Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського » Фізико-технічний інститут

Криптографія

Лабораторна робота №3

Криптоаналіз шифру афінної біграмної підстановки

Варіант 4

Виконали:

Студенти групи ФБ-02

Лугінін Богдан

Хаустович Артем

Перевірила:

Байденко П. В.

Київ 2022 р.

Мета роботи:

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

Постановка задачі:

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.
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.
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

Спершу ми написали необхідні математичні функції: знаходження оберненого за модулем числа, НСД двох чисел, розширений алгоритм Евкліда та розв'язання лінійного рівняння.

Для перевірки змістовності ВТ було використано такі умови:

1) перевірку частот частих літер «о», «а», «е»
2) перевірку частот рідкісних літер «ф», «щ», «ь»

Отриманий ключ: (390, 10)

Зашифрований текст

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфип
мугфбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэ
ысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывдьмиыыяшц
рбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайх
мучмсшывчфвэрфешмяояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзю
длвзбкзешдбшящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэ
жглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшс
зунрмоншзоязшяэдхпезхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщкв
канвказешюшлцромглтдоккжшскзыядншууезжурфешщпнзшятоужертцлвяхщжпофожу
щпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжел
яыцдюппкгфкшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыйм
ывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмо
гйжшфшайрмлзннтзхаокшйбчаощяанбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцз
опзаоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэ

жлыдяюйеызопыщжфоочсквжаббжнзбляьхзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяр
швдшяполфзятзбжьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюшшомглтдо
нзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэ
ечяыжхыхоцыыиеыыяпомггднотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыж
умилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхлдырйпоазсяслщяджипщ
плзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапз
чвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкя
ьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшявжядтцйэоцбчазгфьпмушс
бэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиы
щчыдншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпоно
йкыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзншзунрюпыяябтцю
мюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряешбзкцколппотзу
ыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзхлц
юпзхщжщккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдв
бжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюптжждшсэыпзьцяделo
цлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряе
шйкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешь
оекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножяяоьоэмкзшяпдмыэзгпйш
ууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкз
цжжущпрфуяшфсчдвбждчвхеыщчфочытцмиажщквканфшуufиеыхзаоешезвжпонодаып
иыщомзмятыямйшалтыеызоешыедвайнинзшязпкцрфешмяеыцпяовкрфекуяжубждоджгл
лкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделд
шчфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканп
дпуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсо
чзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиыз
опызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбыщжыйрйшзяошйзоузяждчв
хеыщчпмщпбкуяяоекшярбптхямзюдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяц
псказкзшяллщяанншшкщкпоноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяю
алэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрй
ктзшясжеьзоешрйэжпзжжбяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуе
заяалжшбчшфссешмяпзюнзоешедвдвлгфезшйдбряилгфеыхзсккчвкщыезтлыниоовмушс
сожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитд
оешзхеыхзрэешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэй
йшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцыыиеыыявлаомяркгяшптцпмдущес
зноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбз
бяшждцыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжу
пмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщжшмощквканбчтзябйкжз
шцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячовунщеырэтц
юзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояоносшншмоешд
бждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзб
мушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчбюпповбнзцжшзяой
йппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфссешмяабяопмьос
яцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуи
ырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопжипеызозхьпешьо
мяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяяявлв
жипюпэышбмунрчфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйч
уцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяилщкцжжзщрэысяныблоцлыще

мыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгшьльф
жшншмолдопсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщ
жщлщяджипбжюпмуяззощуиврймзвожзпофотывдохлцюпядайхпимиыраыжнэюшсйокб
яжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносоч
зсыяхщжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущж
зовказхяанаоешезвжбякбмурфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсй
щкжэгщлцечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшкопншф
узхпмдьюшшящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылид
мышкбмщпбкуяяоекзожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэ
охфсфлчжеьзоешэпбжжущчхябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертц
лвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзб
игцскыкфотфлцабгяыовояфяьшмущжвзлжыцмимшшйгшезновжьошйэээфщзрзмкуягш
збезносожзбиеыыядвзбряжзлжипюпоцчбптдохлибвоанаопоьшйкешзокюывруххкнзеявж
йэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофык
сюдабгяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжя
зджпзчзшяжкйкгшмускбфсчаоешезвжпонопмйкйвюпууэжжйюшряшйешпуьгмоешывбз
шхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйскпон
зшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсн
шешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяегдяуярймоаышийшажф
ямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшярллзджипюшлцл
ырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжлкешра
ояазжшжущпщоскскможяскжшбцзвлвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюян
зашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпеяпыэжйэзпэыгдн
шуущешфалноыжгллкеыщжуясащуивхзак

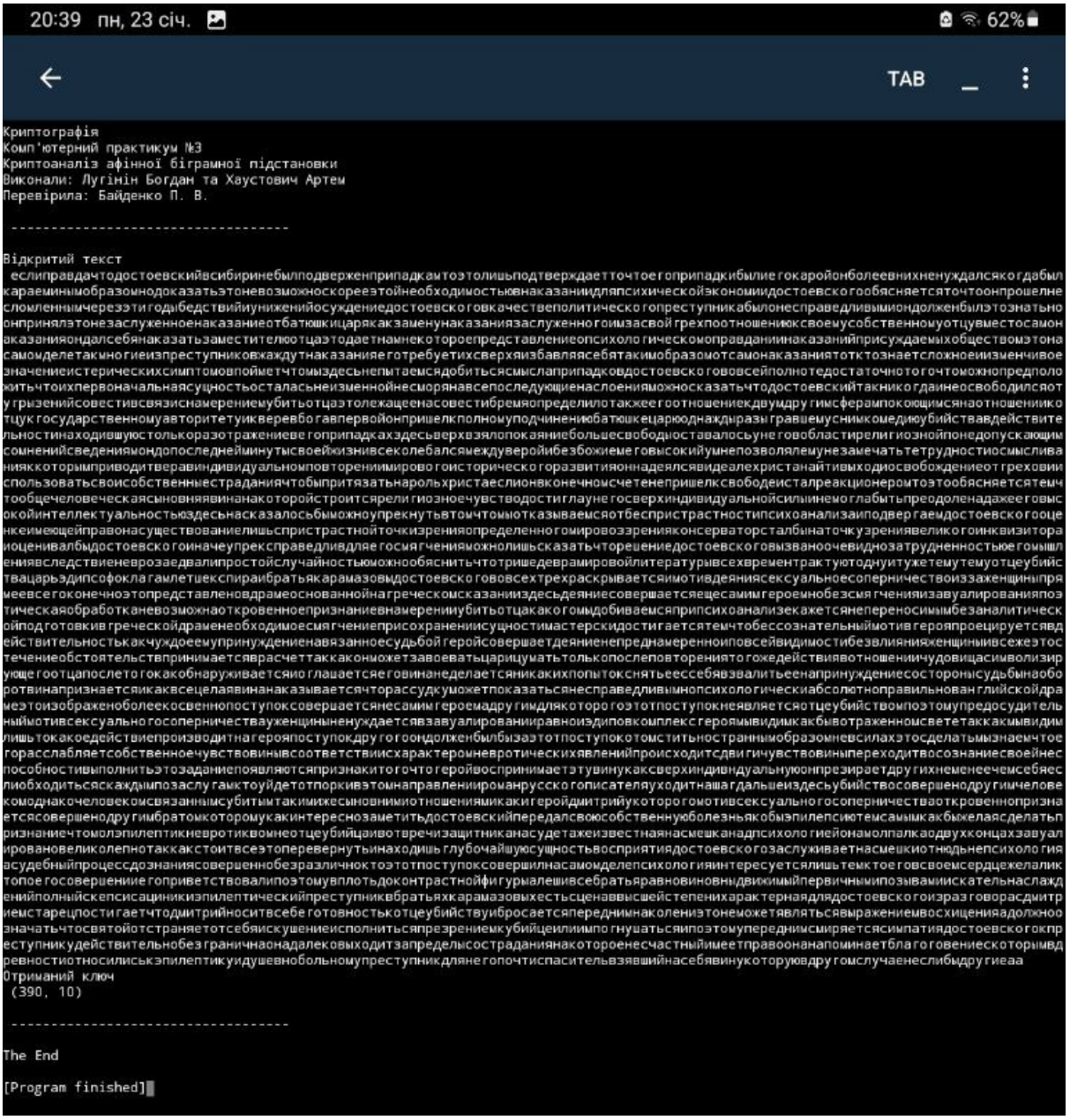
Відкритий текст

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждает
точтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомн
одоказатьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэконом
иидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиуниже
нийосуждениедостоевскоговкачествеполитическогопреступникабылонесправедливыми
ондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзамен
унаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместоса
монаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопс
ихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмног
иеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотса
монаказаниятотктознаетсложноеиизменчивоезначениеистерическихсимптомовпойметч
томыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточно
тогочтоможнопредположитьчтоихпервоначальнаясущностьосталасьнеизменнойнесмор
янавсепоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосвободился
отугрызенийсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопредели
лотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударстве
нномуавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюшкецарюодн
аждыразыгравшемуснимкомедиюубийствавдействительностинаходившуюстолькоразот
ражениевегоприпадкахздесьверхвзялопокаяниебольшесвободыоставалосьунеговобласт

ирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвоейжизни
всеколебалсямеждуверойибезбожиемеговысокийумнепозволялемунезамечатьтетруднос
тиосмысливанияккоторымприводитверавиндивидуальномповторениимировогоисторич
ескогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотгреховииспользо
ватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконечномсчетенеп
ришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеческаясыновняяв
инанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойсилыине
моглабытьпреодоленадажееговысокойинтеллектуальностьюздесьнасказалосьбыможноу
прекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдостое
вскогооценкеимеющейправонасуществованиелишьспристрастнойточкизренияопределе
нногомировоззренияконсерваторсталбынаточкузренияявеликогоинквизитораиоценивалб
ыдостоевскогоиначеупрекправедливдляегосмягченияможнолишьсказатьчторешениедо
стоевскоговызваноочевиднозатрудненностьюегомышленияявследствиеневрозаедвалипро
стойслучайностьюможнообяснитьчтотришедеврамировойлитературывсехвременткту
ютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазов
ыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззаже
нщиныпрямеевсегоконечноэтопредставленовдрамеоснованнойнагреческомсказаниизде
сьдеяниесовершаетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобр
аботканевозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемсяпр
ипсихоанализекажетсянепереносимымбезаналитическойподготовкивгреческойдрамене
обходимоесмягчениеприсохраненииусщностимастерскидостигаетсятемчтобессознатель
ныймотивгеропроецируетсявдействительностькакчуждоеемупринуждениенавязанноес
удьбойгеройсовершаетдеяниенепреднамеренноиповсейвидимостибезвлиянияженщины
ивсежеэтостечениеобстоятельствпринимаетсяврасчеттаккаконможетзавоеватьцарицума
тьтолькопослеповторениятогожедействиявотношениичудовищасимволизирующегоотца
послетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьеессе
бявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелаяви
нанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихологическиабсолют
ноправильнованглийскойдрамеэтоизображеноболеекосвеннопоступоксовершаетсянеса
мимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосу
дительныймотивсексуальногосоперничествауженщиныненуждаетсявзавуалированиира
вноиэдиповкомплексгероямывидимкакбывотраженномсвететтаккакмывидимлишьтокако
едействиепроизводитнаерояпоступокдругогоондолженбылбызаэтотпоступокотомстить
ностраннымобразомневсилахэтосделатьмызнаемчтоегорасслабляетсобственноечувство
винывсоответствииихарактеромневротическихявленийпроисходитсдвигичувствовинып
ереходитвосознаниесвоейнеспособностивыполнитьэтозаданиепоявляютсяпризнакитого
чтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечем
себяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэтомнаправлениироманрусск
огописателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочело
векомсвязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитрийукоторог
омотивсексуальногосоперничествоткровеннопризнаетсясовершенодругимбратомкотор
омукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобыэпилепси
ютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийцаи
вотвречизащитниканасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодвухко
нцахзавуалировановеликолепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшую
сущностьвосприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасудебны
йпроцессдознаниясовершеннобезразличноктоэтотпоступоксовершилнасамомделепсихо

логияинтересуетсялишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнаслажденийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввысшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитрийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотороенесчастныйимеетправоонанапоминаетблагоговениескоторымвдревностиотносилиськэпилептикуидушевнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругомслучаенеслибыдругиеаа

Вивид програми (реалізований на планшетному ПК):



Висновки

У ході комп’ютерного практикуму №3 нам довелося працювати з шифром афінної біграмної підстановки детальніше познайомитися з криптоатакою на цей шифр. Також ми поновили свої знання з модульної арифметики. У результаті створено код, який не тільки шукає ключ і розшифровує шифртекст, але й аналізує і відділяє змістовний текст російською мовою від тексту-шуму, що виникає при неправильному дешифруванні.