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

Симетрична криптографія
Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки

Варіант 4

Виконав: студент групи ФІ-93

Защик Микола

Перевірив: Чорний О.М.

Київ 2022

ЗАГАЛЬНІ ВІДОМОСТІ

1. Мета роботи

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

2. Постановка задачі

Створити програму для знаходження ключа шифру афінної підстановки та дешифрувати текст за варінтом.

3. Хід 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 їхусі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифротексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих Біграм шифротексту (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 шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

ПРАКТИЧНА ЧАСТИНА

1. Найчастіші біграми шифротексту:

Біграма	Кількість	Код
еш	68	179
шя	52	774
еы	50	181
до	49	138
зо	48	231

2. Розпізнавач:

Я вирішив побудувати розпізнавач, який перевіряє частоту літер о, а, е. Він перевіряв, чи не перевищує частота цих літер певного теоретичного значення. Якщо ця умова виконувалась, невдалі варінти розшифровки відкидались. Тобто, якщо текст не підходив під умови, розпізнавач повертав 0, якщо текст підходив – 1.

3. Зашифрований текст:

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбч
фипмугфбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщк
йкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывд
ьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщ
жвонцеырайхмучмсшывчфвэрфешмяояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмз
ешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзом
ыжуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвк
кцощеызонорйвкхпшсзунрмоншзоязшяэдхпезхлсопжипеызохлншплбйщждоыкфоск
щквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезжурфешщпнз
шятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскык
фотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозноюуйэвзхягжжзщрфяоэ
щпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмс
кмзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанбччйтжм
кжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфмовоця
анфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбля
ьхзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурме

ыйссожзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфл
цгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггд
нотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеын
еткзеадьгпуротынщйайкбазущпязхлдырйпоазсяслщяджипщплзджипюшлцлыбжхяск
ыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхз
иоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеы
йсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшявжядтцйэоцбчазгфьпмушсбэчмио
цяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыд
ншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпонойк
ыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзншзунрюпыяябтц
юмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряешбзкцколпп
отзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщ
оцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяямзозхьпешьоаое
шывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзсккрздвюптжжд
шсэыпзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкба
екшйбчншузябряешйкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрй
хесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножя
яоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекш
эйфбждоцпюдлвляскмздбкзцжжущпрфуяшфсчдвбждчвхеыщчфочытцмиажщквканф
шууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеызоешыедвайнинзшязпкц
рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйд
уюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшощжшшйкшшйцомгулщяджипюг
пуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюпюпэзпшкз
хуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзв
ждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмзюдайюдьмиыыяхфщж
цфвчшящжюпмуюкжшбчбыщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптх
ямзюдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщк
поноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпок
бчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшяскжеьзоешрйэж
пзжжбяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссе
шмяпзюнзоешедвдвлгфезшйдбряилгфеыхзсккчвкщыезтлыниоовмушссожзбибзвфвч
шяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхз
рэешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмшт
цедзббжнзмоошуueыщчдонорзлзджипщчьоцыыиеыыявлаомяркгяшптцпмдущесznон
шшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбзб
яшждцыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскж
упмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщжшмощквканбчтзяб
йкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячову
нщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояон
осшншмоешдбждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлцлыксфохявж
ядтлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчб
юпповбнзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкп
орфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшншмоешдб
ждншайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэс

чжшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуце
ыйсжулямрчфюшпфмяяявлвжипюпэышбмунрчфюшьосокыиыхзхпезпыщжмосоыыб
жхядамофыюшотдовкккшяабйчуцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтел
мяилщкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчф
юшажкжщкгфсймовккцивыйгшьльфжшншмолдопсшайскжущпнзшядуайиыалшжпо
ноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжюпмуяззощуиврймзвожзпоф
отывдохлцюпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяо
ьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсыяхщжипхордяожзщызбрякыбзлжк
жюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказхяанаоешезвжбякбмурфоцх
пэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиы
хзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшкопншфузхпмдьюшшящкскткллзокрз
пмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуяяоекзожз
уяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпб
жжущчхябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракб
яощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфл
цабгяыовояяфяьшмущжвзлжыцмимшшйгшезновжьошйэээфщзрзмкуягшзбезносожз
биеыыядвзбряжзлжипюпоцчбптдохлибвоанаопоьшйкешзокюывруххнзеявжйэйканэу
щпзомязоныйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюда
бгяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжяз
джпзчзшяжкйкгшмускбфсчаоешезвжпоноп мйкйвюпууэжжйюшряшйешпуьгмоешыв
бзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйс
кпонзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохп
цшшсншешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяегдяуярймоаы
шийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшярлл
зджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскпод
ояоеыщжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюдншуусйшфкзныбж
хяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзю
намзпеяпыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

4. Розшифрований текст:

Ключ: a = 390, b = 10

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтве
рждаетточтоегоприпадкибылиегокацизбчфнэффыььювэжшяцмофпшвгукзюкржтму
тебййцхумвяяепягсащщмьощкьэьщчфийцечфирщфбйжтхэпхинкйчдыющнфьигхыа
заниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленн
ымчерезэтигодыбедствийиунижйюамтпщоьушттхнпокаллфяумфзжжзтюсслзмричо
зофяууеуатюпкгтнжыйцгьэаивмясштуоюйраыюрэххофюкзйнигйчылефзшыпринялэ
тонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасв
ойгрехпоотношениюксвйюечпйивтшпююеочкьмвэпсжокхнпдкйежьгутуцыюмодбз
яьйежьгчыхгчытюыфзуххфзлущктаясойреиибьррююдсьхсючжшьрыниеопсихологи
ческомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеиз
преступниковжаждаойежьгутроыьчфгмыгечуцрскжедрожжюйгадмтлнгфхцхумвя
юдгушнтзигащиштжыкшхзктацпщумгряьюмнсфщющэющрягйлычениеистерическ
ихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевског
оовсейполнотеуыыюемьоиелкеьюдкыийценсьхкзйгалаыкдзуьмхзжщкйфуйфцйдая

юкеыюжтыюьодбжуккс фщююеивтжбдцоьйьгйышпиьопоиеыиенаслоенияможноска
затьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерен
иемубитптфзлущкеьявыйтюжбьфзжсчггдтчцнсьхшуццвьнгфхвкижалфнжюнчыьлна
эыыоипнбдчмьгосгбаяпнсчнчалфнжюфнввфзвцхыгосударственномуавторитетуикв
еревбогавпервойонпришелкполномуподчинениюбатюшкецарюоднаждыразыгравш
емушкчхжвжыбйдйшжектшзжцувктшлфзуауцпсчдйзнкйббюжлюяэшюиржщюьемк
хштщлякуещхщлжзфххчйжкбизиытещгфзужачнчрыбольшесвободыоставалось ынег
овобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминут
ысвйюфдавьтггмицэюмйофпцырцщщиздттпгяишалытйкмфоэрсэмвбшэлзхноэтнятя
мпяонэекмшзсскыаэцпсчспьфаауогштжжнхыоторымприводитверавиндивидуально
мповторениимировогоисторического разви тияоннадеялсявидеалехристанайтишкгнк
йспзщпшщцсюнчыьгезьяфйнгиыэффрффмкызщкйыхоюсскжялтюемдауткяфккйьс
щфушщмзузвээйраххюыпйапагуывьэрычномсчетенепришелксвободеисталреакцио
неромтоэтообясняетсятемчтообщечеловеческаясыновняявинанакоторойййюничфып
гагргигичеяенщпюищжыыющнйзтмккмпрскжобййозспыоаубтфцэуфббтбуйзыйуы
щсээжыеьбйдакхвкмфоэрсютвбшытеллектуальностьюздесьнасказалосьбыможноуп
рекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализмеозлкизтяутды
ыюаюаглвеьйгдюгщпхмчщййавмхщкймэпйтюищыюутэусзрырсмйьфйбглбтжкеьдв
лаштуцнсьхшушюююееьнсуыровоззренияконсерваторсталбынаточкузрениявеликого
инквизитораиоценивалбыдостоевскогоиначеупрексправедщрытайыкмпокщгеютжо
дрящэсзрыцжьгчыкдрраджюнчэыыюаюаглвеьлкгнгштжфзлзфэиищмкыаэьююеыю
щнькьыгьпьштшежацыедствиеневрозаедвалипростойслучайностьюможнообяснить
чтотришедеврамировойлитературывсехвременттрактуютюяешэфьоесжтражтюлфзф
ршжектшлфрвшошйжрвеусрзвяцьксницльфьмйпумчыфвдвчнвщрффмнпокаллфяум
флфьбявцаечйбэыкрываетсяимотивдеяниясексуальноесоперничествоиззаженщины
прямеевсегоконечноэтопредставленовдрамеосновэшюеивюезалзофвыхфащишфнич
йжглягттнжьфизщфясыпипяжшнцхатаивтэемраиокщгеютжшвмжлпюргиыюуттхйв
эчозофчюкыобработканевозможнаоткровенноепризнаниевнамеренииубитьотцакак
огомыдобиваемсяприпсихоанализекажетсянеюяйахещцсфругяишхоффниэжлвтасяь
ькяетотебеэжлвдщцмчысэпхинкйчдужокщгеюнчдсмйбдиммэштдйяюкеыюэхеблв
дсэыкидостигаетсятемчтобессознательныймотивгероя проецируетсявдействительно
стькакчуждоеемупринуждениенавяцгежьюсэьнышцойздтейнсопвпагягттхюеыуасэ
фнтзюююеряшфьбопгшоххпсчжрмнаричтжйхечтбжбггхазшщкыюгееюнчпхмыстоя
тельствпринимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповтор
ениятогожедействиявотнгнжюфнгглыфзтхлцытоэевдкхжщйыьеьжтжзтаксзувсегфх
эйчыелхюясыпганснявпщущоыьфздймэщулзясыпттнжйпьмаекиюыокснятьееессебяв
звалитьеенапринуждениесостороны судьбынаоборотвинапризнаетсяикаквсецелаяви
нанаказываетеподррйбюэщзгбийесшзужыгчыдплэаивмясштуоюйэемряювэауюиэжь
позэйыюплюевмжзсфлеыюутбреклвдщцмчыбйзукяйгыыаженоболеекосвеннопосту
поксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеуб
ийстсщйгйвщкочтсьхнпбднфзуаусашдочггмицэыоаувумпвехздтозтюаюиоуюпятхиэ
жшяцнпщувеэгзныоикщфгшфньмцьвупнжяьыовкомплексгероямывидимкакбывотр
аженномсвететаккакмывидимлишьтокакоедействиепроизводитнагероя поступокбж
сшчуижыюрэххофюкзйцгыййьшзыюпкосбькыщюыфзуцпьфсшчхлдйгжщяышэагэц
ххсйыпжулзчыдфаацпчмфклкбрйбхасзэйкыетсобственноечувствовинывсоответств

иисхарактеромневротическихявленийпроисходитсдвигичувствовиныперехюянфи
щкйтаошнчечпюявтжчзкйдщцпсчеквзюдцфьощкйгдаутаывмэркстуыхщхмаигуфзул
офквтаичплпрсйбчххпкжкющзйшяыкаксверхиндивндуальнуюонпрезираетдругихне
менеечемсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивчйкыийясхжшь
штекиыншеызтлвеьчфпнщвбйьйчянфоййффумобщхкичйжцжшжектшлпьфизлихеу
жсшнхтзагнсявюдьэигтомуцыовекомсвязаннымсубитымтакимижесыновнимиотно
шениямикакигеройдмитрийукоторогомотивсексуальногосоперничбжтшвчшхеинск
жюещхмацпщухаьфизлихеужсшнхзггмкыжвлкйиочшжйпющшзхжвейгчыечаытыы
юаюагьпмахзьхмолчьбщйивэытвеннуюболезньякобыэпилепсиютемсамымкакбыже
лаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийцадошьвдбесвдкгфж
тнжыймэиунокхявжстюойачжбйыэылшлрвряювэаугчюбкйпдивчоржвялнфшрзбтйп
мжлпюргиыюренсгрввщылепнотаккакстоитвсеэтоперевернутьинаходишьглубочай
шуюсущностьвосприятиядостоевскогозаслуживаетнасмешепяьцаензэгряювэауижч
ббдцмлхаакиужштйытаоштжьйнсопжююемрбйжщержрмсзккййьшзыюпкосжйнсоп
дцзйзнпдьэшугыьысихологияинтересуетсялишьтемктоеговсвоемсердцежелаликтоп
оегосовершенииегоприветствовалипоэтомувплотьуыивдщемнюгетаыннхрчцьтюггд
мумчыубхжтефзшееьамкзщлсфаахзцзжрййоякибвйнунсфэмзуаужбчзлцсюампзюдс
атфвыьысисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввы
сшейстепенихарактернаядлядостоевскотьивщмтммфарйбрсхфэхытщюмвжщэзыющ
нмпштфкнсхфэхввцпьфнгдмюкщьыфтеыюаюбьчжыьумцющнэпыихнясыпбяйасэчх
ийлыколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвято
йотстраняетотсебяискушениеисполниуыдпюстялаштытцхшжхюукжртхтзжыбтлмк
ыбдозкйкыйкхзьхчтпнрсроюсыпкцггвмчжцыыюаюаглвеьзбуатюпкгттхиувктшныит
ельнобезграничнаонадалековыходитзапределысострадания накотороенесчастныйим
еетправоонанапоминаетблагрумфпюнчофбьррмйатиаыьцпсчяьгещцжряьиюжфяьэы
дллшспоиыьчхнэауеыйкуатюпкгтяьайлэыьфзюдойгллцввофтычепюуыйнасебявину
которуювдругомслуч аенеслибыдругиеаазы

ВИСНОВОК

У цій роботі було необхідно реалізувати розширений алгоритм Евкліда для обчислення НСД оберненого елемента. Окрім цього, необхідно було написати функцію, яка розв’язує системи конгруенцій. Розв’язки цих систем в подальшому використовувались яксь як можливі ключі.

Під час відбору правильного ключа утворювалось дуже багато неправильних варіацій розшифрованого тексту, тому необхідно було також реалізувати розпізнавач. Я вибрав його варінт з перевіркою частот літер о, а, е.