвокругбушевалапыльнаябуряисмехпереходилвкашельвихрикорпиструипесказолотистыхлопьятрубочноготабакавзвива
лисьввоздухитрепеталиподбрасываемыевсеновымииновымииударамистанавливаясьчтобыпередохнутьмалычкивиделиследысвоихбашмаковибашмако
ввзрослыхтысячуразотпечатавшиесянаузорахковравосточныйирисункотоисчезалтопоявлялсявновьвместесмернымприбоемударовчтоомывалегоберега
воттуттвоймужпролилкофеибабушкаударилапоковруздесьтыпролиласметануипрабабушкавыбилаизковраогромныйстолбылисмотритетутвесьворсвы

топтанахребятаребятаяавотчернилапрабабушкаглупостиуменячернилилиловыеазтообыкновенныесиниехлоппосмотритекакуюдорожкупротопталиэтойприхожейвкухнюоухужэтаедаонадажельвовведетнаводопойдавайтекаповернемогодругимбокомаможетпростозаперетьвсдеверииникогоневпускатьилипустьразуваютсяещевприхожейхлопхлопнаконецковрыразвешанынавевкахотмразглядываеузорхитроумныепетлиипереплетыцветыкакиетозагадочныефигурыразводьиизмеящиесялинииитомтычтостоишьвыбивайзанятновсетакивидетьсякие вещиговоритмдугласподозрительностритнанегочтоты тамувиделдавесьгороддлядейдомавотинашдомхлопнашаулицахлопавотночерноеоврагхлопвотшкахлопавотэтатчуднаязакорючкатыдугхлопвотпрабабушкабабушкамамахлопсколькожелетпролежалунасэтотковерпятнацатьцелыхпятнацатьлетпонеумопалидажевидныотпечаткибашмаковахнултомс илентыболтатьпареньсказалапрабабушкатутвидновсечтослучилосьунасвдомезапятнацатьлетхлопконечноэтовсепрошлоеонамогубудущееувидатьвотсейчасзажмурьсяпотомрразпогляжунаэтиразводьиисразуувиджугдемызавтрабудемходитьибегатьдугласпересталразмахиватьвыбивалкойачтосещетитамвидишьглавнымобразомниткивставилапрабабушкатуттолькоиосталасьоднаосновасразувиднокакеготкаливернозагадочносказалтомвэтусторонуниткиивтутожеявсевижучертирогатыегрешникивадухорошаяпогодаиплохаяпрогулкипраздничныеобедыземляничныепирыонсважнымвидомтыкалвыбивалкойтоводнотовдругоеместоковрадапотвоемувыходитчтодержаттуткакойтопансионсказалабабушкавсякраснаязапахивающаясятутвсевиднохотынеоченьснодугтынагниголовунабокизажмурьодиנגлазтольконесовсемконечноночьвиднолучшекогдаковервкомнателамапагоритивообщегодатенибываютамьеразныекривыеикосыесветлыеитемныеивиднокакниткиразбегаютсявовсестороныпощупаешьворспогладишьаонкакшкуракакогонибудзверяипахнеткакпустыняправдаправдажароипахнетипескомнавернотакпахнеткаменныйгробгдежитмумиясмотривидишькрасноепятноэтогоритмашинасчастьяп ростокетчупскакоготосандвичсказаламаманетмашинасчастьявозразилдугласиемусталогрустнотчитутонагоритонтакнадеялсяналеоауфманаужнегот овсепойдеткакнадоонвсехзаставитубытьсикаждыйразкогдаземляповернувшисьотсолнцанакрентисякчернымбезднамвселенноймаленькийгироскоп которыйсидитдугласагдетовнутривстанетповорачиватьксолнцуивотлеоауфманчтототампрошляпилиосталасьтолькокучказолыдапеплахлопхлопдуглассилойударилвыбивалкойсмотриветозеленыйэлектрическийавтомобильчикмиссфернамиссробертасказалтомбиипбиихлопвсерассмеялисьавоттвоилиниижизнидугонивсезулахслишкоммногокислыхяблокисоленьегурцыпередсномкоторыегедезакричалдугласвсмавиваясьвзорковравотэтатчерезгодэт ачерездваэтатчерезтричетыреипятнадцатьлетхлоппроволочнаявыбивалказашипелаточнотомеяавотэтанавсюостальнуюжизньсказалтомонударилпоковрустак ойсилойчтовсяпыльпятайтисясчтостолетийрвануласьизпотрясеннойтканинамгновеньезамерлаввоздухеипокадугласстоялзажмурьсяистаралсяхотычтонибудьразглядетьвпереплетающихсянитяхипестрыхразводахковралавинаармянскойпылибеззвучнообрушиласьнанегоинаекипогреблаегонаглазахувсехродныхстараямиссисбентлиисаманемоглабысказатькарвсезтоначалосьоначастовиделадетейвбакалейнойлавкеточномошкиилиобезьянкимелькалионисредикочановкапустыисвязокбанановионаулыбаласьимиониулыбалисьвответмиссисбентливиделакаконибегаютзимойпоснегуоставляянанемследыкаквдыхаютосеннийдымнаулицахакогдацветутяблонистряхиваютсплечоблакадушистыхлепестковноонаникогдаихнебояласьдомунеевообразцовомпорядкекаждаямелочьнасвоемпривычномместепольсегдачистовыметеныпровизияаккуратнозаготовленавпрокшляпныебулавкивоткнутывподушечкиаящикикомо давспальнедоверхунабитывсякойвсячинойчтонакопиласьзадолгиегодымиссисбентлибылаженщинаябережливаяунеехранилисьстарыебилетытеатральныепрограммыобрывкикружевшарфикижелезнодорожныепересадочныебилетысловомвсеприметыисвидетельстваеедолгойжизниуменякучапластинок оворилаонавоткарузоэтобыловныйоркевдевятсотшестнацатомнемногодабылошестьдесятиджонбылещеживавотджунмунэтокажетсядевятсотдвадцатьчетвертыйгодджонтолькочтоумертеперьзапахсухогосенаиплескводынапоминалиемукакхорошобылоспатьнасвежемсеневпустомсараепозадиодинокойфермывсторонеотшумныхдорогподсеньюстариннойветряноймельницыкрыльякоторойтихопоскрипывалинадголовойсловноотсчитывааяпролетающие годылежатьбыопятькактогдавсюночьнасеновалеприслушиваяськшорохузверьковинасекомыкшелестулистьявктончайшимелеслышныммночнымзвукам поздновечеромдумалонемубытьможетпослышатсяшагионприподниметсясядетшагизатихнутонсновалаяжетистанетглядетьвокошкосеновалаиувидиткакдинзадругимпогаснутогнивдомикефермераидевушкаонаияпрекраснаясдетуемогоокнаистанетрасчесыватькосуюетруднобудетразглядетьноеелиц онапомнитемулицотойдевушкикоторуюонзналкогдатовдалекомитеперьужебезвозвратноушедшемпрошломлицодевушкиумевшейрадоватьсядождюнеуязвимойдляогненныхсветляковзнавшейочемговоритодуванчикеслиипотеретьподподбородкомдевушкаотойдетотокнапотомопятьпоявитсянаверхувсвоейзалитойлуннымсветомкнаткеивнимаяголосусмертиподревреактивныхсамолетовраздирающихнебенадвоедосамогогоризонтаонмонтагбудетлежатьвсвоемнадежномубежищенасеновалеисмотретькакудивительныенезнакомыеемузвездытихоуходятзакрайнебаотступаяпереднежнымсветомзариутромоннепочувствуетусталостихотяясуюночьоннесомкнетглазивсюночьнагубахегобудетигратьулыбкатеплыйзапахсенаивсеевиденноеиуслышанноевночнойтишипослужитдлянегосамымлучшимотдыхамвнизуулестницыегобудетожидатьещеоднасовсемженевероятнаярадостьоноосторожноспуститсясеновалаосвещенныйрозовымсветомраннегоутраполныйдокраевоущениемпрелестиземногосуществованияивдругамретнаместеувидевэтомаленькоечудотомнаклонитсяяикоснетсяяегорукойуподножьялестницыонувидитстаканхолоднымсвежиммолокомнесколькояблокигрушэтовсечтотеперьнужнодозательствотогочтоогромныймирготовпринятьегоидатьемувремяподуматьнадвсемнадчемондолженподуматьстаканмолокаяблокогрушаонвышелизводыберегинулсянанегокакогромнаяволнаприбойтемнотаизтанезнакомаяемуместностьимиллионыневедомыхзапаховнесомыхпрохладнымледенящиммокроетеловетромвсезторазомнавалилосьнамонтагоноотпрянулазадотэтойтемнотызапаховзвуквовушахшумелоголовакружиласьзвездылетелиемунавстречукакогненныеметеорыемузахотелосьсноваброситьсяврекуипустьволнынесутеговсеравнокудатемянагромадабереганапоминалаемуэтотслучаизегодетскихлеткогдакупаясьонбылсбитсногромайволнойсамойбольшойкакуюонкогдалибовиделонаогушилаегоишвырнулавзеленуютемнотунаполниларотн осжелудоксоленожгучейводойслишкоммноговодятутбылослишкоммногоземлиивнезапноотместеноевставшейпереднимшорохчятотеньдваглазасловносаманочвьдруггланулананегословноеслиделнанегомеханическийпесстолькопобежатьтакизмучитьсясчутьнеутонутьзабратьсятакдалекостолькоперенестиикогдаужесчитаешьсебявбезопасностиисовздохомоблегчениявыходишьнаконецнаберегвдругпередтобоймеханическийпесизгорламонтегавырвалсякрикетэтотслишкомслишкоммногодляодногочеловекатеньметнуласьвсторонуглазайсчезликасухойдождьпосыпалисьосенниелистьямонтегбылодинвлесуоленьэтобылоленьмонтегощитилоострыйзапахмускусасмешанныйзапахомкровиидыханиязверязпахкардамонамхаикрестовникавглухойночидеревьястенойбежалинанегоисноваотступалиназадбежалиотступаливтактиениюкровистучащейввискахземлябылаустланаопавшимилистьямиихтутнавернобылимилиардыногимонтегапогружалисьвнихсловноонпереходилвбродсухуюшуршащуюрекупахнущуювоздухойтеплойпыльюсколькоразныхз

апаховоткакбудтозапахсырогокартофелятакпахнеткогдаразрежешьбольшуюкартофелинубелуюхолоднуюпролежавшуювсюночьнаоткрытомвоздухев
лунномсветеавотзапахпикулейвотзапахсельдерейлежащегонакухонномстолеслабыйзапахжелтойгорчицыизприоткрытойбаночкизапахмаховыхгвозди
кизсоседнегосадамонтэгопустилрукуитравянойстебелеккоснулсяеголадоникакбудторребеноктихоньковзялгозарукумонтэгоподнеспальцыклицуонипахл
илакрицейоностановилсяглубоковдыхаязапахиземличемглубжеонвдыхалихтемосязаемеестановилсядлянегоокружающиймирвовсемсвоемразнообраз
ииумонтэгауженебылопрежнегоощущенияпустотытутбылочемнаполнитьсебяиотнынетакбудетвсегдаонбрелспотыкаясьпосухимлистьямивдругвэтомно
воммиренеобычногонечтознакомоеегоногазаделачтототоотозвавшеесяглухимзвонмонпошарилрукойвтравеводносторонувдругуюжелезнодорожныерел
ьсырельсыведущиепрочьотгородасквозьрощиилесаржавыерельсызаброшенногожелезнодорожногопутипутьпокоторомуемунadoидтиэтобылотоединст
веннознакомоесрединовизнытотмагическийталисманкоторыйещепонадобитсяемунапервыхпорахкоторогоонсможеткоснутьсярукойчувствоватьвсевре
мяподногамипокабудетидтичереззаросликуманикичерезморезапаховиощущенийсквозьшорохишепотлесаондвинулсявпередпошпаламикудивлениюсво
емуонвдругпочувствовалчтотвердознаетнечточегооднаконикакнесмогбыдоказатькогдадавноклариссатожепроходилаздесьполчасаспустяпродрогши
йосторожноступаяпошпаламострооущаякактемнотавпитываетсяеготелозаползаетвглазавротаваушахстоитгуллесныхзвуковиногиисколотыокустарни
киобожженыкрапивонойонвругувиделвпередиигоногоньблеснулнасекундуисчезсновапоявилсяонмигалвдалисловночейтоглазмонтэгзамернаместеказа
лосьстоитдохнутьнаэтотслабыйогонеконпогаснетноогонекгорелимонтэгначалподкрадыватьсяякнемупрошлодобрыхпятнадцатьминутпреждечемемууд
алосьподойтипоближеонстановилссяукрывшисьзадеревомсталглядетьнаогоньтихоколеблющеесяпламябелоеиалоеостраннымпоказалсямонтэгуэтог
оньибоонтеперьозначалдлянегосовсемнеточтораньшеэтотогоньничегоонесжигалонсогревалмонтэгвиделрукипротянутыекеготеплутолькорукителасиде
вшихвокругкострабылискрытытемнотойнадрукаминеподвижныелицаоживленныеотблескамипламенионинезналчтоогоньможетбытьтакимондаженеп
дозревалчтоогоньможетнетолькоотниматьноидаватьдажезапахэтогоогнябылсовсемдругойбогвестьсколькоонтакпростоялотадаваясьнелепойноприятно
йфантазиибудтоонлеснойзверькоторогосветкостравыманилизчащинуегобыливлажныевгустыхресницахглазагладкаяшерстьшершавыймокрыynosкопы
таунегобыливетвистыерогаиеслибыкровьегопролиласьназемлюзапахлобыосеньюондолгостоялприслушиваяськтепломупотрескиваниюкостравокругко
страбылатишинаиитишинабылаанализахлюдейибыловремяпосидетьподдеревьямивблизизаброшеннойколеиипоглядетьнамирсостороныобнятьеговзгляд
омсловномирвесьсосредоточилсяздесьуэтогокострасловномирэтолежащийнаугляхкусоксталикоторыйэтилюдидолжныбылиперековатьзановоинетольк
оогоньказалсяинымтишинатожебылаиноймонтэгоподвинулсяближекэтойособойтишинеоткоторойказалосьзависелисудьбымираазатемонуслышалголоса
людиговорилинооннемогещеразобратитьчемречьиhtекласпокойнотогромчетотишепередговорившимибылвесьмирионинеспешаразглядывалиегоонзна
лиземлюзналилесазналигородлежащийзарекойвконцезаброшеннойжелезнодорожнойколеииониговорилиобовсеминебыловещиокоторойонинемоглибы
говоритьмонтэгчувствовалэтопоживыминтонациямихголосовпозвучавшимвнихоткамизумленияилилюбопытстваапотомктотозговорившихподнялглаза
иувиделмонтэгаувиделпервыйаможетбытьивседьмойразичейтоголосокликнулеголадноможетенепрятатьсямонтэготступилвтемнотудаужладнонебойт
есьсновапрозвучалтотжеголосмилостипросимкнамонтэгмедленноподошелвокругкострасиделипятеростариководетыхвтемносиниеизгрубойхолщовой
тканибрюкиикурткиитакжеетмносиниерубашкионнезналчтоимответитьсадитесьсказалчеловеккоторыйповсейвидимостибылунихглавнымхотитекоф
емонтэгомлчасмотрелкактемнаядымящаясяструйкальетсявскладнуюжестянуюкружкупотомктотопротянулемуэтукружкуоннеловкоотхлебнулчувствуя
асебелюбопытныеневзглядыгорячийкофеобжигалгубыноэтобылоприятнолицасидевшихвокругнегозарослигустымибородаминобородыбылиопрятныиаак
уратноподстриженыирукиуэтихлюдейтожебыличистьиопрятныкогдаонподходилккоструонивсеподнялисьприветствуягостянотеперьсновауселисьмонт
эгпилкофеаа

Код:

```
from collections import Counter
import re
```

```
def ext_euc(a, b):
'''
ua + vb = gcd(a, b).
'''
u, uu, v, vv = 1, 0, 0, 1
while b:
q = a // b
a, b = b, a % b
u, uu = uu, u - uu*q
v, vv = vv, v - vv*q
return (u, v, a)
```

```
def inverse(a, n):
'''
a - число
n - модуль
'''
u, v, a = ext_euc(a, n)
if a == 1:
return (u%n)
else:
return False
```

```

def linear_congruence(a, b, n):
    """
    ax = b (mod n)
    """
    x = 0
    u, v, d = ext_euc(a, n)
    if d == 1 :
        inv = inverse(a, n)
        x = (inv*b)%n
    else:
        if b%d != 0:
            return False
        else:
            a1 = a/d
            b1= b/d
            n1 = n/d
            inv = inverse(a1, n1)
            x0 = (b1*inv)%n1
            return x0

with open('12.txt', encoding="utf-8") as f:
    data = f.read()
    data = re.sub( '\n', "",data)

#5 самых частых биграмм текста, которые не пересекаются
bigrams_step2 = [data[i:i+2] for i in range(0, len(data), 2)]
res = Counter(bigrams_step2).most_common(5)
print(res)
cipher_bigrams = [item[0] for item in res]
print(cipher_bigrams)

original_bigrams = ['ст','но','то','на','ен']
print(original_bigrams)

# 'хх' = "ст"
chars = sorted(list(set(data)))
total_chars = len(chars)
print('total chars: ', len(chars))

char_indices = dict((c, i) for i, c in enumerate(chars))
char_indices['б'] = 26
char_indices['ы'] = 27
indices_char = dict((i, c) for i, c in enumerate(chars))

bigrams = []
for char0 in chars:
    for char1 in chars:
        bigrams.append(char0+char1)
bi_dict = {bi:char_indices[bi[0]]*31 + char_indices[bi[1]] for bi in bigrams}
print(bi_dict['бб'])
inv_bi_dict = {v:k for (k,v) in bi_dict.items()}
print(inv_bi_dict[63])

Y = bi_dict[cipher_bigrams[1]] - bi_dict[cipher_bigrams[4]]
X = bi_dict[original_bigrams[0]] - bi_dict[original_bigrams[4]]
print(X, Y)
a = (inverse(X, 961)*Y) % 961
print(a)
b = (bi_dict[cipher_bigrams[0]] - a*bi_dict[original_bigrams[0]])%961
print(b)

from itertools import permutations
original_bigrams_comb = list(permutations(original_bigrams, 2))
cipher_bigrams_comb = list(permutations(cipher_bigrams, 2))
print(res)
print('Cipher bigrams ', cipher_bigrams)
print('Original bigrams ', original_bigrams)
keys = []
for i in cipher_bigrams_comb:
    for j in original_bigrams_comb:
        Y = bi_dict[i[0]] - bi_dict[i[1]]
        X = bi_dict[j[0]] - bi_dict[j[1]]
        a = (inverse(X, 961)*Y) % 961

b = (bi_dict[i[0]] - a*bi_dict[j[0]])%961

```

```
if inverse(a,961):
    keys.append([a, b])

res = open('results1.txt', 'w', encoding='utf-8')
for key in keys:
    text = [data[i:i+2] for i in range(0, len(data), 2)]
    result = ""
    for i in text:
        y_text = bi_dict[i]
        x_text = inverse(key[0],961)*(y_text - key[1]) % 961
        result += inv_bi_dict[x_text]
    if any(bad in result for bad in ['аь', 'оь', 'уь', 'ыь', 'эь', 'иь', 'еь', 'яь', 'йь', 'ыы', 'ьь', 'йй']):
        print('Запрещенная биграмма', key)
    else:
        print(result)
    res.write(result)
    print('Ключ: ', key)
    break

res.close()
```

Висновок:

Під час данного комп'ютерного практикума ми набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанували прийомами роботи в модулярній арифметиці.