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:

Христиченко Дмитро ФБ – 72

Нестеров Назар ФБ - 72

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).
шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм 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
щмжзвзгефхмафыяэюэрелфауимчмгембуйвецщкэмоцыэбьекзмафыяэбьшемхдшчюфтчймеацжзвзгефхм
афыяэюэрелфауимчмгелецшвимореиыфемэиоялшоуйфбяшмаокжыцзбкжжябсйцсвещтюсроауцезохюд
бркшомэршйаябйолрхэдаючетжжгтифдзтштгфычсведаетсчлехввамчглмоцтябмчжзвзгефхмаллэзиоаущ
тюсроаучмэзршоюжеоэщедаюцюеютвючавэыфдшгегшчэмэдэдамчвенеттючмочажсвершоюжеоэщечмг
ецехйызребэлхывмыгеузызталлэффшщшьэвемаэфлшщтсэиеабзеьаллжсвелешжфехййэезбйютяшлфнек
цршчмхвсйызвееосэткгйреткммвеуоцыэбьекзюсвершгеюкоюдбкзиэезнжцышоларемангмэяшбшашксй
йгшвозшашткшощсревкэбюсейчффыяэюэчкэбюсейчфокаагтсдвзбэхэвейюейюэббморенеозюбюсбрвеу
шйжфшьэаыфшойызмбибсйвйэффшщшвожкмчрещбдоуйюевебкэфлеишеьэщлэыфэфлшщшнеоюючял
феузхосйлхлецшвиффкшненрлечммэээиожкэщлэыфялфыфедаууййютциимайсмббщтюсрофгмэщтнвда
яферфанрршдедаважсимдэщбдоуйршюетруожсвечмдэшбяеимцщдшшдяэдашзццкэрзнэвччсфбсвьцавьц
ззюевеацмашоцыэбьечюдбмбуйвецщкэрзгшцйьоатчфцтсыэбчажкгзфлнэвдчаозглцтэенемхдшчюфтчйц
эхекэсшворбфжаышолаякркмщбфпжвэщшфаюаяекйвеларбвйчфуйезсмонрквеацкэайчфуэкзхэнэаыжсю
чофббнвдабэуаллжсвеншеьллоюнпмощмнрюэцщдшайатэлллокозтштгфыфцкэрзнэьтжжгтибфбовууочэ
бмоткаувчсймебймещлаюцтьэаэчмнэаюффйшсмвчсверкзшыаакчмеиоеэдагтжкэфршофгшушвосдщтчье
йледэамткьобрмыаакчгйршвзвшломоимцжатяфсчочшйгедйджцтцзцявдлечммэиыяэюэимялфыфшойыз
мбжщмйифршййюэббвчкчменэушдацшушбюэбеиючфцгбаюерючнрбэамткьояшщтюсровшбюэбеимом
чвдааитдфйшмйээбйщклраадшмхреужлалрщтюсроуэнээшьмстевщтюсрощтнвдаяферфанркзщеоэкзмец
ешыозцшщбффсчййчмчмысйвюеэщвроркэфэбхпимдэюебфзшзоюсвегосймэбйозиомойэплфеузхосйлхжй
оюзабряеоэкзмецегегосчмышонвуудабэвшмхредаййцеууашоцнздабрбйюдатэлвдледыяффэуыяэюэюыф

еыжцшдаййэфцтфэдиьшнрлечммэуаркаусшщтюсроаужзмейкжжкзюегшшойечфеймэбфсэцеайжзвзбэббгэааюзлхкзвзилцтэечйчфземхдшчюфтчймеиыфшойызмбтшмйдомчнпрбьояшфбройпрбьояшюшкфллынозбьхжткллокцыозэзюедажычайояфвеяэеомщббзпжцжюзшсшнэчмшоршвзжевшнээароуййцшюгэршвзжевшкюбвьцнеаэютуачучашйссимэкцыознэлехввакздаэбяккчмоьшцщдшэюдбоюдфцеаймшкзюегшшоуэцезоаоючллгечмчмлхйпрбжюаоцыэбьевоьеткгткэнйлафшаерзьэючаадажычафжяфййцрорфрбрбкздажыванфауткмчршчмгечмцезоаозшсшнэчмбйейцтлзйааоиыхпрбябмысйициэлхкзпагтюсццжййцшюсахпрфауимршщегбоюхюзарахпмоючллгечмчмлхцезоошсшнэчмршчмгероютгльогбйэровюдбоюыыяэбьйемхдшчюфтчймененюсофдарзсймеыюгшьэифябвкезгвфшровюдбоюшймчщвцтлзиоаумбуймэттсйхэйэршчмгечмлтьогцтйместрфэбмьйэмысйгшдерздивдоэеавагтдарзйэзыцтйэффлшневенемафыфеыжцшгелтьогцтйтцчтрфэбмьтщчаркюзгшвючжщвреаэогмэуыяэюэвоюсялшоючллгечмчмлхдаябоюзаеыяэюэимюаффлшдэшбшззвыыяэюэьйэфчзнэщблаллжсвечмщтсэюфеймэвемаоюдбсэббнвэфварбйошоюсвершчмгеййвбьсчарбйоаущтюсроаулечммэмзлечммэнвэбгооюдбсйэфцтфэлхнрвемхмеюевеацмазередеспречмгелецшвичавйевэбгохюдбвчфбнэшодбовууаафшщиййчемйцевдушгецшуштквдщцбйчфййцеялгтжжычуээарояфсйвецйвзчзюзецкэрзлхлшашюедесосдвееоаарксшжзюоеймемхмецшмепакчкожжывбфсйвежзкзвзчзсинэверыдбовууаюффлрлшашюедесосддшайчфбркзюегшшоуэябвкезгвозааббэфркаагтсдвзбэлшгежзвзгефхмаоюшйоюзаяшлецшвифбсйвэнэршлецшвифбсйяюдбчарксшузгещтсэюфэбйохкрксвуудабэвкчпденелехввацинвкшнедыкдщвюентвютщфбмышорюгтягвершщегбоюзавэкзушюевеацмащвервенемаоюдфэбдоцыэбьекзшзгшцйьоатваюдцщдшхейкаагтсджзвзгефхвзбэлшгелечммэвюдбуэшыэбршкзршоюжеоэщечмгеледыывмояшашксййгшвосдоюдайрвшмхдаюючжщвренеыжмевеммрйоюзаяшршщегбоюшйэфцтфэлхнрршоюжеоэщечмгемаоюсчфбнэшодбовууттакмдмевеммнюдбывуудабэвшмхкзэйфбуйэбюзщммеveммейютрбибффчжнэщтэфшзйамыжицэкздечмгемаоюоеьэлегбуйфбййвэшыэбьэлхюаофэбышоэьэеосдййэзчмыбовуужюдбмыяэцшдшимтгвеацашксййгшвосчменэушдацедйгегосдозщозеытжжимуыяэюэенваябыжпфййвеяэроеэпюйпмощбтеврэомобрршозоцлосдифгшьэоазшдараюдозоцлосйлхмевеммйчаоиышовчйшшсючаегшючшйызозючнрозоцлозеврэочаюгмэифгшьэифййвеяэчаючшоййызрешрмйеверкзэоцтжжычршеэршюетруоьшжздвзуушгецшьпффуащбэйвюаыэбфжшшмйэйцеаедеивердеданпмобрбфсэыбюсимцьрбууюсофдаэцуабйючсцбшдацедйцевчмазеучхпуалшфсуйюврбвавэнэршюврбвараркзшведшайчфяшрежзцймефешоюврбйшвшнеызявуудабэбгвелецшвиморерфыжцшдаимшчкчмочффшщшьэдаьоэфчанрршцеюфозмэсмдэдшэзуанрдедайрьэючййвеяэффмевефехеревчьшуоейцеаехозшцыфшдещтнврбморечжкзушьэьшдаквцшдагтшоэпыжьэюкчпдешсрбэфвкйпыжщхнэеолрмевеозлаючаегшейцеаехоисючаамбщсморшьшеэйацтейшэыэщовймэрэзолрферфлравщсрбэфвкршыжашгосэшыэбтруащтнвиэезвоошючхжркшонсрбэфвклещоварбйохпффуащбэйвюдосййцыэйюейлещоварбйосчгтлвяшмвердеданпмобрййвеяэушткводоюбшушгецшушткводэшгшайэфцткшвозуюедажыокршцеюфозмэдэдшайчфяшялсйэфчзюзифэффшщшьэочфбнэшомчсвуудабэивьцчэыбовууюейцнзуаййвеяэушткзшщоисмояшушпфыиейвечаушгецшюойеьяейчфморелбейуопьщсючтюэбеивчфбовьчяеьйшрвзйаючаемхкшмбуймэшовчьшуоывьцчэыбовуувшщеушбэхоьшщтнвфыфшдшгшвосйлхроеэпюйпредаякчпденеялфысйицекуйцтфьльетрфэфьцэшаеьхууцзюхейлхозкэдагтйэййвеяэлазшдаяюейлещоварбйолроюьзотзшрзбпыжщхушгецшушдарзбйщкаудэццведпыжьэцзфшгыэбфжшшмйеверлшвржзмеьцоэючщбэйцевдэшгшзоцыэбьевоейщеютдоважсвеючаюэбьшушбкллюзьэжцнхвшюшюхьлщвакжжябсйцсвеааршневзбэлшгефбровкркдысйгшхоючиэфхщшиэезгшацябвкезгвжожкллюзаегшвкрквшюшюхршюещбйпябвшлоеэпюйпимцжркшомчмевеммчжуйызмбибяшнедшайчфьрцеуофимойэлшвржзмшацжзвзгефхюебфзшацщтсэюфэблврбвакверояюбшнедшэзщбээдагтйэвемащвэбгооюдбсйэфцтфэлхнрцщоэвзчзюзщфглябййояфсйвеявервенемаоюфцкэрзлхатэлатэлуэюевзмеццледыывмобрщтюсроюецврбябййвймчййоюьщййэфчзнэсгмэдйоюзаяшташйссвчрбцэуыяэюэгверюаллщвбэсшьэээщбифауимакгтлжьоейоюцщдшьэвкшомэршйаябйоаухэдаючшэншеьллэбквможцшлткчусвбэсшьэрфауткдыьцхйтщщтнвщтролазшжзукжжябсййоцыэбьецццблаллааэбякжсвечмдедаглццлхцегтзпморенедэозфбгюэфвэщтффнсжзлтьогцтйменевчюшозвеозвфауршледыяфдзэйозшыэбхпмоящшнекзфеюзофгшушьэялозгвяещосйлхйыяэневембмочуьтуйжеымюещтглааэфгшьэжэюеютвюредаеыяэоюфшвшьэларквдомнелкаагтошчмокжыфбегмэозодщвшэщвфтузьэдияшюеушдаффатчждшршсвмыгеузмэушткяшюшфшнецемммевеммиыэфмлеркцлеттючмоьэмеююдбффнвмошйййитмоьэипрбьояшмвсймэсшьэхчьтуэмевеммуаэбякнцпжмбибййчмчэбгюяшвеаэатэлаудагтшошэдэшбяеимдэшбяерейвьцчэуыяэюэюыщвдшэздивднрюеоэщшцяьшлецшвичавйэйоюзаяшледыяффэрйьэбкллюзледтрбйрхбоксэчзюзуаааушнешофыывйшвеьаллэбюсведрневшуайжючгшаавененэмаджуйсдйшмйвшгпмочеьаллэбюсвесцфэмйэйэббьючмаааабпрбьшбсвецшвшнацрлшвшнеаавененэмасйвеняючофьэоцузмхюэтцжеушмйэйейлхялшоюсвершщтюсрояфлшюаааэбяксйэфчздшьэуаюдгйгебэгыяэмевеммрйэфцтдзуанрбйщкзшыэщомореьеш

льоюсеймееймэрэзозшлечммэеэвейюааьожкмевеммзовудшбсвещюгемечзюзуааавенемаокгшбсважзозю
бнлйшмйээвеацюедесозшжцдшьарксшщтяфчарксшршщтяфжзцэвеютвюмоокдайрлэлфьэоцмевеммайж
зсшбсвещюгемежыябзеьаллжсвеючыдаарбсйвйейлхялсэмазеучэбфбнроююакчызьпиыозбэршщтяфжцд
шьаааеасйжзсшбсвекзюегшшоюекшшфщеткэцюевеацмазенжмдаарбюаллсэаавенеюечэясвеябвкезгвсж
мдаарбялфыллжюрбжкркщтяфроиыозююлвуавейкветкчпуамаджяфябффдзэйифдэшбяеюылвэфюелкфы
ьокзцлгтпцчзэзаавенемафысйгшхочуозаеуожклветфбюехоьшюеббнвьэстжжцэыкьщбэдагтюсейцэрйою
забряарккзамрзючошцшнэцэрбовййсащркбхксвэщлэмоуэщшрерзьэайоюзатщмевеммуарксшжзоркбхкв
чмоьшбйялсэщшфабфпжййезсмдйоюзаяшбкчпденвуудабэеэнкчпуяьшнрвчщтсэюфэбйосчщбэймчвдлш
врбэдагтюсеймедйсмббмоиыфеыжцемхреьомдщвчанрбйшртэлебйючжededэдагтйэяещтнврбмофыфшщ
фщсрегз

Розшифрований текст:

понятночтощакивцредсщавлялосыделосовременникампонятночтонаполеонуказалосычтопричинойвой
ньбьлиинтригишнглиикакожиговорилэтонаостровесвеленьпонятночточленамшнглийскойпалатьказало
сычтдцричинойвойньбьловластолюбиенхцолюоначтдцричпуолыденбургскомуказалосычтдцричинойво
йньбьлосовершенноыцротивнегонасилиечтокйццамказалосычтопричинойвойньбьлаконтиненталынаяс
истемаразорявшаяеврдцучтостарьмсолдатамигенераламказалосычтоглавнойпричинойбьланеобходимо
стыупотребитыиэвделолегитимистамтоговремениточчтонеобходимобьловоссщановитыздюцломащамто
говремежиточтовсепроизошлоолтогочтосоюзроссиисавстриейвгодунебьлдосщаточноискусноскрьтотн
хцолюонаичтонеловкобьлнаписанзхцонятночтоэтиищебесчисленноебесконечноеколичествдцричинко
личествокоторьхзависитотбесчисленногоразличияточекзрежифцредсщавлялосысовременникамнодлян
аспотомковсозеыпающиэвовсемегообемегромадностысовершившегосясобытияивникающиэвегдцросто
йистрашньйсмьслпричиньэтипредставляютсянедостаточньмидлянаснепонятночтобьмиллионьлюдейхр
истианубивалиимучилидйугдйугапотомучтонхцолюонбьлвластолюбивалексшндртверщцолитикаангли
ихитраигерцоголыденбургскийобиженнелызфцонятыкакуюсвязыимеютэтиобстоятелыствассамьмфакт
омубийстваинасилифцочемувследствиетогочтогеыпогобижентьсячилюдейсдругогокраяеврдцьубивали
бразорялилюдейсмоленскойимосковскойгубержийибьлиубиваемьимидляназцотомковнеисториковнеув
леченньхпршпессомизьскшнияюцотомуснезатемненньмздравьмсмьсломсозерцающихсобьтиыцричинь
егдцредсщавляютсявнеисчислимомколичествечемболышемьуглубляемсявизьскшниепричинтемболыш
енамихоткрьваетсяивсякаяотделыновзятаяпричинаилицедьйрядпричинпредставляютсянамодинаковоз
цраведливьмисамюцосебеиодинаковоложньмипосвоейничтожностивсравнениисгромадностыюсобытия
иодинаковоложньмюцонедействителыностисвоейбезучастиявсехдругихсочцавшилцричигцропзвестисо
вершившюесясобытиетакойжепричинойкакотказнаполеонаотвестисвоивойсказавислуиотдатыназадгер
цогствоолыденбургскоыцредсщавляетсянамижелшниеилинежелшниепервогхфрачпузскогокхцралапос
тйцитынавторичнуюслужбуибоежелибьоннезахотелидтинаслужбуинезахотелбьдйугойитретийиться ячн
ьйкхцралисолдатнастолыкоменюелюдейбьлобьввойскенаполеонаивойньнемоглобьбьтыежелибьнхцол
юонноюскорбилсятребоважиемотстйцитызавислуиневелелнастйцатывойскамнебьлобьвойньноежелибь
всесержантьныцожелалюцоступитынавторичнуюслужбутожевойньнемоглобьбьтытоженемоглобьбьты
войньежелибьнебьлоинтригшнглиииинебьлобшцричпаолыденбургскогоичувстваоскочблежиявалександ
реинебьлобьсамодержавнойвластивроссиииинебьлобьфршнцузскойреволипиииюцоследовавшихдиктато
рстваиивцерииивсеготогочтдцропзвелофршнцузскуюреволипиюитакдалеебезоднойизэтилцричинничег
онемоглобьбьтысталобьтрцричиньэтивсемиллиардшцричижсовпалидлятогочтобьпроизвеститочтобьло
исследователыноничтонебьлоисклцчителыной причинойсобытияасобытиедолжнобьлосовершитысятолык
опотомучтоонодолжнобьлосовершитысядолжньбьлимиллионьлюдейотрекшисыотсвоихчеловеческихч
увствисвоегоразымаидтинавостоксзападаиубиватысебеподобньхточнотакжекакнесколыковековтомуна
ззdсвостоканазападшлитобцьлюдейубиваясебеподобньхдействиянаполеонаиалександраотсловакоторь
хзависелоказалосычтобьсобытиесовершилосыилинесовершилосыбьлитакжемалопроизволынькакидейс
твиекаждогосолдаташедшегочцоходпожребиюилюцонаборуэтонемоглобьтыиначепотомучтодлятогочт
обьволянхцолюонаиалексшндратехлюдейоткоторьхказалосызависелособытиебьлаизцолненанеобходим
обьлосочцздениебесчисленньхобстоятелыствбезодногопзкоторьхсобытиенемоглобьсовершитысянеобх

одимобылочтобьмиллионьлюдейврукахкоторьхбьлздействителынаясилаолдаткоторьестреляливезлип
ровиантюцушкинадобылочтобьожисогласилисыизцолжитыэтуволеедижичньхислабьэлюдейибьлюцрив
еденькэтомубесчисленньмколичествомсложньхразнооиразньлцричинфаталпзмвисториинеизбежендляо
бяснениянеразумньхявлежийтоестытехразумностыкоторьхмьныцонимаемчемболеемьсщараемсяразум
нообяснитыэтиявлежиявисториитемонисщановятсядлянаснеразымнееинепонятнюекаждьйчеловегживе
тдлясебфцолызуетсясвободойдлядостиженияисвоиэличньапелейичувствуетвсемсуществомсвоимчтоонм
ожетсейчасделатыилинесделатытакоетодействиенокакскороонсделаетегощакдействиеэтосовершенно
евпзвестньймоментвремежистшновитсяневозвратимьмиделаетсядостояжиемисториивкоторойоноимюе
тнесвободноехцредопределенноезначежиюестыдвестороньжпживкаждомчеловекежпзныличнаякотор
аятемболеесвободначемотвлеченнеюееинтересьинизныстихийнаяроеваягдечеловекнепзбежноизцолняе
тпредписанньеемузаконьчеловексознателыноживетдлясебянослунитбессознателыньморудиемдлядости
жениияисторическихобщечеловеческихцелейсовершенньйпостйцокневозвратимидействиеегосовпадаяв
овремежисмиллионамидействийдйугиэлюдейполучаетисторическоезначениечемвгшестоитчеловекнао
щщественнойлестнтпечемсболышимилюдумиожсвязантемболышевластионимюетнздйугиэлюдейтемо
чевиднюепреддцределенностыинеизбежностыкаждогоегдцоступкасеропппаревовйуцебояыейцарыесты
рабисторииисториятоестыбессознателынаяобтаяроеваяжпзнычеловечествавсякойминутойжпзжицарея
цолызуетсядлясебякакойудиемдлясвоихцелейнхцолюоннесмотрянаточтоемуболюечемкогдажибудыте
перыыгодуказалосычтоотнегозависелоилинекакчцоследнемписымеписалемуалександрникогдаболеека
ктеперынеподлежалтемнеизбежньмзаконамкоторьезасщавлялиегодействмявотношениисебякакемуказа
лосыпосвоемупроизволуделатыдляобщегоделадляисторииточтодолжнобылосовершитысялюдизападад
вигалисынавостокдлятогочтобьубиватыдругдругаипозаконусочцзденияпричинподделалисысамисобзю
исовпалисэтимсобытиемтьсячимелкилцричиндляэтогодвижежияидлявойньукорьзшнесоблюдежиеконт
иненталынойсистемьигеыпоголыденбургскийидвижежиевойскчцйуссиюпредпринятоекакказалосынхц
олюонудлятоготолыкочтобьдостигнутывооруженногомираилюбовыипривьчкафршнцузскогоимперато
раквойнесочцавшаясразцоложениемегонародаувлечежиеграндиозностыуцриготовлениибрасхольпопри
готовлежиюипотребнострцриобретежиятакихвьгодкоторьебьокйцилиэтирасходьиодурмажившиепочес
тивдрезденеидюцломатическиепереговорькоторьыцовзглядусовременжиковбьливеденьсискренжимже
лшниемдостижежиямбраикоторьетолыкоуязвлялисамолюбиетойидругойстороньимиллионьмиллионов
дйугилцричигцодделавшихсяподимеющюесовершитысясобытиесочцавшихсжимкогдасозрелояблокоип
адаетотчегоондцздаетолтоголичтотяготееткземлеоттоголичтозасьхаетстерженыолтоголичтосушитсясо
лчпемчтотяжелюетчтоветертрясетегооттоголичтостоящемувжизумалычикухочетсясестыегоничтонепр
ичинавсеэтотолыкосовпадежиетехусловияцрикоторьхсовершаетсявсякоенизненноюоргшническоестих
ийноесобытиеитотботшниккоторьйнайдетчтояблокопадаетоттогочтоклетчаткаразлагаетсяитомуподобн
оебуделтакжеправитакженеправкакитотребенокстоящийвжизукоторьйскажетчтояблокойцалоолтогочт
оемыхотелосысестыегоичтоонмолилсяобэтомщагжыцравинеправбуделтоткгоскажетчтонаполеонпоше
лвмосквупотомучтоонзахотелэтогоиоттогопогибчтоалександрзахотелегдцогибеликакправиныцравбуде
ттоткгоскажетчтозавалившаясявмиллиогцудовподкдцшннаягораупалаоттогочтдцоследнийработникуд
арилподнюепоследжийразкичкзювисторическихсобытияхтакназьваемьевеликиелюдисутыярлькидающ
иенаименоважийсобытиюкоторьетакжекакярлькименюевсегоимеютсвязиссамьмсобытиемкаждоедейств
иеихкажущюесяимпроизволыньмдлясамихсебявисторическомсмьсленыцропзволыношнаходитсявсвяз
исовсемходомисторииопределендцредвечноаа

КЛЮЧ: (425, 100) – (нц, зг)

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.

Програмний код

```
import math
from collections import Counter
import random

my_text = open("lab_3_text.txt", "r+", encoding='utf-8')
text_one = my_text.read()
my_text.close()

def reverse_element(a, b):
    x, xx, y, yy = 1, 0, 0, 1
    while b:
        q = a // b
        a, b = b, a % b
        x, xx = xx, x - xx * q
        y, yy = yy, y - yy * q
    return x

def solution(a, b, n):
    result = 0
    if a > n:
        less = n
    else:
        less = a
    for i in range(1, less + 1):
```

```
        if (a % i == 0) and (n % i == 0):
            d = i
            if d == 1:
                result = (reverse_element(a, n) * b) % n
                return result
            elif b % d != 0:
                print("The equation does not have an answer!")
                return None
            else:
                number = reverse_element(a / d, n / d) * b / d
                result = [((number + i * n) % n) for i in range(0, d)]
                return result

def coincidence(text):
    n = 0
    result = 0
    count = Counter()
    value = 0
    array = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
    for i in text:
        if i in "абвгдеёжзийклмнопрстуфхцчшщъыьэюя":
            n += 1
        else:
            n = n
    for i in text:
        for j in array:
            if i == j:
                count[i] += 1
    for i in range(len(count)):
        value += (count[list(count)[i]] * (count[list(count)[i]] - 1))
        result = value / (n * (n - 1))
    return result

def bigram_sequence(text):
dictionary = {}
array = "абвгдежзийклмнопрстуфхцчшщыьэюя"
common = 0
count = Counter("")
number_one = 0
number_two = 0
for i in array:
for j in array:
                dictionary[i + j] = 0
for i in range(0, len(text) - 1, 2):
dictionary[text[i] + text[i + 1]] += 1
print("You may see the numbers of bigrams below!")
common_ciphered = Counter(dictionary).most_common(5)
common_plain = ["ст", "но", "то", "на", "ен"]
print("Numbers for the ciphered text!")
for i in range(len(common_ciphered)):
number_one = array.index(common_ciphered[i][0][0]) * 31 + array.index(common_ciphered[i][0][1])
print(number_one)
print("----------------------------")
print("Numbers for the plain text!")
for i in range(len(common_plain)):
number_two = array.index(common_plain[i][0]) * 31 + array.index(common_plain[i][1])
print(number_two)
print(common_ciphered)

bigram_sequence(text_one)

def cipher_attack(text):
numbers_cipher = [67, 124, 869, 98, 377]
numbers_plain = [545, 417, 572, 403, 168]
keys = []
n = 0
decipher = ""
array = "абвгдежзийклмнопрстуфхцчшщыьэюя"
text_new = ""
```

```
for i in range(0, len(text), 2):
y1 = random.choices(numbers_cipher, k = 1)
y2 = random.choices(numbers_cipher, k = 1)
x1 = random.choices(numbers_plain, k = 1)
x2 = random.choices(numbers_plain, k = 1)
result = solution(x1[0] - x2[0], y1[0] - y2[0], 961)
if result == None:
        return cipher_attack(text_one)
b = ((y1[0] - result * x1[0]) % 961)
keys = (result, b)
for j in range(0, len(text), 2):
        new_text = text[j:j + 2]
        number = array.index(new_text[0]) * 31 + array.index(new_text[1])
        number_plain = (reverse_element(keys[0], 961) * (number - keys[1])) % 961
        bi_second = number_plain % 31
        bi_first = (number_plain - bi_second) // 31
        text_new = array[int(bi_first)] + array[int(bi_second)]
        decipher += text_new
if (0.0553 - coincidence(decipher)) < 0.01 and keys[0] != 0 and keys != (536, 91):
        print(keys)
        print(decipher)
        break
else:
        return cipher_attack(text_one)

cipher_attack(text_one)
```