Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

з дисципліни

«Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Виконав:

студент 3 курсу ФТІ

групи ФБ-74

Сизов Ігор

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

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) ,(b a 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 14

эпцббжпихюыббдьэбшясдбжшозшюбьпжожцюфтдбчюнхпжиавозосдбжпихюмжбдьэбшясшсмгыфлсыжеаепиатпожчдсд
мыбцэызпцтфдякейятгкпяэдфдзодосдщзяакыдытжпифдеолыфтэпшткгыфэяыфгшедзоякэпрдпьнжякапгкэшпхйдззобуолт
льяквыэпейшрхыщжшгвыейбхшшчжльйегжчжэхйдпцвпцтфдшхйдейудйшясшшозятлсойщозпшсщоьхшшщовтцтэлпфшсм
жгтцбазшсыжстйывдчжкалшозцббкжбиоьыщоюспсэппшоклюгждоиттмоыышмдяюейпжныгкяяныкжхюкгизшймыеыссб
жедеойдеткгэяойймякдоккщозпчюлюипгюозфщыжнгмкчюобыултшшозмжныяяыбнэчдпьнжякиььофдудоцдшойзоцзуфк
кщозптмыдхзжбцтфдедуооыфдякйдцтнэеощзыбкзщзяыюсыфякудгсмдцьыдмыжйсдифвэгсмдуооышкяянышынсзйыбэфе
рлтхюкгждвдюьцддоныпхвывдйдякйдцтнэсфщхшсйхршфьыжадмдхцщыаффпзмщздбгучжгтшшеыщжшгвызйятыбцжфйо
бмкфджбышмдсбязшсдбщзяыюсыфякщжлщтшчднкысфоякфдяклщэоыжвдпижошозятгсбжедеобжчжныэбязрдижлхввп
сцжмдадсдьыйдудедцюлхизэогсмдцьыдвщчждкйдвоухйжпыройжшкшсщоюсбкгжщжльаыбдозгшчжэттзыффдедбдьэбш
ясрдцьзпшсйпшшщеышясцтбцяхыфржсщадфдьышыякщобцьрфпдбиаржстшрэдеопифдедцдбдзочгыфрсоййдлхвыопейб
кфпштшсщоьочдэзгсыжныашцдудцтбцчьйдвтжбхзрйкпокфкрйеоэытжпифдедлтльяквыэпшткгизшймыеыпхйдейрукыейй
жыжныссцюфтдбцвышадбшозшюбьпжщжшгвысфтппхйдпцвпцтфдякпсеолыфтэпштдбцдбдэжякщобцрсфпцвйпгшэшчгы
фтфцхвыопейбкфпштяыйбцтйпгшгыякюьдказгшобрмщзпцвпцтфдякпсадмдйдгфтпэбыултшшозмжнычыйжэоюпиащовдз
юнхыфеэвошицдщыьыуфшсбжакнхбюшйфкфпуятзлютжвыаьскщжшгвыиюлюээзфыжщоюсбкмжлтльяквыэпштцоззтзфдм
гшштфтзякудэзшймышцхшфпэшшыщяойймякудзгвовтмжйжякшшпжпыккщозптмщжшгкзхюрмлтльяквыейятыбцжкбыулт
шшозмжныцтлюккизмжщзуяыфбклэбютпшсэпшсрмщзыфшюлыхынсгурйятгкпядхйдпцвпцтфдяклтящбьккщозпыхвыбдп
ыяшпхвыйжчтшсбжедцюлхизэоякщобцфдйжпювобьщощзяыюсыфыбпяейэжкыбсышибыуязбюйыыдякгсвэмкчдорцтроч
ффтдбцтмпфказцбязшсрмуооыфдякйдбкфпштрмщзыфшюлыпсцтззнэлхррнокыдыюьмклэспгсбцгддзшйдбеощзяыюсыфя
кщжгсмдцьыдифейфпштпягдмдйджшэопюшсчднкэпштпянхвоиьэыьющофддхйдейудзэяшгклюажтжчжпдгтяжшжшкхцяз
шйкыттяжээфякдонсзйпсьыщзбыхжвыэтяжршозрмякдоотыбипгюозиаизтфшсятгжхыйбкзбкфпштяжщзяаиззтящтшчднкк
кщзгсвэмклэвдчжшхйдльирхыщжшгкзхюкгдбыултшшозмжнынтйывдчжгююьжтцбшжшкйдезшймыеыэбыултшшозмжны
пэапежяшбатфбхтуфйэжшиацмьхюцжяшпхавеыккщзыфшюлыэдозгшкывзохбцьышжшкщоьыуооыфдякйдцтнэссвэсклээо
цчэфржюфкапжшжзшгютухжзжьстзеокжчтюлйжэожьнгэлщзуяыфбклэбютпяыйфршознопифдедщзяыюсыфякдофтбхпжй
шэоапцтлююьжтцбчюдбыыеоэоьыифмтеьбстзруидафбыьырютптршхйдейудйшясиашйязджяшссвдпихдбштжюжныеощз
псойфдхшызржыбчднкязджяшсслэажчжщтбэюьзошшфдвтбэфоякеюбюпьйемгшшуьспчывдчжшхтпшслтуюбюлочжюыюь
йегжйжэоюпэгвовтгмчдякгсаытшозятыалсьжедыдщжяшадедыдхйгсесмкфдмбфпжьнгхыацыдшычьйдвтжбщоюсбкнэацэ

жвэмклээплблтгждопхйдпцвпцтфдякгылхтптйюлчощююьжтяжьоиозцвдтшбкшсвзохыжшугжьоудгцжстзиофдтжымжжэот
отишосльыныысгмщзбюфкацмьхюцжяшсшгютухжзжьстзхюыбадеалтфкдбчдщзяыюсыфякиьнхккпжопцтэлэплблтгжацщы
аффпзмеолькьеобжчжныссцтззнэьоныуомкыффдейюжьспяйжяксбязрйеоэытжпиеошвгшкиакуяейэжкызыщзбюфкбхшш
бьиомкеоцюлхизмдйтшсбцшхпжзхвыгкнэщыьыкжхюрмщздбгучжгтшшеыеоукяяыбцвышшыгюдбдпгюзцжшшйсосдеаыут
жйпцтлтдойдьжпьнжякиьскщзяыюсыфякдодпгшкбгшуыуышкмкцвышшыябфккзносдсблткзэпштпятфиапжныодйтшсфдцт
бхщоапцтгжлхррнокыьолыпсцтззхыкяыбцвышадяхйдпцвпцтныякпсйхршмпгютзякжшпжйшясьоаышцщоякцтзмнхтпднта
выромдифвэуящзяыюсыфякдошшфдвтяжаозбшрысеыкжхюгжщзэфщзнэеыхялтяынылжэжфтвыеккздеэфшсмжгтяжщвпш
жьдоитпяккщозптмйжофмттзыффдбшюжлыэпейшрхыщжшгвыэдытшшгклэчжаюбэнхшеысбэщздбгучжгтшшкиеонысхвы
бдпыяшядадсддосдудяхйдльирхыяатпожкжлйятгкпячдакыбчдроьотжвэхшозятрдюжпжкомкшшэопибцмгшштфтзякдоуд
якавфдфжхзцхлсадмдхцыслсойбклэбютпцхтпшслтзщтшчднкязджгдэщеыьыккщозпэбнхйдльирхытжухызшшэофгщочткгц
хйдейудйшясгсщжшгвыпсюжвыыфегыфшсоцкыыфныьыейлопцуслшбюуясбязрйящеыхшмдлпчююьжтяжрорыэосдапэчцт
нэжшфпэшадяяойймякудыдафятгжгпнтмгшшшспжйжгтрмуотжвыэпштккяяныкжхюрмточцоыйдадысыжшзцтгжкяойймяк
щжгтюлщзлюеыфьеочвфдтжптцвышшыхфшшеыажныратпфумжщоюсбкгжчджьэыкыжшысойгдитяжщжшиуоэжбшщжгтя
жпдзбцбфккзнопифдедякыбкпязшсятнэикфттзуфршацыдшычьйдвтжбизхонылддогтшшеылхшшиаякуддосдоцякйдчьйдя
кохйдейудйшясгсбккгрйбхкзэдняедцдудаижббжпихюэяойймякщжгтрмщзыфшюлысьйсяыдшпощзыфшюлынхшеысрмщз
дбгучжгтшшеырсфпцвйплэвдпиьжкжхсщожюэызпршщеышясцтбцбдыдижгтшштжзыыффдхзжбцтфддоитпяаодкизшспые
оьыкжхюкгизшймыеыссцтззхыккфдуыяшяднгятцвышадысмпзвцтгжжшпштжчьфгщочткгцхйдейудйшясэпцвбцсхыфыдртп
ябдьэбшясэзэфпшщеышясцтбцбдыдижгтшштжбсцтлжьшадэщадфдьышызпэфджмдкбмкбкэслшбююлякшхцтржэьфоякнэ
сбячльеойдетдбщоаффпцтхыозтфрдаижбвттуыжткизедаппшшшэоапежэхавеычдэзгсыжныашмдыбшшеыдосдудедеолы
фтэпфткгцхйдльдкятящтшчднкчдякохцжясээфыжгдадсдацмьхюцжгдяхйдльирхычкдбэызпкатпожкжхсэжлэеывзохыжшу
уяккщозпхяакефтпсшшшэоапежяшацьждклюыбккщозпэбккфдлэяшссфоякфдякноссльыныысбэщздбгучжгтшшкиаозбшры
сеырощзяаизшшозмжнышхйдейудйшясцочкиаршшсиарсерфпгмщэзхыфккщозптмбжпихюкгэяойймякдонхшеысрмщздбг
учжгтшшеычдроьотжкыудапввцтфдякпсуыякжбьбязшспяцюфтдбцвышшыушдэсжзыцюлхизытрмизгжшкшрхырсцтззхыац
ьжкжчьшшэопибцусшшмдттмжхзцхтмхюуяякщонывдпиоызшясшйбхеффдысйдюжбшшыегшштфтзякчкшсщтквбкфпштрм
якшхцтэдаисшеэмклэлхрргнчюрмщоюсбкнэеойдеткгэяойймякдоккфдуытжпифдраэффдякклчдчжщтцбхыхюцхцжпцыыжй
шшкиасйьозцтыжедхцпюгсчдзпэфыжыспжуэцхпжэжвэйетмтжйфцтлытмщоюсбкнэцюфтдбчюпсцтззхыссвэмклэзопиыжш
убэлттжзшгнчюшрнэвттуыжмднгшспяпсыждтцщадфдьыкжхюуянсзйтмлюеывтмжчвгшеыысысйдюжбшшыщышкмгщолы
фтбц

Найчастіші 5 біграмм тексту

аж 54

цп 50

шы 49

ки 43

тя 41

Складності в реалізації

Фільтрування тексту відбувалося за допомогою заборонених біграмм:

"аь", "иь", "ыь", "йь", "оь", "уь", "еь", "эь", "яь", "ьь", "юь"

Але не усі тексти мали ці біграмми. Й на виході залишався не один текст, а декілька

Розшифрований текст

Key A = 10, Key B = 52

“ст” в “цп”; “ен” в “шы”

вскорепослесвоегоприемавбратствомасоновпьерсполнымнаписаннымимдлясебяруководствомотомчтоондолженбылде
латьвсвоихименияхуехалвкиевскуюгуберниюгденаходиласьбольшаячастьегокрестьянприехаввкиевпьервызвалвглавную
конторувсехуправляющихиобяснилимсвоинамеренияижеланияонсказалимчтонемедленнобудутпринятымерыдлясовер
шенногоосвобождениякрестьяноткрепостнойзависимостичтодотехпоркрестьяненедолжныбытьотягчаемыработойчтоже
нщиныдетьминедолжныпосылатьсянаработычтокрестьянамдолжнабытьоказываемапомощьчтонаказаниядолжныбыть
употребляемыувещательныеанетелесныечтовкаждомимениидолжныбытьучрежденыбольницыприютыишколынекотор
ыеуправляющиетутбылиполуграмотныеэкономыслушалииспуганнопредполагаясмыслречивтомчтомолодойграфнедов

оленихуправлениемиутайкойденегдругиепослепервогостраханаходилизабавнымшепелявеньепьераиновыенеслыханны еимисловатретьинаходилипростоудовольствиепослушатькакговоритбаринчетвертыесамыеумныевтомчислеиглавноупр авляющийпонялиизэтойречитокакимобразомнадообходитьсясбариномдлядостижениясвоихцелейглавноуправляющий выразилбольшоесочувствиенамерениямпьеранозаметилчтокромеэтихпреобразованийнеобходимобыловообщезанятьс яделамикоторыебыливдурномсостоянииинесмотрянаогромноебогатствографабезухогостехпоркакпьерполучилегоиполуч алкакговорилитысячгодовогодоходаончувствовалсебягораздоменеебогатымчемкогдаонполучалсвоитьтысячотпокойног ографавобщихчертахонсмутночувствовалследующийбюджетвсоветплатилосьоколотитысячповсемименияхмоколотитыся чстоилосодержаниеподмосковнойморковскогодомаикняжоноколотитысячвыходилонапенсиистолькоженабогоугодные заведенияграфиненапрожитьепосылалосьтысячпроцентовплатилосьзадолгиоколотитысячпостройканачатойцерквистои лаэтидвагодаоколотитысячостальноеоколотатысячрасходилосьонсамнезналкакипочтикаждыйгодонпринужденбылзани матькрометогокаждыйгодглавноуправляющийписалтоопожарахтоонеурожаяхтоонеобходимостиперестроекфабрикизав одовитакпервоеделопредставившеесяпьерубылотоккоторомуонменеевсегоимелспособностиисклонностизанятиеделам ипьерсглавноуправляющимкаждыйденьзанималсяноончувствовалчтозанятияегонинашагнеподвигалиделаончувствовал чтоегозанятияпроисходятнезависимоотделачтоонинецепляютзаделоинезаставляютегодвигатьсясоднойстороныглавноу правляющийвыставлялделавсамомдурномсветепоказываяпьерунеобходимостьуплачиватьдолгиипредприниматьновые работысиламикрепостныхмужиковначтопьернесоглашалсясдругойстороныпьертребовалприступлениякделуосвобожде нияначтоуправляющийвыставлялнеобходимостьпреждеуплатитьдолгопекунскогосоветаипотомуневозможностьбыстрог оисполненияуправляющийнеговорилчтоэтосовершенноневозможноонпредлагалдлядостиженияэтойцелипродажулесов костромскойгубернииипродажуземельнизовыхикрымскогоименьяновсеэтиоперациивречахуправляющегосвязывалисьст акоюсложностьюпроцессовснятиязапрещенийистребованийразрешенийитпчтопьертерялсяитолькоговорилемудадатаки сделайтепьернеимелтойпрактическойцепкостикотораябыдалаемувозможностьнепосредственновзятьсязаделоипотому оннелюбилегоитолькостаралсяпритворитьсяпередуправляющимчтоонзанятделомуправляющийжестаралсяпритворитьс япередграфомчтоонсчитаетэтизанятиявесьмаполезнымидляхозяинаидлясебястеснительнымивбольшомгороденашлись знакомыенезнакомыепоспешилипознакомитьсяирадушноприветствоваливновьприехавшегобогачасамогобольшоговла дельцагубернииискушенияпоотношениюглавнойслабостипьератойвкоторойонпризналсявовремяприемавложутожебыл итаксильнычтопьернемогвоздержатьсяотнихопятьцелыеднинеделимесяцыжизнипьерапроходилитакжеозабоченноизан ятомеждувечерамиобедамизавтракамибаламинедаваяемувремениопомнитьсякакивпетербургевместоновойжизникото руюнадеялсяповестипьеронжилвстоюжепрежнейжизньютольковдругойобстановкеизтрехназначенийсонствапьерсоз навалчтооннеисполнялтогокоторыепредписывалокаждомумасонубытьобразцомнравственнойжизниииземидобродете лейсовершеннонеимелвсебедвухдобронравияилюбвиксмертионутешалсебятемчтозатоонисполнялдругоеназначениеис правлениеродачеловеческогоиимелдругиедобродетелилюбовьклближнемуивособенностищедростьвеснойгодапьерреш илсяехатьназадвпетербургподорогеназадоннамеревалсяобехатьвсесвоиименьяиличноудостовериться явтомчтосделанои зтогочтоимпредписаноивкакомположенииинаходитсятеперьтотнародкоторыйвверенемубогомикоторыйонстремилсяобл агодетельствоватьглавноуправляющийсчитавшийвсезатеимолодогографапочтибезумствомневыгодойдлясебядлянегодл якрестьянсделалуступкипродолжаяделоосвобожденияпредставлятьневозможнымонраспорядилсяпостройкойвовсехим енияхбольшихзданийшколбольницприютовдляприездабаринавездеприготовилвстречинепышноторжественныекотор ыеонзналнепонравятсяпьеруноименнотакиерелигиозноблагодарственныесобразамиихлебомсольюименнотакиекоторы екаконпонималбаринадолжныбылиподействоватьнаграфаиобманутьегоюжнаявеснапокойноебыстроепутешествиеввен скойколяскеиуединениедорогирадостнодействовалинапьераименьявкоторыхоннебывалещебылиодноживописнеедруг огонародвездепредставлялсяблагоденствующимитрогательноблагодарнымзасделанныеемублагодеяниявездебыливстр ечикоторыехотяиприводиливсмущениепьерановглубинедушиеговызывалирадостноечувствоводномместемужикиподно силиемухлебсольиобразпетраипавлаипросилипозволениявчестьегоангелапетраипавлавзнаклюбвииблагодарностизасде ланныеимблагодеяниявоздвигнутьнасвойсчетновыйприделвцерквивдругомместееговстретилиженщинысгруднымидеть миблагодаряегозаизбавлениеоттяжелыхработвтретьемименьиеговстречалсвященникскрестомокруженныйдетьмикотор ыхонпомилостямграфаобучалграмотеирелигиивовсехименияхпьервиделсвоимиглазамипоодномуплануводвигавшиеся ивоздвигнутыеужекаменныезданиябольницшколбогаделенкоторыедолжныбылибытьвскоромвремениоткрытывездепь ервиделотчетыуправляющихобарщинскихработахуменьшенныхпротивпрежнегоислышалзатотрогательныеблагодарени ядепутацийкрестьянвсинихкафтанахпьертольконезналтогочтотамгдеемуподносилихлебсольистроилиприделпетраипавл абылоторговоеселоиярмаркавпетровденьчтоприделужестроилсядавнобогачамимужикамиселатемикоторыеявилиськне муачтодевятьдесятыхмужиковэтогоселабыливеличайшемразорениионнезналчтовследствиетогочтопересталипоегопри казупосылатьребятницженщинсгруднымидетьминабарщинуэтисамыеребятницытемтруднейшуюработунеслинасвоейпо ловинеоннезналчтосвященниквстретившийегоскрестомотягощалмужиковсвоимипоборамииичтособранныекнемуученик исослезамибылиотдаваемыемуизабольшиеденьгибылиоткупаемыродителямионнезналчтокаменныепоплануздания воздвигалисьсвоимирабочимииувеличилибарщинукрестьянуменьшеннуютольконабумагеоннезналчтотамгдеуправляющий указывалемупокнигенауменьшениепоеговолеоброканаоднутретьбыланаполовинуприбавленабарщиннаяповинностьип отомупьербылвосхищенсвоимпутешествиемпоименьямивполневозвратилсяктомуфилантропическомунастроениювкото ромонвыехализпетербургаиписалвосторженныеписьмасвоемунаставникубратукаконназывалвеликогомастеракаклегкок акмалоусилиянужночтобысделатьтакмногодобрадумалпьерикакмаломыобэтомзаботимся

Висновок.

Набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанував прийоми роботи в модулярній арифметиці.