МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп’ютерний практикум
№3
З дисципліни

Криптографія

Виконав студент групи ФБ-81

Середа А. С.

Перевірив

Чорний О. М.

Київ – 2020
06.11

Тема: Криптоаналіз афінної біграмної підстановки

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

Завдання: Варіант (18)

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.

Зашифрований текст:

юетруожсвеызцэзыфшойызмбибсйкврбсйэффшщшвожкмчюетруожсвекзюегшшоакжжябс
йцсвещтюсроауцезохюдбйэйаяэчэьогбйэжзмеьэнецеяэйгвекзсйютэфейцшгшимюетруожсв
ейбмомчьогбчуткаучзэзщмжзвзгефхмафыяэюэрелфауимчмгембуйвецщкэмоцыэбьекзмаф
ыяэбьшемхдшчюфтчймеацжзвзгефхмафыяэюэрелфауимчмгелецшвимореиыфемэиоялшоу
йфбяшмаокжыцзбкжжябсйцсвещтюсроауцезохюдбркшомэршйаябйолрхэдаючетжжгтифдз
тшттфычсведаетсчлехввамчглмоцтябмчжзвзгефхмаллэзиоаущтюсроаучмэзршоюжеоэщед
аюцюеютвючавэыфдшгегшчэмэдэдамчвенеттючмочажсвершоюжеоэщечмгецехйызребэлх
ывмыгеузызталлэффшщшьэвемаэфлшщтсэиеабзеьаллжсвелешжфехййэезбйютяшлфнекцр
шчмхвсйызвееосэткгйреткммвеуоцыэбьекзюсвершгеюкоюдбкзиэезнжцышоларемангмэяш
бшашксййгшвозшашткшощсревкэбюсейчффыяэюэчкэбюсейчфокаагтсдвзбэхэвейюейюэб
бморенеозюбюсбрвеушйжфшьэаыфшойызмбибсйвйэффшщшвожкмчрещбдоуйюевебкэфл
еишеьэщлэыфэфлшщшнеоююючялфеузхосйлхлецшвиффкшненрлечммэээиожкэщлэыфялф
ыфедаууййютциимайсмббщтюсрофгмэщтнвдаяферфанрршдедаважсимдэщбдоуйршюетру
ожсвечмдэшбяеимцщдшшдяэдашзццкэрзнэвччсфбсвьцавьцззюевеацмашоцыэбьечюдбмбу
йвецщкэрзгшцйьоатчфцтсыэбчажкгзфлнэвдчаозглцтэенемхдшчюфтчйцэхекэсшворбфжаы
шолаякркмщбфпжвэщшфаюаяекйвеларбвйчфуйезсмонрквеацкэайчфуэкзхэнэаыжсючофббб
нвдабэуаллжсвеншеьллоюнпмощмнрюэцщдшайатэлллокозтшттфыфцкэрзнэьтжжгтибффбо
вууочэбмоткаувчсймебймещлаюцтьэаэчмнэаюффйшсмвчсверкзшыаакчмеиоеэдагтжкэфр
шофгшушвосдщтчьейледэамткьобрмыаакчгйршвзвшломоимцжатяфсчочшйгедйджцтцзця
вдлечммэиыяэюэимялфыфшойызмбжщмйифршййюэббвчкчменэушдацшушбюэбеиючфцг
баюерючнрбэамткьояшщтюсровшбюэбеимомчвдааитдфйшмйээбйщклраадшмхреужлалрщ
тюсроуэнээшьмстевщтюсрощтнвдаяферфанркзщеоэкзмецешыозцшщбффсчййчмчмысйвюе
эщврокэфэбхпимдэюебфзшзоюсвегосймэбйозиомойэплфеузхосйлхжйоюзабряеоэкзмецег
егосчмышонвуудабэвшмхредаййцеууашоцнздабрбйюдатэлвдледыяффэуыяэюэюыфеыжц
шдаййэфцтфэдиьшнрлечммэуаркаусшщтюсроаужзмейкжжкзюегшшойечфеймэбфсэцеайж
звзбэббгэааюзлхкзвзилцтэечйчфземхдшчюфтчймеиыфшойызмбтшмйдомчнпрбьояшфброй
прбьояшюшкфллынозбьхжтклложцыозэзюедажычайояфвеяэеомщббзпжцжюзшсшнэчмшо
ршвзжевшнээароуййцшюгэршвзжевшкюбвьцнеаэютуачучашйссимэкцыознэлехввакздаэбя
ккчмоьшцщдшэюдбоюдфцеаймшкзюегшшоуэцезоаоючллгечмчмлхйпрбжюаоцыэбьевоьет
кгткэнйлафшаерзьэючаадажычафжяфйййцрорфрбрбкздажыванфауткмчршчмгечмцезоаоз
шсшнэчмбйейцтлзйааоиыхпрбябмысйициэлхкзпагтюсццжййцшюсахпрфауимршщеъбяюх

юзарахпмоючллгечмчмлхцезоошсшнэчмршчмгероютгльогбйэровюдбоюыыяэбьйемхдшч
юфтчйменеюсофдарзсймеыюгшьэифябвкезгвфшровюдбоюшймчщвцтлзиоаумбуймэттсйхэ
йэршчмгечмлтьогцтйместрфэбмьйэмысйгшдерздивдоэеавагтдарзйэзыцтйэффлшневенема
фыфеыжцшгелтьогцтйтцчтрфэбмьтщчаркюзгшвючжщвреаэогмэуыяэюэвоюсялшоючллгеч
мчмлхдаябоюзаеыяэюэимюаффлшдэшбшззвыыяэюэьйэфчзнэщблаллжсвечмщтсэюфеймэв
емаоюдбсэббнвэфварбйошоюсвершчмгеййвбьсчарбйоаущтюсроаулечммэмзлечммэнвэбго
оюдбсйэфцтфэлхнрвемхмеюевеацмазередеспречмгелецшвичавйевэбгохюдбвчфбнэшодбов
ууаафшщиййчемйцевдушгецшуштквдщцбйчфййцеялгтжжычуээарояфсйвецйвзчзюзецкэрз
лхлшашюедесосдвееоаарксшжзюоеймемхмецшмепакчкожжывбфсйвежзкзвзчзсинэверыдб
овууаюффлрлшашюедесосддшайчфбркзюегшшоуэябвкезгвозааббэфркаагтсдвзбэлшгежзвз
гефхмаоюшйоюзаяшлецшвифбсйвэнэршлецшвифбсйяюдбчарксшузгещтсэюфэбйохкрксву
удабэвкчпденелехввацинвкшнедыкдщвюентвютщфбмышорюгтягвершщегбоюзавэкзушюе
веацмащвервенемаоюдфэбдоцыэбьекзшзгшцйьоатваюдцщдшхейкаагтсджзвзгефхвзбэлшге
лечммэвюдбуэшыэбршкзршоюжеоэщечмгеледыывмояшашксййгшвосдоюдайрвшмхдаюю
чжщвренеыжмеваммрйоюзаяшршщегбоюшйэфцтфэлхнрршоюжеоэщечмгемаоюсчфбнэшо
дбовууттакмдмеваммнюдбывуудабэвшмхкзэйфбуйэбюзщммевеммейютрбибффчжнэщтэф
шзйамыжицэкздечмгемаоюоеьэлегбуйфбййвэшыэбьэлхюаофэбышоэьэеосдййэзчмыбовуу
жюдбмыяэцшдшимтгвеацашксййгшвосчменэушдацедйгегосдозщозеытжжимуыяэюэенвая
быжпфййвеяэроеэпюйпмощбтеврэомобрршозоцлосдифгшьэоазшдараюдозоцлосйлхмевем
мйчаоиышовчйшшсючаегшючшйызозючнрозоцлозеврэочаюгмэифгшьэифййвеяэчаючшой
йызрешрмйеверкзэоцтжжычршеэршюетруоьшжздвзуушгецшьпффуащбэйвюаыэбфжшшм
йэйцеаедеивердеданпмобрбфсэыбюсимцьрбууюсофдаэцуабйючсцбшдацедйцевчмазеучхп
уалшфсуйюврбвавэнэршюврбвараркзшведшайчфяшрежзцймефешоюврбйшвшнеызявууда
бэбгвелецшвиморерфыжцшдаимшчкчмочффшщшьэдаьоэфчанрршцеюфозмэсмдэдшэзуан
рдедайрьэючййвеяэффмевефехеревчьшуоейцеаехозшцыфшдещтнврбморечжкзушьэьшдак
вцшдагтшоэпыжьэюкчпдешсрбэфвкйпыжщхнэеолрмевеозлаючаегшейцеаехоисючаамбщс
моршьшеэйацтейшэыэщовймэрэзолрферфлравщсрбэфвкршыжашгосэшыэбтруащтнвиэезв
оошючхжркшонсрбэфвклещоварбйохпффуащбэйвюдосййцыэйюейлещоварбйосчгтлвяшм
вердеданпмобрййвеяэуштквдоюбшушгецшуштквдэшгшайэфцткшвозуюедажыокршцеюфо
змэдэдшайчфяшялсйэфчзюзифэффшщшьэочфбнэшомчсвуудабэивьцчэыбовууюейцнзуайй
веяэуштказшщоисмояшушпфыиейвечаушгецшюойеьяейчфморелбейуопьщсючтюэбеивчфб
овьчяеьйшрвзйаючаемхкшмбуймэшовчьшуоывьцчэыбовуувшщеушбэхоьшщтнвфыфшдшг
швосйлхроеэпюйпредаякчпденеялфысйицекуйцтфьльетрфэфьцэшаеьхууцзюхейлхозкэдаг
тйэййвеяэлазшдаяюейлещоварбйолроюьзотзшрзбпыжщхушгецшушдарзбйщкаудэццведпы
жьэцзфшгыэбфжшшмйеверлшвржзмеьцоэючщбэйцевдэшгшзоцыэбьевоейщеютдоважсве
ючаюэбьшушбкллюзьэжцнхвшюшюхьлщвакжжябсйцсвеааршневзбэлшгефбровкркдысйг
шхоючиэфхщшиэезгшацябвкезгвжожкллюзаегшвкрквшюшюхршюещбйпябвшлоеэпюйпи
мцжркшомчмевеммчжуйызмбибяшнедшайчфьрцеуофимойэлшвржзмшацжзвзгефхюебфз
шацщтсэюфэблврбвакверюбшнедшэзщбээдагтйэвемащвэбгооюдбсйэфцтфэлхнрцщоэвзчз
юзщфглябййояфсйвеявервенемаоюфцкэрзлхатэлатэлуэюевзмеццледыывмобрщтюсроюец
врбябййвймчййоюьщййэфчзнэсгмэдйоюзаяшташйссвчрбцэуыяэюэгверюаллцвбэсшьэээщ
бифауимакгтлжьоейоюцщдшьэвкшомэршйаябйоаухэдаючшэншеьллэбквможцшлткчусвбэ
сшьэрфауткдыьцхйтщщтнвщтролазшжзукжжябсййоцыэбьеццщблаллааэбякжсвечмдедагл
ццлхцегтзпморенедэозфбгюэфвэщтффнсжзлтьогцтйменевчюшозвеозвфауршледыяфдзэйоз
шыэбхпмояшщшнекзфеюзофгшушьэялозгвяещосйлхйыяэневембмочуьтуйжеымюещтглаа
эфгшьэжэюеютвюредаеыяэоюфшвшьэларквдомнелкаагтошчмокжыфбегмэозодщвшэщвфт
узьэдияшюеушдаффатчждшршсвмыгеузмэушткяшюшфшнецеммвеммиыэфмлеркцлетт
ючмоьэмеююдбффнвмошййитмоьэипрбьояшмвсймэсшьэхчьтуэмевеммуаэбякнцпжмбиб
ййчэбгюяшвеаэатэлаудагтшошэдэшбяеимдэшбяерейвьцчэуыяэюэюыщвдшэздивднрюеоэ
щшцяьшлецшвичавйэйоюзаяшледыяффэрйьэбкллюзледтрбйрхбоксэчзюзуаааушнешофыы
вйшвеьаллэбюсведрневшуайжючгшаавененэмаджуйсдйшмйвшгпмочеьаллэбюсвесцфэмйэ
йэббьючмаааабпрбьшбсвецшвшнацрлшвшнеаавененэмасйвеняючофьэоцузмхюэтцжеущий

эйейлхялшоюсвершщтюсрояфлшюаааэбяксйэфчздшьэуаюдгйгебэгыяэмевеммрйэфцтдзуа
нрбйщкзшыэщомореьешльоюсеймееймэрэзозшлечммэеэвейюааьожкмевеммзовудшбсвещ
югемечзюзуааавенемаокгшбсважзозюбнлйшмйээвеацюедесозшжцдшьарксшщтяфчарксшр
шщтяфжзцэвеютвюмоокдайрлэлфьэоцмевеммайжзсшбсвещюгемежыябзеьаллжсвеючыдаа
рбсйвйейлхялсэмазеучэбфбнроююакчызьпиыозбэршщтяфжцдшьаааеасйжзсшбсвекзюегш
шоюекшшфщеткэцюевеацмазенжмдаарбюаллсэаавенеюечэясвеябвкезгвсжмдаарбялфылл
жюрбжкркщтяфроиыозююлвуавейкветкчпуамаджяфябффдзэйифдэшбяеюылвэфюелкфыьо
кзцлгтпцчзэзаавенемафысйгшхочуозаеуожклветфбюехоьшюеббнвьэстжжцэыкьщбэдагтюс
ейцэрйоюзабряарккзамрзючошщшнэцэрбовййсащркбхксвэщлэмоуэщшрерзьэайоюзатщмев
еммуаркссшжзоркбхквчмоьшбйялсэщшфабфпжййезсмдйоюзаяшбкчпденвуудабэеэнкчпуяь
шнрвчщтсэюфэбйосчщбэймчвдлшврбэдагтюсеймедйсмббмоиыфеыжцемхреьомдщвчанрб
йшртэлебйючжededэдагтйэяещтнврбмофыфшщфщсрегз

Хід роботи:

Спершу я створив фунцкії що рахували НСД, та пошук оберненого за модулем. Далі застосовуючи їх я створив функцію що розв'язує лінійні рівняння. Для цього мені довелось окрім звичайной функції пошуку НСД, створити функцію що разом із пошуком НСД за оберненним алгоритмом Евкліда запам'ятовує масив коефіцієнтів. Для того щоб коректно обробити варіант із декількома відповідями, я додав у функцію масив, який у разі єдиності рішення залишається порожнім, а при декількох, заповнюється. Далі в залежності від того скільки рішеннь, функція повертає різні значення, що і дозволяє мені відслідкувати всі можливі рішення.

Далі, застотувавши частину коду із першої лабораторної я визначив найчастіші біграми шифротексту. Я одразу перевів їх у чисельні значення відповідно до формули із методички і створив масив.

Далі я перебрав всі можливі варіанти співставлення перших п'яти біграмм відкритого та шифротексту за допомогою чотирьох циклів і розшифрував їх. Після кожного розшифрування текст перевірявся на істотність за умовою частот літер "а", "о", "е".

Я отримав один, наступний текст:

понятночтотакимпредставлялосыделосовременникампонятночтонаполеонуказалосычтопр
ичинойвойньбылиинтригианглиикаконигоговорилэтонаостровесвеленыпонятночточленаман
глийскойпалатыказалосьчтопричинойвойныбыловластолюбиенаполеоначтопринцуольден
бургскомуказалосьчтопричинойвойныбылосовершенноепротивнегонасилиечтокупцамказа
лосычтопричинойвойньбылаконтиненталынаясистемаразорявшаяевропучтостарьмсолдата
мигенераламказалосьчтоглавнойпричинойбыланеобходимостыупотребитыихделолегити
мистамтоговремениточтонеобходимобыловосстановитьадипломатамтоговремениточтовсе
произошлооттогочтосоюзроссиисавстриейвгодунебылдостаточноискусноскрытотнаполео
наичтонеловкобылнаписанзапонятночтоэтииещебесчисленноебесконечноеколичествоприч
инколичествокоторьхзависитотбесчисленногоразличияточекзренияпредставлялосысоврем
енникамнодлянаспотомковсозерцающихвовсемегообемегромадностьсовершившегосясобы
тияивникающихвегопростойистрашныйсмыслпричиньэтипредставляютсянедостаточными
длянаснепонятночтобымиллионылюдейхристианубивалиимучилидругдругапотомучтонап
олеонбылвластолюбивалександртвердполитикаанглиихитраигерцогольденбургскийобижен
нелызяпонятыкакуюсвязыимеютэтиобстоятелыствассамымфактомубийстваинасилияпоче
мувследствиетогочтогерцогобижентысячилюдейсдругогокраяевропьубивалииразорялилю
дейсмоленскойимосковскойгубернийибылиубиваемыимидлянаспотомковнеисториковнеув
леченьхпроцессомизысканияипотомуснезатемненнымздравьмсмьсломсозерцающихсобы
тиепричиныегопредставляютсявнеисчислимомколичествечемболышемьуглубляемсявизыс
каниепричинтемболышенамихоткрьваетсяивсякаяотдельновзятаяпричинаилицелыйрядпри
чинпредставляютсянамодинаковосправедливьмисамипосебеиодинаковоложнымипосвоейн
ичтожностивсравнениисгромадностьюсобьтияиодинаковоложньмипонедействительностис

воейбезучастиявсехдругихсовпавшихпричинпроизвестисовершившеесясобытиетакойжепр
ичинойкакотказнаполеонаотвестисвоивойсказавислуиотдатьназадгерцогствоольденбургск
оепредставляетсянамижеланиеилинежеланиепервогофранцузскогокапралапоступитынавто
ричнуюслужбуибоежелибыоннезахотелидтинаслужбуинезахотелбьдругойитретийитьсячн
ыйкапралисолдатнастолыкоменеелюдейбылобьввойскенаполеонаивойньнемоглобыбытьеж
елибьнаполеоннеоскорбилсятребованиемотступитызавислуиневелелнаступатывойскамнеб
ылобывойньноежелибывсесержантьнепожелалипоступитьнавторичнуюслужбутожевойны
немоглобьбьтытоженемоглобыбытьвойньежелибынебылоинтриганглииинебьлобьпринцао
льденбургскогоичувстваоскорблениявалександреинебьлобьсамодержавнойвластивроссии
инебылобыфранцузскойреволюцииипоследовавшихдиктаторстваиимпериииивсеготогочтоп
роизвелофранцузскуюреволюциюитакдалеебезоднойизэтихпричинничегонемоглобыбытьс
талобьтыпричиныэтивсемиллиардьпричинсовпалидлятогочтобыпроизвеститочтобылоисле
довательноничтонебылоисключительнойпричинойсобытияасобытиедолжнобылосоверши
тьсятолькопотомучтоонодолжнобылосовершитысядолжньбылимиллионьлюдейотрекшисы
отсвоихчеловеческихчувствисвоегоразумаидтинавостокасзападаиубиватьсебеподобньхточ
нотакжекакнескольковековтомуназадсвостоканазападшлитолпылюдейубиваясебеподобнь х
действиянаполеонаиалександраотсловакоторьхзависелоказалосьчтобьсобьтиесовершилос
ыилинесовершилосыбылитакжемалопроизволынькакидействиекаждогосолдаташедшеговп
оходпожребиюилипонаборуэтонемоглобьтыиначепотомучтодлятогочтобьволянаполеонаи
александратехлюдейоткоторьхказалосьзависелособытиебылаисполненанеобходимобылосо
впадениебесчисленньхобстоятельствбезодногоизкоторыхсобытиенемоглобьсовершитьсяне
обходимобылочтобьмиллионьлюдейврукахкоторыхбыладействительнаясиласолдатыкотор
ыестрелялиивезлипровиантипушкинадобылочтобьонисогласилисыисполнитьэтуволюедини
чньхислабыхлюдейибылиприведеныкэтомубесчисленньмколичествомсложньхразнообразн
ыхпричинфатализмвисторииинеизбежендляобясненияразумньхявленийтоестытехразумно
стькоторыхмьнепонимаемчемболеемьстараемсяразумнообяснитыэтиявлениявисториитемо
нистановятсядлянаснеразумнееинепонятнеекаждьйчеловекживетдлясебяполызуетсясвобо
дойдлядостижениясвоихличныхцелейичувствуетвсемсуществомсвоимчтоонможетсейчасс
делатыилинесделатытакоетодействиенокакскорооносделаетеготакдействиеэтосовершенное
визвестныймоментвременистановитсяневозвратимымиделаетсядостояниемисториивкотор
ойоноимеетнесвободноеапредопределенноезначениеестыдвесторонькизнивкаждомчелове
кежизньличнаякотораятемболеесвободначемотвлеченнееееинтересыижизныстихийнаяроев
аягдечеловекнеизбежноисполняетпредписанньеемузаконьчеловексознательноживетдлясе
бяослужитбессознательньморудиемдлядостиженияисторическихобщечеловеческихцеле
йсовершенньйпоступокневозвратимидействиеегосовпадаявовременисмиллионамидействи
йдругихлюдейполучаетисторическоезначениечемвьшестоитчеловекнаобщественнойлестн
ицечемсбольшимилюдымионсвязантембольшевластионимеетнадругихлюдейтемочевидне
епредопределенностьинеизбежностыкаждогоегопоступкасердцецаревоврцебожьейцарьес
тьрабисторииисториятоестыбессознательнаяобщаяроеваяжизньчеловечествавсякойминут
ойжизницарейполызуетсядлясебякакорудиемдлясвоихцелейнаполеоннесмотрянаточтоему
болеечемкогданибудьтеперьвгодуказалосычтоотнегозависелоилинекаквпоследнемписьме
писалемуалександрникогдаболеекактеперьнеподлежалтемнеизбежнымзаконамкоторыезас
тавлялиегодействуявотношениисебякакемуказалосьпосвоемупроизволуделатыдляобщегод
еладляисторииточтодолжнобылосовершитьсялюдизапададвигалисынавостокдлятогочтобь
убиватьдругдругаипозаконусовпаденияпричинподделалисысамисобоюисовпалисэтимсобь
тиемтьсячимелкихпричиндляэтогодвиженияидлявойныукорьзанесоблюдениеконтинентал
ынойсистемыигерцоголыденбургскийидвижениевойсквпруссиюпредпринятоекакказалосы
наполеонудлятогототолькочтобыдостигнутьвооруженногомираилюбовыипривьчкафранцузс
когоимператораквойнесовпавшаясрасположениемегонародаувлечениеграндиозностьюпри
готовленийирасходыпоприготовлениюипотребностыприобретениятакихвыгодкоторьебыо
купилиэтирасходыиодурманившиепочестивдрезденеидипломатическиепереговорыкоторые
повзглядусовременниковбыливеденьсискреннимжеланиемдостижениямираикоторыетолык

оуязвлялисамолюбиетойидругойстороньимиллионымиллионовдругихпричинподделавших
сяподимеющеесовершитысясобытиесовпавшихснимкогдасозрелояблокоипадаетотчегооно
падаетоттоголичтотяготеетземлеоттоголичтозасьхаетстерженьоттоголичтосушитсясолнц
емчтотяжелеетчтоветертрясетегооттоголичтостоящемувнизумальчикухочетсясестьегонич
тонепричинавсеэтотолькосовпадениетехусловийприкоторыхсовершаетсявсякоежизненно
еорганическоестихийноесобытиеитотботаниккоторыйнайдетчтояблокопадаетоттогочтокле
тчаткаразлагаетсяитомуподобноебудеттакжеправитакженеправкакитотребенокстоящийвн
изукоторыйскажетчтояблокоупалооттогочтоемухотелосысестьегоичтоонмолилсяобэтомта
кжеправинеправбудеттоктоскажетчтонаполеонпошелвмосквупотомучтоонзахотелэтогои
оттогопогибчтоалександрзахотелегопогибеликакправинеправбудеттоктоскажетчтозавали
вшаясявмиллионпудовподкопаннаягораупалаоттогочтопоследнийработникударилподнееп
оследнийразкиркоювисторическихсобытияхтакназываемьевеликиелюдисутыярлькидающи
енаименованийсобытиюкоторыетакжекакярлькименеевсегоимеютсвязиссамымсобытиемка
ждоедействиеихкажущеесяимпроизволыньмдлясамихсебявисторическомсмысленепроизво
льноанаходитсявсвязисовсемходомисторииопределенопредвечноаа

П’ять найчастіших біграм шифротексту:
ве 104
да 61
эб 54
ою 51
чм 50

Ключ:
A=425
B=100

Під час виконання роботи я майже не мав проблем, окрім однієї прикрої помилки в функції розшифрування (при переводі із char в int забув додати 32), шукаючи яку я витратив близько двох годин. Також довелось трохи витратити часу щоб зрозуміти що потрібно ще поміняти місцями літери “ы” та “ь” у шифротексті, бо без цього в відкритому тексті деякі біграми були не правильні.

Висновок

Під час виконання лабораторної роботи я пригадав як працювати з модулярною арифметикою (шукати НСД та обернене за Алгоритмом Евкліда, та вирішувати лінійні рівняння). Також я навчився методу знаходження можливих ключів та подальшого розшифрування тексту, зашифрованого Афінним біграмним шифром.