Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

З дисципліни «Криптографія»

Криптоаналіз афінної

біграмної підстановки

Виконав:

студент 3 курсу ФТІ

групи ФБ-83
Самчук Тарас

Перевірив:

Чорний О. М.

Київ – 2020

Варіант №18

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.

Результат виконання роботи:

5 найчастіших біграм шифрованого тексту: ве, да, эб, ге, ме.
Ключ шифру: (a = 425, b = 100)
Для визначення коректності розшифрованого тексту було використано два методи: підрахунок заборонених біграм та частот букв в тексті.

Шифрований текст:

юетруожсвеызцэзыфшойызмбибсйкврбсйэффшщшвожкмчюетруожсвекзюегшшоакжжябсйц
свещтюсроауцезохюдбйэйаяэчэьогбйэжзмеьэнецеяэйгвекзсйютэфейцшгшимюетруожсвейбм
омчьогбчуткаучзэзщмжзвзгефхмафыяэюэрелфауимчмгембуйвецщкэмоцыэбьекзмафыяэбьше
мхдшчюфтчймеацжзвзгефхмафыяэюэрелфауимчмгелецшвимореиыфемэиоялшоуйфбяшмаок
жыцзбкжжябсйцсвещтюсроауцезохюдбркшомэршйаябйолрхэдаючетжжгтифдзтшттфычсведа
етсчлехввамчглмоцтябмчжзвзгефхмаллэзиоаущтюсроаучмэзршоюжеоэщедающюеютвючавэ
ыфдшгегшчэмэдэдамчвенеттючмочажсвершоюжеоэщечмгецехйызребэлхывмыгеузызталлэф
фшщшьэвемаэфлшщтсэиеабзеьаллжсвелешжфехййэезбйютяшлфнекцршчмхвсйызвееосэткгй
реткммвеуоцыэбьекзюсвершгеюкоюдбкзиэезнжцышоларемангмэяшбшашксййгшвозшашткш
ощсревкэбюсейчффыяэюэчкэбюсейчфокаагтсдвзбэхэвейюейюэббморенеозюбюсбрвеушйжф
шьэаыфшойызмбибсйвйэффшщшвожкмчрещбдоуйюевебкэфлеишеьэщлэыфэфлшщшнеоюю
чялфеузхосйлхлецшвиффкшненрлечммэээиожкэщлэыфялфыфедаууййютциимайсмббщтюсро
фгмэщтнвдаяферфанрршдедаважсимдэщбдоуйршюетруожсвечмдэшбяеимцщдшшдяэдашзцц
кэрзнэвччсфбсвьцавьцззюевеацмашоцыэбьечюдбмбуйвецщкэрзгшцйьоатчфцтсыэбчажкгзфл
нэвдчаозглцтэенемхдшчюфтчйцэхекэсшворбфжаышолаякркмщбфпжвэщшфаюаяекйвеларбв
йчфуйезсмонрквеацкэайчфуэкзхэнэаыжсючофббнвдабэуаллжсвеншеьллоюнпмощмнрюэцщд
шайатэлллокозтшттфыфцкэрзнэьтжжгтибффбовууочэбмоткаувчсймебймещлающтьэаэчмнэаю
ффйшсмвчсверкзшыаакчмеиоеэдагтжкэфршофгшушвосдщтчьейледэамткьобрмыаакчгйршвз
вшломоимцжатяфсчочшйгедйджцтцзцявдлечммэиыяэюэимялфыфшойызмбжщмйифршййюэ
ббвчкчменэушдацшушбюэбеиючфцгбаюерючнрбэамткьояшщтюсровшбюэбеимомчвдааитдф
йшмйээбйщклраадшмхреужлалрщтюсроуэнээшьмстевщтюсрощтнвдаяферфанркзщеоэкзмеце
шыозцшщбффсчййчмчмысйвюеэщвроркэфэбхпимдэюебфзшзоюсвегосймэбйозиомойэплфеуз
хосйлхжйоюзабряеоэкзмецегегосчмышонвуудабэвшмхредаййцеууашоцнздабрбйюдатэлвдле
дыяффэуыяэюэюыфеыжцшдаййэфцтфэдиьшнрлечммэуаркаусшщтюсроаужзмейкжжкзюегш
шойечфеймэбфсэцеайжзвзбэббгэааюзлхкзвзилцтэечйчфземхдшчюфтчймеиыфшойызмбтшмй
домчнпрбьояшфбройпрбьояшюшкфллынозбьхжткллокцыозззюедажычайояфвеяэеомщббзпж
цжюзшсшнэчмшоршвзжевшнээароуййцшюгэршвзжевшкюбвьцнеаэютуачучашйссимэкцыозн
элехввакздаэбяккчмоьшцщдшэюдбоюдфцеаймшкзюегшшоуэцезоаоючллгечмчмлхйпрбжюао

цыэбьевоьеткгткэнйлафшаерзьэючаадажычафжяфййцрорфрбрбкздажыванфауткмчршчмгеч
мцезоаозшсшнэчмбйейцтлзйааоиыхпрбябмысйициэлхкзпагтюсццжййцшюсахпрфауимршщег
боюхюзарахпмоючллгечмчмлхцезоошсшнэчмршчмгероютгльогбйэровюдбоюыыяэбьйемхдш
чюфтчйменеюсофдарзсймеыюгшьэифябвкезгвфшровюдбоюшймчщвцтлзиоаумбуймэттсйхэй
эршчмгечмлтьогцтйместрфэбмьйэмысйгшдерздивдоэеавагтдарзйэзыцтйэффлшневенемафыф
еыжцшгелтьогцтйтцчтрфэбмьтщчаркюзгшвючжщвреаэогмэуыяэюэвоюсялшоючллгечмчмлх
даябоюзаеыяэюэимюаффлшдэшбшззвыыяэюэьйэфчзнэщблаллжсвечмщтсэюфеймэвемаоюдб
сэббнвэфварбйошоюсвершчмгеййвбьсчарбйоаущтюсроаулечммэмзлечммэнвэбгооюдбсйэфц
тфэлхнрвемхмеюевеацмазередеспречмгелецшвичавйевэбгохюдбвчфбнэшодбовууаафшщийй
чемйцевдушгецшуштквдщцбйчфййцеялгтжжычуээарояфсйвецйвзчзюзецкэрзлхлшашюедесо
сдвееоааркссшжзюоеймемхмецшмепакчкожжывбфсйвежзкзвзчзсинэверыдбовууаюффлрлшаш
юедесосддшайчфбркзюегшшоуэябвкезгвозааббэфркаагтсдвзбэлшгежзвзгефхмаоюшйоюзаяш
лецшвифбсйвэнэршлецшвифбсйяюдбчаркссшузгещтсэюфэбйохкрксвуудабэвкчпденелехвваци
нвкшнедыкдщвюентвютщфбмышорюгтягвершщегбоюзавэкзушюевеацмащвервенемаоюдфэб
доцыэбьекзшзгшцйьоатваюдцщдшхейкаагтсджзвзгефхвзбэлшгелечммэвюдбуэшыэбршкзршо
южеоэщечмгеледыывмояшашксййгшвосдоюдайрвшмхдаюючжщвренеыжмевеммрйоюзаяшр
шщегбоюшйэфцтфэлхнрршоюжеоэщечмгемаоюсчфбнэшодбовууттакмдмевеммнюдбывууда
бэвшмхкзэйфбуйэбюзщммевеммейютрбибффчжнэщтэфшзйамыжицэкздечмгемаоюоеьэлегбу
йфбййвэшыэбьэлхюаофэбышоэьэеосдййэзчмыбовуужюдбмыяэцшдшимтгвеацашксййгшвосч
менэушдацедйгегосдозщозеытжжимуыяэюэенваябыжпфййвеяэроеэпюйпмощбтеврэомоббрш
озоцлосдифгшьэоазшдараюдозоцлосйлхмевеммйчаоиышовчйшшсючаегшючшйызозючнрозо
цлозеврэочаюгмэифгшьэифййвеяэчаючшоййызрешрмйеверкзэоцтжжычршеэршюетруоьшжз
двзуушгецшьпффуащбэйвюаыэбфжшшмйэйцеаедеивердеданпмобрбфсэыбюсимцьрбууюсоф
даэцуабйючсцбшдацедйцевчмазеучхпуалшфсуйюврбвавэнэршюврбвараркзшведшайчфяшре
жзцймефешоюврбйшвшнеызявуудабэбгвелецшвиморерфыжцшдаимшчкчмочффшщшьэдаьоэ
фчанрршцеюфозмэсмдэдшэзуанрдедайрьэючййвеяэффмевефехеревчьшуоейцеаехозшцыфшд
ещтнврбморечжкзушьэьшдаквцшдагтшоэпыжьэюкчпдешсрбэфвкйпыжщхнэеолрмевеозлаюч
аегшейцеаехоисючаамбщсморшьшеэйацтейшэыэщовймэрэзолрферфлравщсрбэфвкршыжашг
осэшыэбтруащтнвиэезвоошючхжркшонсрбэфвклещоварбйохпффуащбэйвюдосййцыэйюейле
щоварбйосчгтлвяшмвердеданпмобрййвеяэуштквдоюбшушгецшуштквдэшгшайэфцткшвозую
едажыокршцеюфозмэдэдшайчфяшялсйэфчзюзифэффшщшьэочфбнэшомчсвуудабэивьцчэыбо
вууюейцнзуаййвеяэуштказшщоисмояшушпфыиейвечаушгецшюойеьяейчфморелбейуопьщсю
чтюэбеивчфбовьчяеьйшрвзйаючаемхкшмбуймэшовчьшуоывьцчэыбовуувшщеушбэхоьшщтн
вфыфшдшгшвосйлхроеэпюйпредаякчпденеялфысйицекуйцтфьльетрфэфьцэшаеьхууцзюхейл
хозкэдагтйэййвеяэлазшдаяюейлещоварбйолроюьзотзшрзбпыжщхушгецшушдарзбйщкаудэцц
ведпыжьэцзфшгыэбфжшшмйеверлшвржзмеьцоэючщбэйцевдэшгшзоцыэбьевоейщеютдоважс
веючаюэбьшушбкллюзьэжцнхвшюшюхьлщвакжжябсйцсвеааршневзбэлшгефбровкркдысйгш
хоючиэфхщшиэезгшацябвкезгвжожкллюзаегшвкрквшюшюхршюещбйпябвшлоеэпюйпимцж
ркшомчмевеммчжуйызмбибяшнедшайчфьрцеуофимойэлшвржзмшацжзвзгефхюебфзшацщтс
эюфэблврбвакверююбшнедшэзщбээдагтйэвемащвэбгооюдбсйэфцтфэлхнрцщоэвзчзюзщфгляб
йййояфсйвеявервенемаоюфцкэрзлхатэлатэлуэюевзмеццледыывмобрщтюсроюецврбябййвймч
ййоюьщййэфчзнэсгмэдйоюзаяшташйссвчрбцэуыяэюэгверюаллщвбэсшьэээщбифауимакгтлж
ьоейоюцщдшьэвкшомэршйаябйоаухэдаючшэншеьллэбквможцшлткчусвбэсшьэрфауткдыьцх
йтщщтнвщтролазшжзукжжябсййоцыэбьеццщблаллааэбякжсвечмдедаглццлхцегтзпморенедэо
зфбгюэфвэщтффнсжзлтьогцтйменевчюшозвеозвфауршледыяфдзэйозшыэбхпмояшщшнекзфе
юзофгшушьэялозгвяещосйлхйыяэневембмочуьтуйжеымюещтглааэфгшьэжэюеютвюредаеыяэ
оюфшвшьэларквдомнелкаагтошчмокжыфбегмэозодщвшэщвфтузьэдияшюеушдаффатчждшр
шсвмыгеузмэуштказшюшфшнецемммевеммиыэфмлеркцлеттючмоьэмеююдбффнвмошййитм
оьэипрбьояшмвсймэсшьэхчьтуэмевеммуаэбякнцпжмбибййчэбгюяшвеаэатэлаудагтшошэдэ
шбяеимдэшбяерейвьцчэуыяэюэюыщвдшэздивднрюеоэщшцяьшлецшвичавйэйоюзаяшледыяф
фэрйьэбкллюзледтрбйрхбоксэчзюзуаааушнешофыывйшвеьаллэбюсведрневшуайжючгшаавен
енэмаджуйсдйшмйвшгпмочеьаллэбюсвесцфэмйэйэббьючмаааабпрбьшбсвецшвшнацрлшвшне
аавененэмасйвеняючофьэоцузмхюэтцжеушмйэйейлхялшоюсверщтюсрояфлшюаааэбяксйэф
чздшьэуаюдгйгебэгыяэмевеммрйэфцтдзуанрбйщкзшыэщомореьешльоюсеймееймэрэзозшлеч

ммэеэвейюааьожкмевеммзовудшбсвещюгемечзюзуааавенемаокгшбсважзозюбнлйшмйээвеац
юедесозшжцдшьарксшщтяфчарксшршщтяфжзцэвеютвюмоокдайрлэлфьэоцмевеммайжзсшбс
вещюгемежыябзеьаллжсвеючыдаарбсйвйейлхялсэмазеучэбфбнроююакчызьпиыозбэршщтяф
жцдшьаааеасйжзсшбсвекзюегшшоюекшшфщеткэцюевеацмазенжмдаарбюаллсэаавенеюечэяс
веябвкезгвсжмдаарбялфыллжюрбжкркщтяфроиыозююлвуавейкветкчпуамаджяфябффдзэйиф
дэшбяеюылвэфюелкфыьокзцлгтпцчзээаавенемафысйгшхочуозаеуожклветфбюехоьшюеббнвь
эстжжцэыкьщбэдагтюсейцэрйоюзабряарккзамрзючошцшнэцэрбовййсащркбхксвэщлэмоуэщ
шрерзьэайоюзатщмевеммуарксшжзоркбхквчмоьшбйялсэщшфабфпжййезсмдйоюзаяшбкчпде
нвуудабэеэнкчпуяьшнрвчщтсэюфэбйосчщбэймчвдлшврбэдагтюсеймедйсмббмоиыфеыжцемх
реьомдщвчанрбйшртэлебйючжededэдагтйэяещтнврбмофыфшщфщсрегз

Розшифрований текст:

понятночтотакимпредставлялосьделосовременникампонятночтонаполеонуказалосьчтопричи
нойвойныбылиинтригианглиикаконiговорилэтонаостровесвеленыпонятночточленаманглийс
койпалатыказалосьчтопричинойвойныбыловластолюбиенаполеоначтопринцуольденбургско
муказалосьчтопричинойвойныбылосовершенноепротивнегонасилиечтокупцамказалосьчтопр
ичинойвойныбылаконтинентальнаясистемаразорявшаяевропучтостарымсолдатамигенералам
казалосьчтоглавнойпричинойбыланеобходимостьупотребитьихвделолегитимистамтоговреме
ниточтонеобходимобыловосстановитьадипломатамтоговремениточтовсепроизошлооттогочт
осоюзроссиисавстриейвгодунебылдостаточноискусноскрытотнаполеонаичтоневловкобылнапи
санзапонятночтоэтиищебесчисленноебесконечноеколичествопричинколичествокоторыхзав
иситотбесчисленногоразличияточекзренияпредставлялосьсовременникамнодлянаспотомковс
озерцающихвовсемегообемегромадностьсовершившегосясобытияивникающихвегопростойис
трашныйсмыслпричиныэтипредставляютсянедостаточнымидлянаснепонятночтобымиллион
ылюдейхристианубивалиимучилидругдругапотомучтонаполеонбылвластолюбивалександртв
ердполитикаанглиихитраигерцогольденбургскийобиженнельзяпонятькакуюсвязьимеютэтиоб
стоятельствассамымфактомубийстваинасилияпочемувследствиетогочтогерцогобижентысячи
людейсдругогокраяевропыубивалииразорялилюдейсмоленскойимосковскойгубернийибылиу
биваемыимидлянаспотомковнеисториковнеувлеченныхпроцессомизысканияипотомуснезате
мненнымздравымсмысломсозерцающихсобытиепричиныегопредставляютсявнеисчислимомк
оличествечембольшемыуглубляемсявизысканиепричинтембольшенамихоткрываетсяивсякая
отдельновзятаяпричинаилицелыйрядпричинпредставляютсянамодинаковосправедливымисам
ипосебеиодинаковоложнымипосвоейничтожностивсравнениисгромадностьюсобытияиодинак
оволожнымипонедействительностисвоейбезучастиявсехдругихсовпавшихпричинпроизвестис
овершившееясобытиетакойжепричинойкакотказнаполеонаотвестисвоивойсказавислуиотдат
ьназадгерцогствоольденбургскоепредставляетсянамижеланиеилинежеланиепервогофранцузс
когокапралапоступитьнавторичнуюслужбуибоежелибыоннезахотелидтинаслужбуинезахотел
быдругойитретийитысячныйкапралисолдатнастолькоменеелюдейбылобыввойскенаполеонаи
войнынемоглобыбытьежелибынаполеоннеоскорбилсятребованиемотступитьзавислуиневелел
наступатьвойскамнебылобывойныноежелибывсесержантынепожелалипоступитьнавторичну
юслужбутожевойнынемоглобыбытьтоженемоглобыбытьвойныежелибынебылоинтриганглии
инебылобыпринцаольденбургскогоичувстваоскорбленияалександреинебылобысамодержавн
ойвластивроссииинебылобыфранцузскойреволюцииипоследовавшихдиктаторстваиимпериии
всеготогочтопроизвелофранцузскуюреволюциюитакдалеебезоднойизэтихпричинничегонемо
глобыбытьсталобытьпричиныэтивсемиллиардыпричинсовпалидлятогочтобыпроизвеститочто
былоисследовательноничтонебылоисключительнойпричинойсобытияасобытиедолжнобылосо
вершитьсятолькопотомучтоонодолжнобылосовершитьсядолжныбылимиллионылюдейотрек
шисьотсвоихчеловеческихчувствисвоегоразумаидтинавостоксзападаиубиватьсебеподобныхт
очнотакжекакнесколькovековтомуназадсвостоканазападшлитолпылюдейубиваясебеподобны
хдействиянаполеонаиалександраотсловакоторыхзависелоказалосьчтобысобытиесовершилось
илинесовершилосьбылитакжемалопроизвольныкакидействиекаждогосолдаташедшеговпоход
пожребиюилипонаборуэтонемоглобытьиначепотомучтодлятогочтобыволянаполеонаиалексан
дратехлюдейоткоторыхказалосьзависелособытиебылаисполненанеобходимобылосовпадение
бесчисленныхобстоятельствбезодногоизкоторыхсобытиенемоглобысовершитьсянеобходимо

былочтобымиллионылюдейврукахкоторыхбыладействительнаясилаолдатыкоторыестреляли везлипровиантипушкинадобылочтобыонисогласилисьисполнитьэтуволюединичныхислабых людейибылиприведеныкэтомубесчисленнымколичествомсложныхразнообразныхпричинфата лизмвисториинеизбежендляобъясненияразумныхявленийтоестьтехразумностькоторыхмыне понимаемчемболеемыстараемсяразумнообяснитьэтиявленияисториитемонистановятсядляна сразумнееинепонятнеекаждыйчеловекживетдлясебяпользуетсясвободойдлядостижениясво ихличныхцелейичувствуетвсемсуществомсвоимчтоонможетсейчасделатьилинесделатьтакое тодействиенокакскороонсделаетеготакдействиеэтосовершенноевизвестныймоментвременист ановитсяневозвратимымиделаетсядостояниемисториивкоторойоноимеетнесвободноеапредоп ределенноезначениеестьдвестороныжизнивкаждомчеловекежизньличнаякоторыйтемболеесво боднаячемотвлеченнеееинтересыижизньстихийнаяроеваягдечеловекнеизбежноисполняетпре дписанныеемузаконычеловексознательноживетдлясебянослужитбессознательныморудиемдл ядостиженияисторическихобщечеловеческихцелейсовершенныйпоступокневозвратимидейст виеегосовпадаявовременисмиллионамидействийдругихлюдейполучаетисторическоезначение чемвышестоитчеловекнаобщественнойлестницечемсбольшимилюдьмионсвязантембольшевл астионимеетнадругихлюдейтемочевиднеепредопределенностьинеизбежностькаждогоегопост упкасердцецаревоврученебожьейцарьестьрабисториииисториятоестьбессознательнаяобщаяроева яжизньчеловечествавсякойминутойжизницарейпользуетсядлясебякакорудиемдлясвоихцелей наполеоннесмотрянаточтоемуболеечемкогданибудьтеперьвгодуказалосьчтоотнегозависелоил инекаквпоследнемписьмеписалемуалександрникогдаболеекактеперьнеподлежалтемнеизбежн ымзаконамкоторыезаставлялиегодействуявотношениисебякакемуказалосьпосвоемупроизвол уделатьдляобщегоделадляисторииточчтодолжнобылосовершитьсялюдизапададвигалисьнавос токдлятогочтобыубиватьдругдругаипозаконусовпаденияпричинподделалисьсамисобоюисовп алисэтимсобытиемтысячимелкихпричиндляэтогодвиженияидлявойныукорызанесоблюдение континентальнойсистемыигерцогольденбургскийидвижениевойсквпруссиюпредпринятоекак казалосьнаполеонудлятоготолькочтобыдостигнутьвооруженногомираилюбовьипривычкафра нцузскогоимператоракквойнесовпавшаясрасположениемегонародаувлечениеграндиозностьюп риготовленийирасходыпоприготовлениюипотребностьприобретениятакихвыгодкоторыебыок упилиэтирасходыиодурманившиепочестивдрезденеидипломатическиепереговорыкоторыепо взглядусовременниковбыливеденысискреннимжеланиемдостижениямираикоторыетолькоуяз влялисамолюбиетойидругойстороныимиллионымиллионовдругихпричинподделавшихсяпод имеющеесовершитьсясобытиесовпавшихснимкогдасозрелояблокоипадаетотчегоонопадаетот тоголичтотяготеетземлеоттоголичтозасыхаетстерженьоттоголичтосушитсясолнцемчтотяже леетчтоветертрясетегооттоголичтостоящемувнизумальчикухочетсясестьегоничтонепричинав сеэтотолькосовпадениетехусловийприкоторыхсовершаетсявсякоежизненноеорганическоести хийноесобытиеитотботаниккоторыйнайдетчтояблокопадаетоттогочтоклетчаткаразлагаетсяит омуподобноебудеттакжеправитакженеправкакитотребенокстоящийвнизукоторыйскажетчтоя блокоупалооттогочтоемухотелосьсестьегоичтоонмолилсяобэтомтакжеправинеправбудеттотк тоскажетчтонаполеонпошелвмосквупотомучтоонзахотелэтогоиоттогопогибчтоалександрзахо телегопогибеликакправинеправбудеттоткткоскажетчтозавалившаясявмиллионпудовподкопан наягораупалаоттогочтопоследнийработникударилподнеепоследнийразкиркоювисторических событияхтакназываемыевеликиелюдисутьярлыкидающиенаименованийсобытиюкоторыетак жекакярлыкименеевсегоимеютсвязиссамымсобытиемкаждоедействиеихкажущееясяимпроизв ольнымдлясамихсебявисторическомсмысленепроизвольноанаходитсявсвязисовсемходомист ориииопределенопредвечно.

Висновки: під час виконання практичної роботи №3 я отримав навички моноалфавітної підстановки. Навчився розшифровувати текст зашифрований афінною підстановкою. На практиці навчився визначати некоректний відкритий текст.