Міністерство освіти і науки України НТУУ«Київський політехнічний інститут» Фізико-технічний інститут

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ No3 Криптоаналіз афінної біграмної підстановки

Виконали:

студент групи ФБ-84 Ніколаєнко Едуард студент групи ФБ-84 Коцюк Роман

Мета роботи:

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

Завдання:

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 No1, 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 (а, 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

П'ять найчастіших біграм шифртексту:

ве, да, эб, рб, чм

Опис роботи автоматичного розпізнавача російської мови:

перевіряє частоти двух найчастіших літер(о, а) та найрідкіснішої(ф)

Шифрований текст:

юетруожсвеызцэзыфшойызмбибсйкврбсйэффшщшвожкмчюетруожсвекзюегшшоакжжябсйцсвещтюсроауцезохюдбйэйаяэчэьогбйэжзмеьэне цеяэйгвекзсйютэфейцшгшимюетруожсвейбмомчьогбчуткаучзэзцмжзвзгефхмафыяэюэрелфауимчмгембуйвецщкэмоцыэбьекзмафыяэбьшем хдшчюфтчймеацжзвзгефхмафыяэюэрелфауимчмгелецшвимореиыфемэиоялшоуйфбяшмаокжыцзбкжжябсйцсвещтюсроауцезохюдбркшомэр шйаябйолрхэдаючетжжгтифдэтшттфычсведаетсчлехввамчглмоцтябмчжзвзгефхмаллэзиоаущтюсроаучмээршоюжеоэщедаюцюеютвючавэыф дшгегшчэмэдэдамчвенеттючмочажсвершоюжеоэщечмгецехйызребэлхывмыгеузызталлэффшщшьэвемаэфлшщтсэиеабзеьаллжсвелешжфехй йэезбйютяшлфнекцршчмхвсйызвееосэткгйреткммвеуоцыэбьекзюсвершгеюкоюдбкзиэезнжцышоларемангмэяшбшашксййгшвозшашткшощс ревкэбюсейчффыяэюэчкэбюсейчфокаагтсдвзбэхэвейюейюэббморенеозюбюсбрвеушйжфшьэаыфшойызмбибсйвйэффшщшвожкмчрещбдоуй юевебкэфлеишеьэщлэыфэфлшщшнеоюючялфеузхосйлхлецшвиффкшненрлечммэээиожкэщлэыфялфыфедаауййютциимайсмббщтюсрофгмэ щтнвдаяферфанрршдедаважсимдэщбдоуйршюетруожсвечмдэшбяеимцшдшшдяэдашзццкэрзнэвччсфбсвьцавьцззюевеацмашоцыэбьечюдбмб уйвецщкэрэгшцйьоатчфцтсыэбчажкгэфлнэвдчаозглцтэенемхдшчюфтчйцэхекэсшворбфжаышолаякркмщбфпжвэщшфаюаяекйвеларбвйчфуй езсмонрквеацкэайчфуэкзхэнэаыжсючофббнвдабэуаллжсвеншеьллоюнпмощмнрюэцщдшайатэлллокозтшттфыфцкэрзнэьтжжгтибфбовууочэ бмоткаувчсймебймещлаюцть эа эчмн эа юффйшсмв чсверк зшы аакчме и ое эдагтжкэфршофгшуш восдщтчьей ледэам ткь обрмы аакчгйршв звшлом оимцжатяфсчочшйгедйджцтцзцявдлечммэиыяэюэимялфыфшойызмбжшмйифршййюэббвчкчменэушдацшушбюэбеиючфцгбаюерючнрбэамт кьояшщтюсровшбюэбеимомчвдааитдфйшмйээбйщклраадшмхреужлалрщтюсроуэнээшьмстевщтюсрощтнвдаяферфанркзщеоэкзмецешыоэц шщбффсчйимчмысйвюеэщвроркэфэбхпимдэюебфзшзоюсвегосймэбйозиомойэплфеузхосйлхжйоюзабряеоэкзмецегегосчмышонвуудабэвшм хредаййцеууашоцнздабрбйюдатэлвдледыяффэуыяэюэюыфеыжцшдаййэфцтфэдиьшнрлечммэуаркаусшцтюсроаужэмейкжжкэюегшшойечфе ймэбфсэцеайжзвэбэббгэааюэлхкзвзилцтэечйчфземхдшчюфтчймеиыфшойызмбтшмйдомчнпрбьояшфбройпрбьояшюшкфллынозбьхжткллок цыоэээюедажычайояфвеяэеомщббзпжцжюзшсшнэчмшоршвзжевшнээароуййцшюгэршвзжевшкюбвьцнеаэютуачучашйссимэкцыознэлехввак здаэбяккчмоьшцщдшэюдбоюдфцеаймшкзюегшшоуэцезоаоючллгечмчмлхйпрбжюаоцыэбьевоьеткгткэнйлафшаерзьэючаадажычафжяфйййц рорфрбрбкздажыванфауткмчршчмгечмцезоаозшсшнэчмбйейцтлзйааоиыхпрбябмысйициэлхкзпагтюсццжййцшюсахпрфауммршцегбоюхюза рахпмоючилгечмчмихцезоошсшнэчмршчмгероютгиьогбйэровюдбоюьыяэбьйемхдшчюфтчйменеюсофдарзсймеыюгшьэифябвкезгвфшровю дбоюшймчщвцтлзиоаумбуймэттсйхэйэршчмгечмлтьогцтйместрфэбмьйэмысйгшдерздивдоэеавагтдарэйээыцтйэффлшневенемафыфеыжцшг елтьогцтйтцчтрфэбмьтщчаркюзгшвючжщвреаэогмэуыяэюэвоюсялшоючллгечмчмлхдаябоюзаеыяэюэимюаффлшдэшбшззвыыяэюэьйэфчзнэ щблаллжсвечмщтсэюфеймэвемаоюдбсэббнвэфварбйошоюсвершчмгеййвбьсчарбйоаущтюсроаулечммэмэлечммэнвэбгооюдбсйэфцтфэлхнрв емхмеюевеацмазередеспречмгелецшвичавйевэбгохюдбвчфбнэшодбовууаафшщиййчемйцевдушгецшуштквдицбйчфййцеялгтжжычуээарояф сйвецйвзчзюзецкэрэлхлшашюедесосдвееоаарксшжзюоеймемхмецшмепакчкожжывбфсйвежзкзвзчзсинэверыдбовууаюффлрлшашюедесосдд шайчфбркзюегшшоуэябвкезгвозааббэфркаагтсдвзбэлшгежзвзгефхмаоюшйоюзаяшлецшвифбсйвэнэршлецшвифбсйяюдбчарксшузгещтсэюф эбйохкрксвуудабэвкчпденелехввацинвкшнедыкдщвюентвютщфбмьшорюгтягвершщегбоюзавэкзушюевеацмащвервенемаоюдфэбдоцыэбьек зшэгшцйьоатваюдцидшхейкаагтсджэвэгефхвэбэлшгелечммэвюдбуэшыэбршкэршоюжеоэщечмгеледыывмояшашксййгшвосдоюдайрвшмхда юючжщвренеыжмевеммрйоюзаяшршщегбоюшйэфцтфэлхнрршоюжеоэщечмгемаоюсчфбнэшодбовууттакмдмевеммнюдбывуудабэвшмхкзэй фбуйэбюэщммевеммейютрбибффчжнэштэфшзйамыжицэкздечмгемаоюосьэлегбүйфбййвэшыэбьэлхюаофэбышоэьэеосдййээчмыбовуужюдб мыяэциидиимтгвеацашксййгшвосчменэушдацедйгегосдозщозеытжжимуыяэюэенваябыжпфййвеяэроеэпюйпмощбтеврэомобрршозоцлосдиф гшьэоазшдараюдозоцлосйлхмевеммйчаоиышовчйшшсючаегшючшйызозючнрозоцлозеврэочаюгмэифгшьэифййвеяэчаючшоййызрешрмйеве ркзэоцтжжычршеэршюетруоьшжздвзуушгецшыпффуащбэйвюаыэбфжшшмйэйцеаедеивердеданпмобрбфсэыбюсимцьрбууюсофдаэцуабйючс цбшдацедйцевчмазеучхпуалшфсуйюврбвавэнэршюврбвараркзшведшайчфяшрежзцймефешоюврбйшвшнеызявуудабэбгвелецшвиморерфыж цшдаимшчкчмочффшщшьэдаьоэфчанрршцеюфозмэсмдэдшэзуанрдедайрьэючййвеяэффмевефехеревчьшуоейцеаехозшцыфшдещтнврбморе чжкзушьэьшдаквцшдагтшоэпыжьэюкчпдешсрбэфвкйпыжщхнэеолрмевеозлаючаегшейцеаехоисючаамбщсморшьшеэйацтейшэыэщовймэрэз олрферфлравщербэфвкршыжашгосэшыэбтруащтнвиэезвоошючхжркшонсрбэфвклещоварбйохпффуащбэйвюдосййцыэйюейлещоварбйосчгт

лвяшмвердеданпмобрййвеяэуштквдоюбшушгецшуштквдэшгшайэфцткшвозуюедажыокршцеюфозмэдэдшайчфяшялсйэфчзюзифэффшщшьэ очфбнэшомчсвуудабэивьцчэыбовууюейцнзуаййвеяэушткзшщоисмояшушпфыиейвечаушгецшюойеьяейчфморелбейуопьщсючтюэбеивчфбо вьчяеьйшрвзйаючаемхкшмбуймэшовчьшуоывьцчэыбовуувшщеушбэхоьшщтнвфыфшдшгшвосйлхроеэпюйпредаякчпденеялфысйицекуйцтф ьльетрфэфьцэшаеьхууцзюхейлхозкэдагтйэййвеяэлазшдаяюейлещоварбйолроюьзотэшрэбпыжщхушгецшушдарэбйщкаудэццведпыжьэцэфшг ыэбфжшшмйеверлшвржзмеьцоэючщбэйцевдэшгшзоцыэбьевоейщеютдоважсвеючаюэбьшушбкллюзьэжцнхвшюшюхьлщвакжжябсйцсвеаар шневзбэлшгефбровкркдысйгшхоючиэфхицшиэезгшацябвкезгвжожкллюзаегшвкрквшюшюхршюещбйпябвшлоеэпюйпимцжркшомчмевеммч жуйызмбибяшнедшайчфьрцеуофимойэлшвржзмшацжзвзгефхюебфзшацщтсэюфэблврбваквероюбшнедшэзщбээдагтйэвемащвэбгооюдбсйэф цтфэлхнрцщоэвзчзюзщфглябйййояфсйвеявервенемаоюфцкэрэлхатэлатэлуэюевэмеццледыывмобрщтюсроюецврбябййвймчййоюьщййэфчэнэ сгмэдйоюзаяшташйссвчрбцэуыяэюэгверюаллщвбэсшьэээщбифауимакгтлжьоейоюцщдшьэвкшомэршйаябйоаухэдаючшэншеьллэбквможцш лткчусвбэсшьэрфауткдыьцхйтщщтнвщтролазшжзукжжябсййоцыэбьеццщблаллааэбякжсвечмдедаглццлхцегтэпморенедэоэфбгюэфвэщтффн сжэлтьогцтйменевчюшозвеозвфауршледыяфдээйозшыэбхпмояшщшнекэфеюзофгшушьэялозгвяещосйлхйыяэневембмочуьтуйжеымюещтгла аэфгшьэжэюеютвюредаеыяэоюфшвшьэларквдомнелкаагтошчмокжыфбегмэозодщвшэщвфтузьэдияшюеушдаффатчждшршсвмыгеузмэуштк яшюшфшнецемммевеммиыэфмлеркцлеттючмоьэмеююдбффнвмошйййитмоьэипрбьояшмвсймэсшьэхчьтуэмевеммуаэбякнцпжмбибйймчэбг юяшвеаэатэлаудагтшошэдэшбяеимдэшбяерейвьцчэуыяэюэюыщвдшэздивднрюеоэщшцяьшлецшвичавйэйоюзаяшледыяффэрйьэбкллюзледт рбйрхбоксэчзюзуаааушнешофыывйшвеьаллэбюсведрневшуайжючгшаавененэмаджуйсдйшмйвшгпмочеьаллэбюсвесцфэмйэйэббьючмааабп рбьшбсвецшвшнацрлшвшнеаавененэмасйвеняючофьэоцузмхюэтцжеушмйэйейлхялшоюсвершщтюсрояфлшюаааэбяксйэфчздшьэуаюдгйгеб эгыяэмевеммрйэфцтдзуанрбйщкзшыэщомореьешльоюсеймееймэрэзозшлечммэеэвейюааьожкмевеммзовудшбсвещюгемечзюзуааавенемаокг шбсважзозюбнлйшмйээвеацюедесозшжцдшьарксшщтяфчарксшршщтяфжэцэвеютвюмоокдайрлэлфьэоцмевеммайжэсшбсвещюгемежыябзеь аллжсвеючыдаарбсйвйейлхялсэмазеучэбфбнроююакчызьпиьюзбэршцтяфжцдшьаааеасйжэсшбсвекзюегшшоюекшшфщеткэцюевеацмазенж мдаарбюаллсэаавенеюечэясвеябвкезгвсжмдаарбялфыллжюрбжкркщтяфроиьюзююлвуавейкветкчпуамаджяфябффдээйифдэшбяеюылвэфюел кфыьокзцлгтпцчзэзаавенемафысйгшхочуозаеуожклветфбюехоьшюеббнвьэстжжцэыкьщбэдагтюсейцэрйоюзабряарккзамрзючошцшнэцэрбов ййсащркбхксвэщлэмоуэщшрерзьэайоюзатщмевеммуарксшжзоркбхквчмоьшбйялсэщшфабфпжййезсмдйоюзаяшбкчпденвуудабэеэнкчпуяьш нрвчщтсэюфэбйосчщбэймчвдлшврбэдагтюсеймедйсмббмоиыфеыжцемхреьомдщвчанрбйшртэлебйючжедедэдагтйэяещтнврбмофыфшщфщс регз

Розшифрований текст:

понятночтотакимпредставлялосьделосовременникампонятночтонаполеонуказалосьчтопричинойвойныбылиинтригианглиикакониговорилэт онаостровесвеленыпонятночточленаманглийскойпалатыказалосьчтопричинойвойныбыловластолюбиенаполеоначтопринцуольденбургском указалось что причиной войны было совершенное противнего насилиечто купцам казалось что причиной войны былаконтинентальная системаразо рявшаяевропучтостарымсолдатамигенераламказалосьчтоглавнойпричинойбыланеобходимостьупотребитьихвделолегитимистамтоговремен иточтонеобходимобыловосстановитьадипломатамтоговремениточтовсепроизошлооттогочтосоюзроссиисавстриейвгодунебылдостаточноис кусноскрытотнаполеонаичтонеловкобылнаписанзапонятночтоэтииещебесчисленноебесконечноеколичествопричинколичествокоторыхзавис итотбесчисленногоразличияточекзренияпредставлялосьсовременникамнодлянаспотомковсозерцающихвовсемегообемегромадностьсоверш ившегосясобытияивникающихвегопростойистрашныйсмыслпричиныэтипредставляютсянедостаточнымидлянаснепонятночтобымиллионыл юдейхристианубивалиимучилидругдругапотомучтонаполеонбылвластолюбивалександртвердполитикаанглиихитраигерцогольденбургскийо биженнельзяпонятькакуюсвязьимеютэтиобстоятельствассамымфактомубийстваинасилияпочемувследствиетогочтогерцогобижентысячилюд ейсдругогокраяевропыубивалииразорялилюдейсмоленскойимосковскойгубернийибылиубиваемыимидлянаспотомковнеисториковнеувлече нныхпроцессомизысканияипотомуснезатемненнымздравымсмысломсозерцающихсобытиепричиныегопредставляютсявнеисчислимомколич ествечембольшемыуглубляемсявизысканиепричинтембольшенамихоткрываетсяивсякаяотдельновзятаяпричинаилицелыйрядпричинпредста вляютсянамодинаковосправедливымисамипосебеиодинаковоложнымипосвоейничтожностивсравнениисгромадностьюсобытияиодинаковол ожнымипонедействительностисвоейбезучастиявсехдругихсовпавшихпричинпроизвестисовершившеесясобытиетакойжепричинойкакотказн аполеонаотвестисвоивойсказавислуиотдатьназадгерцогствоольденбургскоепредставляетсянамижеланиеилинежеланиепервогофранцузского капралапоступитьнавторичнуюслужбуибоежелибыоннезахотелидтинаслужбуинезахотелбыдругойитретийитысячныйкапралисолдатнастоль коменеелюдейбылобыввойскенаполеонаивойнынемоглобыбытьежелибынаполеоннеоскорбилсятребованиемотступитьзавислуиневелелнаст упатьвойскамнебылобывойныноежелибывсесержантынепожелалипоступитьнавторичнуюслужбутожевойнынемоглобыбытьтоженемоглобы бытьвойныежелибынебылоинтриганглииинебылобыпринцаольденбургскогоичувстваоскорблениявалександреинебылобысамодержавнойвла стивроссииинебылобыфранцузскойреволюцииипоследовавшихдиктаторстваиимперииивсеготогочтопроизвелофранцузскуюреволюциюитак далеебезоднойизэтихпричинничегонемоглобыбытьсталобытыпричиныэтивсемиллиардыпричинсовпалидлятогочтобыпроизвеститочтобылои следовательноничтонебылоисключительнойпричинойсобытияасобытиедолжнобылосовершитьсятолькопотомучтоонодолжнобылосовершит ьсядолжныбылимиллионылюдейотрекшисьотсвоихчеловеческихчувствисвоегоразумаидтинавостоксзападаиубиватьсебеподобныхточнотак жекакнескольковековтомуназадсвостоканазападшлитолпылюдейубиваясебеподобныхдействиянаполеонаиалександраотсловакоторыхзависе локазалосьчтобысобытиесовершилосьилинесовершилосьбылитакжемалопроизвольныкакидействиекаждогосолдаташедшеговпоходпожреби юилипонаборуэтонемоглобытьиначепотомучтодлятогочтобыволянаполеонаиалександратехлюдейоткоторыхказалосьзависелособытиебылаи сполненанеобходимобылосовпадениебесчисленныхобстоятельствбезодногоизкоторыхсобытиенемоглобысовершитьсянеобходимобылочтоб ымиллионылюдейврукахкоторыхбыладействительнаясиласолдатыкоторыестреляливезлипровиантипушкинадобылочтобыонисогласилисьис полнитьэтуволюединичныхислабыхлюдейибылиприведеныкэтомубесчисленнымколичествомсложныхразнообразныхпричинфатализмвисто риинеизбежендляобяснениянеразумныхявленийтоестьтехразумностькоторыхмынепонимаемчемболеемыстараемсяразумнообяснитьэтиявле ниявисториитемонистановятсядлянаснеразумнееинепонятнеекаждыйчеловекживетдлясебяпользуетсясвободойдлядостижениясвоихличных целейичувствуетвсемсуществомсвоимчтоонможетсейчассделатьилинесделатьтакоетодействиенокакскороонсделаетеготакдействиеэтосовер шенноевизвестныймоментвременистановитсяневозвратимымиделаетсядостояниемисториивкоторойоноимеетнесвободноеапредопределенно езначениеесть двестороны жизнивкаж домчеловеке жизньличная котораятем болеесвободначем отвлечениееее интересыи жизньстихий на яроевая гдечеловекнеизбежноисполняетпредписанныеемузаконычеловексознательноживетдлясебянослужитбессознательныморудиемдлядостижени яисторическихобщечеловеческихцелейсовершенныйпоступокневозвратимидействиеегосовпадаявовременисмиллионамидействийдругихлю дейполучаетисторическоезначениечемвышестоитчеловекнаобщественнойлестницечемсбольшимилюдьмионсвязантембольшевластионимее тнадругихлюдейтемочевиднеепредопределенностьинеизбежностькаждогоегопоступкасердцецаревовруцебожьейцарьестьрабисторииистори ятоестьбессознательнаяобщаяроеваяжизньчеловечествавсякойминутойжизницарейпользуетсядлясебякакорудиемдлясвоихцелейнаполеонне смотрянаточтоемуболеечемкогданибудьтеперьвгодуказалосьчтоотнегозависелоилинекаквпоследнемписьмеписалемуалександрникогдаболе екактеперьнеподлежалтемнеизбежнымзаконамкоторыезаставлялиегодействуявотношениисебякакемуказалосьпосвоемупроизволуделатьдля общегоделадляисторииточтодолжнобылосовершитьсялюдизапададвигалисьнавостокдлятогочтобыубиватьдругдругаипозаконусовпаденияп ричинподделалисьсамисобоюисовпалисэтимсобытиемтысячимелкихпричиндляэтогодвиженияидлявойныукорызанесоблюдениеконтинента льнойсистемыигерцогольденбургскийидвижениевойсквпруссиюпредпринятоекакказалосьнаполеонудлятоготолькочтобыдостигнутьвооруж енногомираилюбовьипривычкафранцузскогоимператораквойнесовпавшаясрасположениемегонародаувлечениеграндиозностьюприготовлен оматическиепереговорыкоторыеповзглядусовременниковбыливеденысискреннимжеланиемдостижениямираикоторыетолькоуязвлялисамол юбиетойидругойстороныимиллионымиллионовдругихпричинподделавшихсяподимеющеесовершитьсясобытиесовпавшихснимкогдасозрело яблокоипадаетотчегоонопадаетоттоголичтотяготееткземлеоттоголичтозасыхаетстерженьоттоголичтосушитсясолнцемчтотяжелеетчтоветерт рясетегооттоголичтостоящемувнизумальчикухочетсясестьегоничтонепричинавсеэтотолькосовпадениетехусловийприкоторыхсовершаетсяв сякоежизненноеорганическоестихийноесобытиеитотботаниккоторыйнайдетчтояблокопадаетоттогочтоклетчаткаразлагаетсяитомуподобное будеттакжеправитакженеправкакитотребенокстоящийвнизукоторыйскажетчтояблокоупалооттогочтоемухотелосьсестьегоичтоонмолилсяоб

этомтакжеправинеправбудеттотктоскажетчтонаполеонпошелвмосквупотомучтоонзахотелэтогоиоттогопогибчтоалександрзахотелегопогибе ликакправинеправбудеттотктоскажетчтозавалившаясявмиллионпудовподкопаннаягораупалаоттогочтопоследнийработникударилподнеепос леднийразкиркоювисторическихсобытияхтакназываемыевеликиелюдисутьярлыкидающиенаименованийсобытиюкоторыетакжекакярлыким енеевсегоимеютсвязиссамымсобытиемкаждоедействиеихкажущеесяимпроизвольнымдлясамихсебявисторическомсмысленепроизвольноана ходитсявсвязисовсемходомисториииопределенопредвечноаа

Ключ: a = 425, b = 100

Висновок:

під час виконання даної лабораторної роботи ми написали автоматичний дешифратор афінної біграмної підстановки та ознайомилися зі способами побудови автоматичного розпізнавача мови.