Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Лабораторна робота

із Криптографії №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Топчій Микита ФБ - 74

Височанська Вікторія ФБ - 71

Перевірено_____

Київ 2019

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

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

Порядок виконання 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 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.

Варіант 18

Шифрований текст:

юетруожсвеызцэзыфшойызмбибсйкврбсйэффшщшвожкмчюетруожсвекзюегшшоакжжябсйцсвещтюср
оауцезохюдбйэйаяэчэьогбйэжзмеьэнецеяэйгвекзсйютэфейцшгшимюетруожсвейбмомчьогбчуткаучзэз
щмжзвзгефхмафыяэюэрелфауимчмгембуйвецщкэмоцыэбьекзмафыяэбьшемхдшчюфтчймеацжзвзгефх
мафыяэюэрелфауимчмгелецшвимореиыфемэиоялшоуйфбяшмаокжыцзбкжжябсйцсвещтюсроауцезох
юдбркшомэршйаябйолрхэдаючетжжгтифдзтшттфычсведаетсчлехввамчглмоцтябмчжзвзгефхмаллэзио
аущтюсроаучмэзршоюжеоэщедаюцюеютвючавэыфдшгегшчэмэдэдамчвенеттючмочажсвершоюжеоэщ
ечмгецехйызребэлхывмыгеузызталлэффшщшьэвемаэфлшщтсэиеабзеьаллжсвелешжфехййэезбйютяшл
фнекцршчмхвсйызвееосэткгйреткммвеуоцыэбьекзюсвершгеюкоюдбкзиэезнжцышоларемангмэяшбша
шксййгшвозшашткшощсревкэбюсейчффыяэюэчкэбюсейчфокаагтсдвзбэхэвейюейюэббморенеозюбюс
брвеушйжфшьэаыфшойызмбибсйвйэффшщшвожкмчрещбдоуйюевебкэфлеишеьэщлэыфэфлшщшнеою
ючялфеузхосйлхлецшвиффкшненрлечммэээиожкэщлэыфялфыфедааууййютциимайсмббщтюсрофгмэщ
тнвдаяферфанрршдедаважсимдэщбдоуйршюетруожсвечмдэшбяеимцщдшшдяэдашзццкэрзнэвччсфбсв
ьцавьцззюевеацмашоцыэбьечюдбмбуйвецщкэрзгшцйьоатчфцтсыэбчажкгзфлнэвдчаозглцтэенемхдшч
юфтчйцэхекэсшворбфжаышолаякркмщбфпжвэщшфаюаяекйвеларбвйчфуйезсмонрквеацкэайчфуэкзхэ
нэаыжсючофббнвдабэуаллжсвеншеьллоюнпмощмнрюэцщдшайатэлллокозтшттфыфцкэрзнэьтжжгтиб
фбовууочэбмоткаувчсймебймещлаюцтьэаэчмнэаюффйшсмвчсверкзшыаакчмеиоеэдагтжкэфршофгшу
швосдщтчьейледэамткьобрмыаакчгйршвзвшломоимцжатяфсчочшйгедйджцтцзцявдлечммэиыяэюэимя
лфыфшойызмбжщмйифршййюэббвчкчменэушдацшушбюэбеиючфцгбаюерючнрбэамткьояшщтюсров
шбюэбеимомчвдааитдфйшмйээбйщклраадшмхреужлалрщтюсроуэнээшьмстевщтюсрощтнвдаяферфан
ркзщеоэкзмецешыозцшщбффсчйймчмысйвюеэщвроркэфэбхпимдэюебфзшзоюсвегосймэбйозиомойэп
лфеузхосйлхжйоюзабряеоэкзмецегегосчмышонвуудабэвшмхредаййцеууашоцнздабрбйюдатэлвдледыя
ффэуыяэюэюыфеыжцшдаййэфцтфэдиьшнрлечммэуаркаусшщтюсроаужзмейкжжкзюегшшойечфеймэб
фсэцеайжзвзбэббгэааюзлхкзвзилцтэечйчфземхдшчюфтчймеиыфшойызмбтшмйдомчнпрбьояшфбройп
рбьояшюшкфллынозбьхжткллокцыозэзюедажычайояфвеяэеомщббзпжцжюзшсшнэчмшоршвзжевшнээ
ароуййцшюгэршвзжевшкюбвьцнеаэютуачучашйссимэкцыознэлехввакздаэбяккчмоьшцщдшэюдбоюдф
цеаймшкзюегшшоуэцезоаоючллгечмчмлхйпрбжюаоцыэбьевоьеткгткэнйлафшаерзьэючаадажычафжяф
йййцрорфрбрбкздажыванфауткмчршчмгечмцезоаозшсшнэчмбйейцтлзйааоиыхпрбябмысйициэлхкзпаг
тюсццжййцшюсахпрфауимршщегбоюхюзарахпмоючллгечмчмлхцезоошсшнэчмршчмгероютгльогбйэ
ровюдбоюыыяэбьйемхдшчюфтчйменеюсофдарзсймеыюгшьэифябвкезгвфшровюдбоюшймчщвцтлзиоа
умбуймэттсйхэйэршчмгечмлтьогцтйместрфэбмьйэмысйгшдерздивдоэеавагтдарзйэзыцтйэффлшневене
мафыфеыжцшгелтьогцтйтцчтрфэбмьтщчаркюзгшвючжщвреаэогмэуыяэюэвоюсялшоючллгечмчмлхда
ябоюзаеыяэюэимюаффлшдэшбшззвыыяэюэьйэфчзнэщблаллжсвечмщтсэюфеймэвемаоюдбсэббнвэфва
рбйошоюсвершчмгеййвбьсчарбйоаущтюсроаулечммэмзлечммэнвэбгооюдбсйэфцтфэлхнрвемхмеюеве
ацмазередеспречмгелецшвичавйевэбгохюдбвчфбнэшодбовууаафшщиййчемйцевдушгецшуштквдщцбй
чфййцеялгтжжычуээарояфсйвецйвзчзюзецкэрзлхлшашюедесосдвееоаарксшжзюоеймемхмецшмепакчк
ожжывбфсйвежзкзвзчзсинэверыдбовууаюффлрлшашюедесосддшайчфбркзюегшшоуэябвкезгвозааббэ
фркаагтсдвзбэлшгежзвзгефхмаоюшйоюзаяшлецшвифбсйвэнэршлецшвифбсйяюдбчарксшузгещтсэюф
эбйохкрксвуудабэвкчпденелехввацинвкшнедыкдщвюентвютщфбмышорюгтягвершщегбоюзавэкзушю
евеацмащервенемаоюдфэбдоцыэбьекзшзгшщйьоатваюдцшдшхейкаагтсджзвзгефхвзбэлшгелечммэвю
дбуэшыэбршкзршоюжеоэщечмгеледыывмояшашксййгшвосдоюдайрвшмхдаюючжщвренеыжмевеммр
йоюзаяшршщегбоюшйэфцтфэлхнрршоюжеоэщечмгемаоюсчфбнэшодбовууттакмдмевеммнюдбывууда
бэвшмхкзэйфбуйэбюзщммевеммейютрбибффчжнэщтэфшзйамыжицэкздечмгемаоюоеьэлегбуйфбййвэ
шыэбьэлхюаофэбышоэьэеосдййэзчмыбовуужюдбмыяэцшдшимтгвеацашксййгшвосчменэушдацедйгег
осдозщозеытжжимуыяэюэенваябыжпфййвеяэроеэпюйпмощбтеврэомобрршозоцлосдифгшьэоазшдара
юдозоцлосйлхмевеммйчаоиышовчйшшсючаегшючшйызозючнрозоцлозеврэочаюгмэифгшьэифййвеяэ
чаючшоййызрешрмйеверкзэоцтжжычршеэршюетруоьшждвзуушгецшьпффуащбэйвюаыэбфжшшмйэ
йцеаедеивердеданпмобрбфсэыбюсимцьрбууюсофдаэцуабйючсцбшдацедйцевчмазеучхпуалшфсуйювр
бвавэнэршюврбвараркзшведшайчфяшрежзцймефешоюврбйшвшнеызявуудабэбгвелецшвиморерфыжц
шдаимшчкчмочффшщшьэдаьоэфчанррщцеюфозмэсмдэдшэзуанрдедайрьэючййвеяэффмевефехеревчь
шуоейцеаехозшцыфшдещтнврбморечжкзушьэьшдаквцшдагтшоэпыжьэюкчпдешсрбэфвкйпыжщхнэео

лрмевеозлаючаегшейцеаехоисючаамбщсморшьшеэйацтейшэыэщовймэрэзолрферфлравщсрбэфвкршы
жашгосэшыэбтруащтнвиэезвоошючхжркшонсрбэфвклещоварбйохпффуащбэйвюдосййцыэйюейлещов
арбйосчгтлвяшмвердеданпмобрййвеяэуштквдоюбшушгецшуштквдэшгшайэфцткшвозуюедажыокршц
еюфозмэдэдшайчфяшялсйэфчзюзифэффшщшьэочфбнэшомчсвуудабэивьцчэыбовууюейцнзуаййвеяэу
шткзшщоисмояшушпфыиейвечаушгецшюойеьяейчфморелбейуопьщсючтюэбеивчфбовьчяеьйшрвзйа
ючаемхкшмбуймэшовчьшуоывьцчэыбовуувшщеушбэхоьшщтнвфыфшдшгшвосйлхроеэпюйпредаякчп
денеялфысйицекуйцтфьльетрфэфьцэшаеьхууцзюхейлхозкэдагтйэййвеяэлазшдаяюейлещоварбйолрою
ьзотзшрзбпыжщхушгецшушдарзбйщкаудэццведпыжьэцзфшгыэбфжшшмйеверлшвржзмеьцоэючщбэй
цевдэшгшзоцыэбьевоейщеютдоважсвеючаюэбьшушбкллюзьэжцнхвшюшюхьлщвакжжябсйцсвеааршн
евзбэлшгефбровкркдысйгшхоючиэфхщшиэезгшацябвкезгвжожкллюзаегшвкрквшюшюхршюещбйпяб
вшлоеэпюйпимцжркшомчмевеммчжуйызмбибяшнедшайчфьрцеуофимойэлшвржзмшацжзвзгефхюебф
зшацщтсэюфэблврбваквероюбшнедшэзщбээдагтйэвемащвэбгооюдбсйэфцтфэлхнрцщоэвзчзюзщфгляб
йййояфсйвеявервенемаоюфцкэрзлхатэлатэлуэюевзмеццледыывмобрщтюсроюецврбябййвймчййоюьщ
ййэфчзнэсгмэдйоюзаяшташйссвчрбцэуыяэюэгверюаллщвбэсшьэээщбифауимакгтлжьоейоюцщдшьэвк
шомэршйаябйоаухэдаючшэншеьллэбквможцшлткчусвбэсшьэрфауткдыьцхйтщщтнвщтролазшжзукжж
ябсййоцыэбьецццщблаллааэбякжсвечмдедаглццлхцегтзпморенедэозфбгюэфвэщтффнсжзлтьогцтйменев
чюшозвеозвфауршледыяфдзэйозшыэбхпмояшщшнекзфеюзофгшушьэялозгвящосйлхйыяэневембмоч
уьтуйжеымюещтглааэфгшьэжэюеютвюредаеыяэоюфшвшьэларквдомнелкаагтошчмокжыфбегмэозодщ
вшэщвфтузьэдияшюеушдаффатчждшршсвмыгеузмэуштквшюшфшнецеммвеммиыэфмлеркцлеттючм
моьэмеююдбффнвмошййиитмоьэипрбьояшмвсймэсшьэхчьтуэмевеммуаэбякнцпжмбибййчэбгюяшве
аэатэлаудагтшошэдэшбяеимдэшбяерейвьцчэуыяэюэюыщвдшэздивднрюеоэщшцяьшлецшвичавйэйоюз
аяшледыяффэрйьэбкллюзледтрбйрхбоксэчзюзуааяушнешофыывйшвеьаллэбюсведрневшуайжючгшаа
вененэмаджуйсдйшмйвшгпмочеьаллэбюсвесцфэмйэйэббьючмаааабпрбьшбсвецшвшнацрлшвшнеаавен
енэмасйвеняючофьэоцузмхюэтцжеушмйэйейлхялшоюсвершщтюсрояфлшюаааэбяксйэфчздшьэуаюдгй
гебэгыяэмевеммрйэфцтдзуанрбйщкзшыэщомореьешльоюсеймееймэрэзозшлечммэеэвейюааьожкмеве
ммзовудшбсвещюгемечзюзуаааvenемаокгшбсважзозюбнлйшмйээвеацюедесозшжцдшьарксшщтяфчар
ксшршщтяфжзцэвеютвюмоокдайрлэлфьэоцмевеммайжзсшбсвещюгемежыябзеьаллжсвеючыдаарбсйв
йейлхялсэмазеучэбфбнроююакчызьпиыозбэршщтяфжцдшьаааеасйжзсшбсвекзюегшшоюекшшфщеткэ
цюевеацмазенжмдаарбюаллсэаавенеюечэясвеябвкезгвсжмдаарбялфыллжюрбжкркщтяфроиыозююлву
авейкветкчпуамаджяфябффдзэйифдэшбяеюылвэфюелкфыьокзцлгтпцчзззаавенемафысйгшхочуозаеуо
жклветфбюехоьшюеббнвьэстжжцэыкьщбэдагтюсейцэрйоюзабряарккзамрзючошцшнэцэрбовййсащркб
хксвэщлэмоуэщшрерзьэайоюзатщмевеммуарксшжзоркбхквчмоьшбйялсэщшфабфпжййезсмдйоюзаяш
бкчпденвуудабэеэнкчпуяьшнрвчщтсэюфэбйосчщбэймчвдлшврбэдагтюсеймедйсмббмоиыфеыжцемхре
ьомдщвчанрбйшртэлебйючжededэдагтйэяещтнврбмофыфшщфщсрегз

Розшифрований текст:

понятночтотакимпредставлялосьделосовременникампонятночтонаполеонуказалосьчтопричинойвойн
ыбылиинтригианглиикакониговорилэтонаостровесвеленыпонятночточленаманглийскойпалатыказало
сьчтопричинойвойныбыловластолюбиенаполеоначтопринцуольденбургскомуказалосьчтопричинойво
йныбылосовершенноепротивнегонасилиечтокупцамказалосьчтопричинойвойныбылаконтинентальная
системаразорявшаяевропучтостарымсолдатамигенераламказалосьчтоглавнойпричинойбыланеобходи
мостьупотребитьихвделолегитимистамтоговремениточтонеобходимобыловосстановитьадипломатамт
оговремениточтовсепроизошлооттогочтосоюзроссиисавстриейвгодунебылдостаточноискусноскрытот
наполеонаичтоненовкобылнаписанзапонятночтоэтиещебесчисленноебесконечноеколичествопричинк
оличествокоторыхзависитотбесчисленногоразличияточекзренияпредставлялосьсовременникамнодлян
аспотомковсозерцающихвовсемегообемегромадностьсовершившегосясобытияивникающихвегопросто
йистрашныйсмыслпричиныэтипредставляютсянедостаточнымидлянаснепонятночтобымиллионылюде
йхристианубивалиимучилидругдругапотомучтонаполеонбылвластолюбивалександртвердполитикаанг
лиихитраигерцогольденбургскийобиженнельзяпонятькакуюсвязьимеютэтиобстоятельствассамымфакт
омубийстваинасилияпочемувследствиетогочтогерцогобижентысячилюдейсдругогокраяевропыубивал
иираздорялилюдейсмоленскойимосковскойгубернийибылиубиваемыимидлянаспотомковнеисториковн
еувлеченныхпроцессомизысканияипотомуснезатемненнымздравымсмысломсозерцающихсобытиепри
чиныегопредставляютсявнеисчислимомколичествечембольшемыуглубляемсявизысканиепричинтембо
льшенамихоткрываетсяивсякаяотдельновзятаяпричинаилицелыйрядпричинпредставляютсянамодинак
овосправедливымисамипосебеиодинаковоложнымипосвоейничтожностивсравнениисгромадностьюсо
бытияиодинаковоложнымипонедействительностисвоейбезучастиявсехдругихсовпавшихпричинпроизв
естисовершившееясобытиетакойжепричинойкакотказнаполеонаотвестисвоивойсказавислуиотдатьназ
адгерцогствоольденбургскоепредставляетсянамижеланиеилинежеланиепервогофранцузскогокапралап
оступитьнавторичнуюслужбуибоежелибыоннезахотелидтинаслужбуинезахотелбыдругойитретийитыс
ячныйкапралисолдатнастолькоменеелюдейбылобыввойскенаполеонаивойнынемоглобыбытьежелибын
аполеоннеоскорбилсятребованиемотступитьзавислуиневелелнаступатьвойскамнебылобывойныноеже
либывсесержантынепожелалипоступитьнавторичнуюслужбутожевойнынемоглобыбытьтоженемоглоб
ыбытьвойныежелибынебылоинтриганглиииинебылобыпринцаольденбургскогоичувстваоскорблениява
лександреинебылобысамодержавнойвластивроссииинебылобыфранцузскойреволюцииипоследовавши
хдиктаторстваимперииивсеготогочтопроизвелофранцузскуюреволюциюитакдалеебезоднойизэтихпр
ичинничегонемоглобыбытьсталобытьпричиныэтивсемиллиардыпричинсовпалидлятогочтобыпроизвес
титочтобылоисследовательноничтонебылоисключительнойпричинойсобытияасобытиедолжнобылосов
ершитьсятолькопотомучтоонодолжнобылосовершитьсядолжныбылимиллионылюдейотрекшисьотсво
ихчеловеческихчувствисвоегоразумаидтинавостоксзападаиубиватьсебеподобныхточнотакжекакнеско
льковековтомуназадсвостоканазападшлитолпылюдейубиваясебеподобныхдействиянаполеонаиалекса
ндраотсловакоторыхзависелоказалосьчтобысобытиесовершилосьилинесовершилосьбылитакжемалопр
оизвольныкакидействиекаждогосолдаташедшеговпоходпожребиюилипонаборуэтонемоглобытьиначеп
отомучтодлятогочтобыволянаполеонаиалександратехлюдейоткоторыхказалосьзависелособытиебылаи
сполненанеобходимобылосовпадениебесчисленныхобстоятельствбезодногоизкоторыхсобытиенемогл
обысовершитьсянеобходимобылочтобымиллионылюдейврукахкоторыхбыладействительнаясиласолда
тыкоторыестреляливезлипровиантипушкинадобылочтобыонисогласилисьисполнитьэтуволюединичны
хислабыхлюдейибылиприведеныкэтомубесчисленнымколичествомсложныхразнообразныхпричинфат
ализмвисториинеизбежендляобъясненияразумныхявленийтоестьтехразумностькоторыхмынепонимае
мчемболеемыстараемсяразумнообъяснитьэтиявленияисториитемонистановятсядлянасразумнееинеп
онятнеекаждыйчеловекживетдлясебяпользуетсясвободойдлядостижениясвоихличныхцелейичувствует
всемсуществомсвоимчтоонможетсейчасделатьилинесделатьтакоетодействиенокакскороонсделаетего
такдействиеэтосовершенноевизвестныймоментвременистановитсяневозвратимымиделаетсядостояние
мисториивкоторойоноимеетнесвободноеапредопределенноезначениеестьдвестороныжизнивкаждомче
ловекежизньличнаякотораятемболеесвободначемотвлеченнееееинтересыижизньстихийнаяроеваягдече
ловекнеизбежноисполняетпредписанныеемузаконычеловексознательноживетдлясебянослужитбессозн
ательныморудиемдлядостиженияисторическихобщечеловеческихцелейсовершенныйпоступокневозвр
атимидействиеегосовпадаявовременисмиллионамидействийдругихлюдейполучаетисторическоезначен
иечемвышестоитчеловекнаобщественнойлестницечемсбольшимилюдьмионсвязантембольшевластион

имеетнадругихлюдейтемочевиднеепредопределенностьинеизбежностькаждогоегопоступкасердцецаре
вовруцебожьейцарьестьрабисториииисториятоестьбессознательнаяобщаяроеваяжизньчеловечествавсяк
ойминутойжизницарейпользуетсядлясебякакорудиемдлясвоихцелейнаполеоннесмотрянаточтоемубол
еечемкоганибудьтеперьвгодуказалосьчтоотнегозависелоилинекаквпоследнемписьмеписалемуалекса
ндрникогдаболеекактеперьнеподлежалтемнеизбежнымзаконамкоторыезаставлялиегодействуявотноше
ниисебякакемуказалосьпосвоемупроизволуделатьдляобщегоделадляисторииточтодолжнобылосоверш
итьсялюдизапададвигалисьнавостокдлятогочтобыубиватьдругдругаипозаконусовпаденияпричинподде
лалисьсамисобоюисовпалисэтимсобытиемтысячимелкихпричиндляэтогодвиженияидлявойныукорыза
несоблюдениеконтинентальнойсистемыигерцогольденбургскийидвижениевойсквпруссиюпредпринят
оекакказалосьнаполеонудлятоготолькочтобыдостигнутьвооруженногомираилюбовьипривычкафранцу
зскогоимператораквойнесовпавшаясрасположениемегонародаувлечениеграндиозностьюприготовлени
йирасходыпоприготовлениюипотребностьприобретениятакихвыгодкоторыебыокупилиэтирасходыиод
урманившиепочестивдрезденеидипломатическиепереговорыкоторыеповзглядусовременниковбыливед
енысискреннимжеланиемдостижениямираикоторыетолькоуязвлялисамолюбиетойидругойстороныими
ллионымиллионовдругихпричинподделавшихсяподимеющеесовершитьсясобытиесовпавшихснимкогд
асозрелояблокоипадаетотчегоонопадаетоттоголичтотяготееткземлеоттоголичтозасыхаетстерженьотто
голичтосушитсясолнцемчтотяжелеетчтоветертрясетегооттоголичтостоящемувнизумальчикухочетсясе
стьегоничтонепричинавсеэтотолькосовпадениетехусловийприкоторыхсовершаетсявсякоежизненноео
рганическоестихийноесобытиеитотботаниккоторыйнайдетчтояблокопадаетоттогочтоклетчаткаразлага
етсяитомуподобноебудеттакжеправитакженеправкакитотребенокстоящийвнизукоторыйскажетчтоябл
окоупалооттогочтоемухотелосьсестьегоичтоонмолилсяобэтомтакжеправинеправбудеттоткткоскажетчт
онаполеонпошелвмосквупотомучтоонзахотелэтогоиоттогопогибчтоалександрзахотелегопогибеликакп
равинеправбудеттоткткоскажетчтозавалившаясявмиллионпудовподкопаннаягораупалаоттогочтопослед
нийработникударилподнеепоследнийразкиркоювисторическихсобытияхтакназываемыевеликиелюдис
утьярлыкидающиенаименованийсобытиюкоторыетакжекакярлыкименеевсегоимеютсвязиссамымсобы
тиемкаждоедействиеихкажущеесяимпроизвольнымдлясамихсебявисторическомсмысленепроизвольно
анаходитсявсвязисовсемходомисторииопределенопредвечноаа

КЛЮЧ: (425, 100)

Найчастіші біграми шифрованого тексту:

1. ве
2. да
3. эб
4. ге
5. ме

Розпізнавач російської мови:

Для визначення того, чи являється текст інформативним використовувався підхід на основі індексу відповідності та ентропії. Для кожного набору ключів аналізувався розшифрований текст, у випадку коли ентропія та індекс відповідності були у допустимих межах, то текст вважається коректним. Межі допустимості були визначені емпіричним шляхом.

Труднощі:

При виконанні даного практикуму виникли деякі труднощі. По-перше, некоректно було дане пояснення щодо необхідного алфавіту, а саме заміна твердого та м’якого знака.
Окрім цього деякі труднощі викликав алгоритм перебору можливих наборів біграм.

Висновок: у ході виконання практикуму було набуто знань з використання афінного шифру та методів його криптоаналізу. Було набуто навичок аналізу тексту на його інформативність за допомогою статистичних даних, розглянуто декілька моделей на основі яких проводився аналіз.