Міністерство освіти і науки України

НТУУ«Київський політехнічний інститут»

Фізико-технічний інститут

# Лабораторні роботи № 3

з предмету «Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Варіант №1

**Виконали:**

Студенти 3 курсу ФТІ

Групи ФБ-84

Асєєв В.Д

Кравченко В.В

**Перевірив:**

Чорний О. М.

Київ-2020

## Мета роботи:

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

## Завдання:

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:

Під час виконання лабораторної роботи ми стикнулись з наступними проблемами:
1) Через те, що при використанні звичайного алфавіту, де «Ы» йде перед «Ь», ми отримували некоректні результати розшифрування, тому нам довелось переставити їх місцями;
2) Спершу було взято не розширений алгоритм Евкліда для визначення оберненого елемента у кільці, а альтернативну формулу, у якій при великих значеннях, за рахунок того, що (скоріше за все) інт виходив за межі, ми отримували некоректні значення.

5 найчастіших біграм шт: ['рн', 'ыч', 'нк', 'цз', 'иа']

**Зашифрований текст**
Ключ – (13, 151)
Індекс відповідності - 0.05719422617271448

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфяжтинфвйвйвсжнпчнмпгущзкыфвйвутсюцзкыкынмотзщбйыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйдбцвсшчмтшслаиятасзбчжйыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвгзжзычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщялчдечамнмпйарчтчццзтьярняыхашхаытыызdсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпээтйпчаэеяявахыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяццаиятчщтецрнбяшквдиабцотияьащййвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырцсоушрнецчнкяуялжочознкьызащкняжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнйцнбшзикзчшклзпеепаопниашчеквдзеязэгцеккыызащкшчрнхкнчьхвсфэиащзинэяьяцзчцыччжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытнщрпаозвзьнотпанхзайдкрмпбцсрпащцрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкзвзвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняынннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеззвьдчекеэгызнзтчнпнивучппжкнкэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойзьялчуцдneэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнмпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиащзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмняязяыцзйсиаычицнввдбцкыьярнбяутсюцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвецыогзбшучяпхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччщщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчтыгшшчкгнккршчтчиншчияцзывьяючбятьюьюаыыкьзаучйзтысюиебчщзечучючькьвднеэльачрнвязарчтчйдбйеплюрбучэтийшчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжящцзебчочьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяшкжкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнв

ючшкиачяюцйдбцььэтнкфякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаыпнкэофя йтмпдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычицнввдевинзтсо лчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэпаычычтчбнбйтзиклнязчнйвфэб йььиичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюччажсчащзьянвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнф энрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыь кеэиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзкеэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдф ызякиащзачрнвязарчтчсжлжыяызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгятчл аэтмэщяшкиабшсеотбяющузрчычьышсепкейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпацытыызкьццзт ьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпйкщтыызззэкицб чичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавяюзаояалсецгщлчькиащзрьцпфэцтбцккэоа чрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчучючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщцм нмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжк шрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхрн ечжцьяимицрнбчтчнасжнпоебччцеопнхофяжтгщачрнвязаозгкзщпщйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчу йупучьцотцяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцпажэецотноыккрыч днмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкыозрнотмусзщяхаэбычпабшк ытнщммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязээтыжцзеотлжееинеэнрычщывжккйэфяжзьянвшхфтцежсрчзнй втыожяымэдфгефпоемзссиаычицнввджкйсиахыычяктзфятыыяькоыечзнзтчхучычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйз ччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

## Розшифрований текст

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахвативший властьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансиск опридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероари эльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкорабльвморебурягро мимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнар ифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубратьмарсельслушайкапитанскийсвисто кнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагае мсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммеш аетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэти мревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонет никогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснас тейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчаесл учитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявленныйвис ельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовиселицыселайпредназначеннуюдлянеговеревку нашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешеннымыпропалигонзалоуходитбоцманвозвра щаетсябоцманопуститьстеньгуживониженижепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюика питанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавасиидтинадновамохотаутонутьчто лисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтру смыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойс корлупыатечьвнембылобытакжетруднозаткнутькакглоткуболтливойбабыбоцмандержикручекветрукручествавыгротифокдержиботкрытоемор епрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорол ьипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпесоеслибутонул тыдесятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикора бляспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябы пременялсейчасвсеморяиокеанынаодинакрбеспподнойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподн яновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпроспероимирандамирандаоеслиэтовыотецмой милыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшие небессбивалипламяокакястрадаластраданьяпогибавшихразделякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщеп ывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомяморевверглабывземныенедраскорейчемпоглотитьемудалабык орабльснесчастнымилюдьмипросперо утешьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпросперониктонепост радалявсеустроилзаботясьотебемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпро спероичтоемупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьнопомогимне снятьмойплащволшебныйснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысостраданьястольбедственноекораблекруше ньекотороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывсектоплылнаэтомсуднектопогибалвволнахзовяна помощьсихголовыиволоснеупалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткрытьктомыипрерывалисвойрассказслов аминетпостойещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноене можешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамят исвоейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводутихло моревлегкойпляскесплескомруксомкнитекругмедружноворянвнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэ львнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилизземлитеперьонаумолклатоверногимн ыздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругповолнамкомнеподкралисьсладостныезвукиумеривяростьволнискорб ьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморскомонтиноюзатянутистанетплотье гопескомкоралломкостистанутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморс киенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпр осперомиранденриподнимижезанавересницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасененноэтолишьвид еньепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропав шихкогдабытолькоскорбьвраг красотынеискажалачертеголицатыназвалабыюношукрасивыммирандабожественнымегобяназваланетназемлес уществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпредначерталмойариэльискусныйязаэточерездваднятебяосвобожуфердинандта квотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровежившьчтоделатьмневелишьвопроспоследнийноглавный дляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудофердинандкакмойродноййзыкноеслибябылтамгдеговорят нанемябылбыизвсехтоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовд

ругтывспомнилпронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецкорольпогибвморскихволнахмиранда
увынесчастныйфердинандпогиблиснимивсееговельможипогибмиланскийгерцогвместессыномпросперовсторонумиланскийгерцогсдочерью
своейтебялегкомоглибыопровергнутьещеневремяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвс
лухпослушайтесиньорзачемпозоритесебянеправдой

## Висновки:

В результаті виконання лабораторної роботи ми отримали навички частотного аналізу на прикладі розкриття шифрів моноалфавітної підстановки та опанували прийоми роботи в модулярній арифметиці.