МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

з дисципліни

Криптографія

З теми: «Криптоаналіз афінної біграмної підстановки»

Виконав студент
групи ФБ-91
Братунець Дмитро

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 2

Найчастіші біграми шифртексту 02.txt

```
['рщ', 'юд', 'чш', 'юа', 'йа']
```

Шифрований текст:

рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюоэдсецч
тыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпр
бкажлащваэщюемечшщипнипнучбусхекайаэкяуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуы
уйацднфзхащаукйнхжукчщысаэарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаю
йзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщбероюазанхзушщимзс
бючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфуыуйацдаюваллйыачларщзщ
роюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпз
лиекдкглаедюднфэщйдшгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюд
ушлсбубеюыхрдщндщфщейерйсдкммьофкаюйажйаидхйьнхершхлкшьсжуиеишбпымюенпчщроюаеймюберо
юарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйюенщлуч
ихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкен
лхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшы
швамносвиййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчты
кйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценав
сачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешбероюачпщы
лшыщдшэасуйаьпымкуюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьй
ацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричикзддрятаршроюазахачшфщчшурпрбу
ашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфи
кайаэкишныцмбээелучылшрщашошзсбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюберояарптыл
шцюцрчийщпаюеющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюезлиекдф
фыршдчимшлчлэфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйющешхщнкшлную
сэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшсосгпэпщепщчшфихехщюе
дшэпеемучщройкэысарепуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллир
мффаыпмяызшщфзсййымзсхажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплах
щдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюдбучихеэ
дэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэшсающуонафщгшмейррих
ушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшцшмейряжпшюешпщьбудшоылшищгамуыщюа
ешлуьппрринхдщцадуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчуш

угрйхпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщ
щчшмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьчмб
юдпаюехдхвамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкду
сосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюга
рпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикммьлевлщднхбмнхшсзмгь
хпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйкаю
щамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаю
ьичбзлцчтыкйэщыштыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйац
чтыкйдшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушцькышзшв
ыйафщцышхпцмдрщыыуюехакчщуиезафнщцыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсд
фмчзьчжлаыпмяызшжхбмнхшсбужичлщерпюабуашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчола
мчэичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпреш
хнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяавдчишхтаичшзыйыуйау
сйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщьбукаюдуыдщимюдкечушгмщрща
шщппрэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщцтвкчисжлзсйепртшййыуйау
сйрпншдажйазмгьусффщлщрбезахемчтэлекмаюрщудеапамдосшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщ
ыхубвчочпщаэщялчохехалюидвиаммсееапегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдк
йчбйкишугрййкоыдднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрйщ
ызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрмфукукчщгчилиачгшзсечмбрмфуэ
снарпзючшпмвпфчбшмейрпныурщгпзхцмчэиорщэаэшшщрщхезакдььрмьрпнхщшдькюедефщроошкаюрпркд
чэуырщлхчээпмеидбюхахщимюдюарппьщсрплаэщкаюытэтедщпуэщвкющциулаэиыйхллланажахоусиппрсеэщ
юхыййаькэиеыйееуйафмыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюахйщ
фрпешбероюарущефпкезарчцптддчшфдщпуэщвкющньйашегахлтейицмрйыезаокнейежпэиэщгэхувлуоыуыщ
имфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчитысазшйыжжйажлчпнхыезахаэасачшашйарока
мейецыьпяйхеейыуйаусйрнфйщхлюеерффасхйюдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущеф
птачштэрщзщяпэптбьерпимюдкеслщещцримежагекаюрэпьчяфьеруюсхпымздюлщелшашфьымосьрчифшцк
щедеюакайасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюадуклзщачисюаре
хеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифусицлщеомхпипчушгмщрща
шгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфшроошэщнхльюаэпеямшщевлэияффубелшщфцчтыкйхр
мсуювпьюыщдшварчмэчиащварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

Розшифрований текст:

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноепри
падкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизниприводящегоктяж
комусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойсилыослабляясьдократкихсос
тоянийабсансадобыстропроходящихголовокруженийимогуттакжесменятьсякраткимипериодамико
гдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообусла
вливаясьвобщемкакбыстранноэтониказалосьчистотелеснымипричинамиэтисостояниямогутпервон
ачальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимост
иотдушевныхволненийкакнихарактернодляогромногобольшинствослучаевинтеллектуальноесниже
ниеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеяте
льностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныилиподле
жатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечат
лениетупостинедоразвитоститаккакэтаболезньчастосопряженасярковыраженнымидиотизмомикру
пнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезнин
оэтиприпадкисовсемисвоимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвит
иемискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюне
удивительночтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффект
аэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональ
ногопониманиякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовл
енорганическимеханизмкоторыйиспользуетсяприналичииивесьмаразныхусловийкакпринарушении
мозговойдеятельностипритяжкомзаболеванииткапейилитоксическомзаболеваниитакипринедостат
очномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделен
иемнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпо

зывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедр
евнейшиевračиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациювысв
обожденияэпилептическогоотводараздраженияэпилептическаяреакциякаковымименемможноназва
тьвсеэтовместевзятоенесомненнотакжепоступаетивраспоряжениеневрозасущностькотороговтомчт
обыликвидироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихически
эпилептическийприпадокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидоизмен
яетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессатакимобразомм
ыполнымправомразличаеморганическуюиаффективнуюэпилепсиюпрактическоезначениеэтогосле
дующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедуш
евнаяжизньподверженанарушениюизвневоторомслучаенарушениеявляетсявыражениемсамойдуш
евнойжизнивесьмавероятночтоэпилепсиядостоевскогоотноситсяковторомувидуточнодоказатьэтон
ельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодушевнойжизниначалоприпадк
овипоследующиевидоизмененияэтихприпадковадляэтогоунаснедостаточноданныхописаниясамих
припадковничегонедаютсведенияосоотношенияхмеждуприпадкамииипереживанияминеполныичаст
опротиворечивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевдетствечт
оонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотрясшегоегопереживани
янавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылобывесьмауместноеслибы
оправдалосьточтоониполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупротив
оречатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадост
оевскогобросиласьвглазанеодномубиографудостоевскогоипослужилаимуказаниемнаизвестноесовр
еменноепсихологическоенаправлениепсихоанализтаккакподразумеваетсяименноонсклоненвидетьв
этомсобытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначну
обосновыватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунез
накомыучениеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслперв
ыхприпадковдостоевскоговегоюношескиегодызадолгодопоявленияэпилепсииуэтихприпадковбыло
подобиесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииелетаргическогоснаэтаболезн
ьнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяподавленностьчувство
каконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейчасжеумеретьив
самомделенаступалосостояниесовершенноподобноедействительнойсмертиегобратандрейрассказы
валчтофедоружевмолодыегодыпередтемкаказаснутьоставлялзаписькичтобоитсяночьюзаснутьсмерто
подобнымсномипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойв
ведениеснамизвестнысмыслинамерениетакихприпадковсмертониозначаюттотождествлениесумер
шимчеловекомкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмерти
второйслучайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожелалисмерт
идругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучениеутверждаетчт
оэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокявляетсятакимобразомсамонак
азаниемзапожеланиесмертиненавистномуотцуа

Ключ: a=27, b=211

Висновки: працюючи на цим практикумом я навчився розшифровувати текст зашифрований афінною біграмною підстановкою. Написав розпізнавач російської мови та згадав деяку теорію з розширеного алгоритму Евкліда.