МІНІСТЕРСТВО ОСВІТИ І НАУКИ
УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ
СІКОРСЬКОГО»
Фізико-технічний інститут

Криптографія
Комп’ютерний практикум №3

Виконали:
Студенти групи ФБ-05
Сапожник М.В.
Карась Б.І.

Київ - 2022

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.

Хід роботи:

1. Перед початком виконання роботи ми ознайомились з теоретичними відомостями та методичними вказівками до виконання лабораторної роботи.
2. Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь.
3. Визначили 5 найчастіших біграм шифротексту варіанту 2 ['на', 'но', 'об', 'нн', 'ен'] та знайшли кандидатів на ключ.

Труднощі при виконанні

При виконанні завдання, ми зіткнулися з деякими труднощами з шифруванням, оскільки при деяких випадках код виводив помилку або неповне розшифровування тексту. Ця помилка була вирішена простою заміною коду для сортування літер на speriod = sorted(bg_q, key=lambda l: bg_q[l], reverse=1)

5 найчастіших біграм у шт ['на', 'но', 'об', 'нн', 'ен']

Варіант 2 ШТ:

щоыкцрылжцьштхъогзцуэцъмщкубфющъуытфьбахсюьувчузюмопощквкъмьчтмусуьш
юхуцтрцоэитсуряхяьъыежърцяросыотюрщмчщсфьйоыоюыуъоэиътшйдхъьъхефярцйы
хявэцьщзхщцыфущкборяэййшдцчмцубжцюхшмяилхэвгшсоьлмтшцытъиоуянюбкрши
рчюгмчфщцшбвъинзьтьтэчшлцциучеутьхаюятужифкчтщььэщявтчлшообцуафъцгепхщ
умямщмьйэужйэнмдъптрчрмърйюхьпцйыхрувлейжннчщйувфющмапыэчпьлыюыыцн
цйрмйщьтьфььюльйякофахъбъьцьшрэиудыхлвэцюпнжхмьдщгыроюцлпъхзмйямюгьоа
ыуцхккящхфряшяцнъышйхшчобьуьщцаьцфебшахщоьупдьнфашпэюбоэшкстэлдазувац
ьжцонпйпнтцжэсцькфнщчжямъяэпсохтпнфтьшрхбыцъхдпрфаывчвкрмьэмцфйзазшяэ
щдвнпыщехщъершыяшуцикдхжпчяэецчшжищбмгуоуэрглпктхйлййообъсоерхкцйшзах
тьбуоуыъчрбюаюяошшнъянкъмщмъххтдшнрххйхахщмщьюрмснясцуткэпегщтйщцпйаи
йвлцввнхшнцдцфутэхэщлсыцшфулуычанхчтюрфаымурщаяьрдоноуюхпюяъяэепмйчф
цшцуьогзкжхяиуьфцьпмющсстхощрзарфавурямхорькбяяьъэнснчицйряыэчфрцйэччхъ

хаафщвржйьцнськцяэтхррсыщутъиьвчыылфйюцууьлпаэящцзжыпнчгяоуьбьнфйэннмц
шехцлгщьцыщчжущняэттыуххушйюмтбэпяффйюцуьокыгърархйсъвйафьякаскцаьцтро
щкбсыпэксйъосцфускщяшнытлчсупхьфыщцухйзштэчуцьуэюухяилдщшнэпецэзйэъчря
тьхчяглттпрфтягрбфгяцуиъноуочьвыьцоуииэйсцжбцфыцыехюнсжотяпруьжстоуйышх
ърщььйьмщрсзщзъшэямъепюзцдэмяющюстзйэхьжжпяммаянцйрмйуюхзхюящаупылс
ыушшшчяылчапгюттцьчптщкцитуйпжзсшсййррснъщйапчгяьуртаюыхфосотрувбзйяхд
нщзпшяцюэнлзннйыфйесюцчкстфудъмыэкгацнцъиноьщьакъщькфтучсцошюфхсьчяпа
ойымпющьцоййьцудъфмббуьурмюдляяхгичувэкешрштгхфшфысъхморыячуьаэхячзал
хчоэмюхяьвэуотбоьокрвэюяфцпысъчъчоъпшсчксъгтпоицачыгшеоэгфмэмюхющцэксъг
ожущршчукрфйэкднятьщвфцшконфоскъфхаацшамытцдхфоъэъмрццтхдрьшшюсяыщи
тыьсхофьзььфщйтфцшдрмсюабэрхйдхчрьищшжкцъухшннсцуббчщшрсгпглдщпщбоц
шьшрэиудрчуръкюжорхшшфнуьтщотутйялохучоапхдчкйящиьуыбцфящпкпптщйятуро
эягецикйгягявэньъкфтмцмъфбъпшылптьфчзъмыпээцыкихъежулкюьэягкпъишгавчбъь
ълдсняйпрвгюуцгзнлюыхфосоъэсхлдчпрнйщюаювацмдсхяозьфуяэщдвейящихшзхръс
цькфсипйымсыотршертхицьййифщщтцчщшйоофояянэюгмфчицькьбъьрнтдюъчгзпчьч
юршкхщцмхшчйвлбхузптхсгтзевэацмдчсрлпнмапюьчлрушнадъпышжуфщтйамсжщжу
вфяьуийюнщлоььзфааыкуымцйящцььувйхуэррчымсюрбхрчтршчрывчткпяыдтднцаъфь
уэсяшклъизмлщьюрцхшухчирдщкубфювкйарцщттмдъччрькпъишфыщцттуврхдюучкцт
югщцюлптшнцгглоцфсяцужацшчящцырбхэужднхцьюбтааущздшщлтмйцэвоюэусвцщт
жпчьпсуькзсинтящцупугьзттлчрькбйфягнежъыпсьмрафърьрпдфифьуыэющоюрццнхоьк
убфяуцшкхяицйжгяшъкюркуытйсушарьуйзцмшдцйуфуюсщспкйедляяяущыофукньцу
дымьтъохркьйкдхжмчьпсщросткфйхмжмсьалцсинхйящогбуткцмяыйъцжбэчшсцбснзы
яэхэръэяпусьцхтюацыаншлппмъсйвъоапыгжццнуляяяцьыофщсстйьибюцъмаячшзыъч
жйутрвацмдйюъехцтофпамюсйтаеймъэапрькчахъчыахалаабюйтщмопотюрькйрчйьнщ
аымяюааснргтъшфьищхыяыщрачцыяэчьскщюльйякофахъбъьцьшрэиудцшцфчжнхеоъ
рлыууыхрйулртъцлтащьзфсяэастыхйщчоэлжцщтлнфчпезщпьодвшхййчфцшцуьогзкжх
яъоооыорыщтъттчсдхртауаынлъизцещыпууьлглъиамамщмьйцюцутэстщгсрарцэрдъи
нйщзуилщцоптьшслызщуфяцычяунцйяхрбфъщпнтяяытпвыхяошннжнъехнфьбфчилцц
ихйуьуцэпуйзсстхотэваээсянуихъопнсьвэюмффтшлчиоцьъпасццгъипмсъщпдцупхчрщ
опхзюгъкфщттдхчзьыуаяобутйяэькуооавщнхефйнщськьбпъяьздшикйщзхрсувщсжско
хапаюьыиэууыурйашусфэяьфмэифмрвучхоцэнлчищаучорянхщсуэцшдящктаьгшгртъщ
трзарырюумчтмьцтчбучувлстюкйпйхтээаущксткофыхуфсцчртмтшолшпчяэряыуцэыфг
цтцфяьфшшжеиисоцуфпщщшузнчфтгхпгуугнцйщччсцуоооошщнтчшхчгрййбзццшкфп
ифхниьачящотдядожцюлвэрмчксмцыуюзршъцуъузыхзлосьббуъкчйозцмрюуььудъхйч
измэварнянчттрцхчызбзчаньпдфифзушуачтянупйхчсуцьбъухщздянфаыхтюроуурщыъ
ецйхтэпфхжнтятйлотяпрйгзстхфьыуфцъэъръхтщцфыотьвщюмнфдьтьжутцъччфрцйэп
йжнойтпщгрцйщтссоиоэбцыкуеъищчфпщзфамыкхпнпйыгшшфукрфдвхьэцмашюьфые
шютчншчобщьъоелтъцяуййафхыущдчщсцюпвюбьфыешхрыфцййафхыужяшрцдофсыч
чвхуръицмгжцбэябрйтяцамщшнтюубншвыяофулкяфюулджишолшзэафтвэежшзфдяхп
юшшяыуцчызлоуувщбяъхтхщбйящршчргюхмюъсыушшюыогэхдчюстымэюухцчкпйзб
татоэуцщхеомччснтрнбьэтежтмосцптюсььзттяиумпзыръкющсжншсдыщуъэъюлчяюъ
щдгзцчцогръсхяохшпгэфэяцеиытштсппавявхнняыщмящэюухцчкпйзкящпхрщюмэауы
усъцжэаэряпнцэиъхщмтюсоюукмпгихыжувьугцнжяшйзулцшсцюжфйэщчсототбьблдл
нфоцшзплъоыюйдьцнфьиыхфэбщчйвхсыушшшфыцъупнмумбнуэфпмцусхщфтрзахщя
гмапънхсьншюабжщздягхионуяфтсшчмдхдряфоапяглгэхфлтщфуэчуэкффыясцотевээя
онеертирзтжпащъдцхуоцыпчтчшгщхуэцютюхргжцььджкмсспъюуашячшсхкофяпахбут
жрхихчрюъябщьфщфтшрымшзряэтшрсйшдитацюрсцььджщнъцушыхсувэуньшспущут
зуъумфыщъмцйоыфющрощыфутызюгщожхуцышчнцшшюьесццгыъштамюшщюяннж
янхсьщуввющьчмднъоькьрбаблпъхццдшщьвээцыкфтпйпуубуэюьщнпхяытахэхяубрмд
шцкйтхщртовуййшкхйящубьуурццыслпьльзщуыщчтэиирулщхьыяъряшиштшчьтпряф
хйчнхйщсьщщоюлзоткчоюъсчпъылздщчсфьйрюцъясттхпъцуфйвэюилрдчиуднщьюааб
лдктуолшзшюбьблдмьцфтяфбыпрщхчтэыштжмуфэещэежсцжцькььфяглджфмчщыъщ

шюьвчуцэнфсокубфюсючйозлхуктрцоэрьдянфаыхэюъбилртюджблшррыэщыерхщудхз
щифвюлцйчыцибхаюярснэмюдчцяйьшдпдчезяшоцкжхрыугхееиуймхсоъэчгщлйшъчн
жхаыпыхьптцлйлущуэщцщнуцяыыоьфузььчрежяцщфошяъпхсццщэибсбецббьбугуэцът
рчуьфыюжъжнфшмюхръэаяыайпцхфосурбаблпъхцщтршьбваыыужйщлтцьфхяауриъмъ
щыжуфыюшьбуимъифаыхчффасцбвогфтбщрхяфхртмтоьфызщшаасвчтыйдыыхррыэщ
ыажищйхййообяущнщунщцрфуэпяэрхцйхчфбшяъччвэшитхыоосэюъьчрттэыъхшхъгрй
ьшехяцфашхэмоыиэуетмцячяьвъоюпцохслдъццабьчрмдвфопутцгсщцхцгънърьщюпьо
уьгцэиммефьббкщьчтэрсгхзяьфнььдктуыднцюхаясщтдпцлхууъшяуяпнснтчжошшрцоь
окхтшцйэхтэчъскипнпъдъхугховшуйдъчцосрбфцтжртютйлотнъяьэрфамхъцрзшюьуиш
уоэыпооццтпхсщжйсцххькщрацььдзтщофематфюглджишолшзплъощтпдчцтцьфоифчф
лмйягцйшчыыэсвщжтшнрсьйоэчньрусхмьуюхгюяьуюййыыыдаъсюабхлххякосыхчфвъ
мвкнюгццюзсшжувхнуылсенйхпъщщьчтчьйоязлвэшсхдмьшоиэхщртоьмапымчсушуэч
уяэттдхчзьльчэюсоуфымйбтпысвюфлэтяуйстпнтфщщхуеэрыдыпнэфъющлоыхотпвеэк
ъяхелнуъгщпжмптбрцдящйрсмяхяоюруутшйццйылштцсшфъгтмщпюгщьущймянфаъм
ффвысыуиъцмтьщтхъощэусьръаъзегбктщрйтусыывчзфъащрдриоцяжрюгцзуепйхдщтх
шгыуюэещнщчиучфрьццчксмхочтпршъьвъхмютчфппуьаьямюдтфштюмхгъкглчдщъвд
амщмььаыужтмосыхсюуьшшесхзштщфопюьгрхгчшчжццюшцысхужххсъцздшчыцнаг
пуосьцююсухртсинштцшшшяушюраяиытрфуфпщщъхмпуоыуфйывейукххудйятцьэяы
щзхчцоталуыфыщрцыхъййафуюргяпнрифцдэчотчанъкфтмйжорярыйцэкушгоуюпрхбй
яцбзтцайыгюрухсэкемщыдювчъэргщхтцусхахшдпшвлуцюыыхайьтпщууймщцыдъийы
чяыцгыхъопкфьычеюжоцттъцэхлвэъдуфтсчсхцжыхврщпкпбцхдщмюьэыгьпдфифзушу
атщснеьыъфдыляъэсяпулышйхазюлштбюидрирдтъъзчряъхтязцчщжхэпещэтдерллстнф
кьакчапщыфущцычяншкцаощттшатфыюуппхццрцьошъбпыбйпрачязъбююяьньйщудхз
щуфяцыдтсшьзьушюмаяхурнхнмюсьнбьфрцйэпйуыъщбоцвкзсифцйтхрюъквэзтщччоь
шцыанюлрмюъчошхлвэшяичтянкгбнуэфшсьейящигэхяьэаббрсньчцькюргцщчупымчн
емщюсуыичтхйдппмтюъофлзмчъчфтмргзшсьужюнхвызнхтьюрзйюъйыахагбсспецйрх
чфпшяэяглхьтцыйдйцъбьблптюкосывуфпыюжкзыкчфнщьэпэспксхрлдъццапыяъуытфь
хцщбрецрэхйоыоцызжхтьучкьнъопкшатпяаыуххуисояцбэьгрьйюълйыфцъчесьчйъдутс
ппэвашлхчонптъпьвсоэънфыкытфмрльухщзйэзоцуыььфццоууымамымыэкъхщзйэззсь
ъышдъсцутьгыджхаыпыхудрхшцднъмвьорьфтчцтсожявяоюлусхфчзбщыхаэблзмядъго
щйзпягртачцсруттхъьвнерьрщдъпшюьуишумпщоцосцффщянчтщяытукьюбузъупхъсос
мяхяэячуфжрфхнлоъпшяфусьцфмапшсчхюрцртхшфьиюръярнййыыыдавыртььщцтпиц
мньфьфаышуучршталгюькыюптэцыоьпнбььющтйпнщвещьэфаяьуеысшфцюцэксцькф
ппнтгфбыэацбгсыасирзтжпанцкцъирдтийыээбрййшнцоосэюбуюбндшдцячшрхбщмфн
сыснтрхщмььвураъгттапышецсбнмыъудхзщбоьтеджхкацьььзфаяьчдядъгемщюсуыщсц
тфцягшюрцбчрфтюуйпэчьзлыяьтдщрштглуахцулрсттчцьчйхщьюэеоягсськтрюьэщидш
зумрфбыуовцшынсщйтсцщьуилццыузицхаъпхмневящитащоъчгущмрыоцтящущжаящ
чоэглдмщяпюубрймъгхмъхфээяылмдядацьжегсягншвюнкгрпыюсогжсутшоиэчьеэюян
арюъйфжпъбщошлрзтщофцмяычбчшкрыльуьуьзлямшшцыхоуьорюъмцоучортъуъчвчп
цттдчирдыфйьбйащкитаежллцэрбботдцмоькдаютьвюсдюаоижмсющюянухыщймюзхт
фуйзфтпныфбдаюрйьъхмчирсьжцсфхгщитънътппюръярьфтэрыашхнэфряцбсыпйуыъщ
бошяойдшныйагхрштщнсйумьсочьфьйъщчитуыйпмтюъфюжжяшрштткьвэрщэбиытьр
уфалрцьрчяснцаспцыфсцшйч

Розшифровка(ключ(27, 211))

Текст

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопред
еленноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодля
жизниприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостига
тьтакойсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокруже
нийимогуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприр

одепоступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстр
анноэтониказалосьчистотелеснымипричинамиэтисостояниямогутпервоначальновозни
катьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимости
отдушевныхволненийкакнихарактернодляогромногобольшинстваслучаевинтеллектуа
льноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысше
йинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношенииикоторыхутвержд
алосьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодостоевскоголица
страдающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститаккакэт
аболезньчастосопряженасярковыраженнымидиотизмомикрупнейшимимозговымидефе
ктаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадки
совсемисвоимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвити
емискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффект
ивностьюнеудивительночтопритакихобстоятельствахневозможноустановитьсовокупн
остьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимпт
омовтребуетповидимомуфункциональногопониманиякакеслибымеханизманормальног
овысвобожденияпервичныхпозывовбылподготовленорганическимеханизмкоторыйисп
ользуетсяприналичииивесьмаразныхусловийкакпринарушениимозговойдеятельностипр
итяжкомзаболеваниитканейилитоксическомзаболеваниитакипринедостаточномконтро
ледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделени
емнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпе
рвичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейо
сноветоксическиужедревнейшиеврачиназываликоитусмалойэпилепсиейивиделивполо
вомактесмягчениеиадаптациювысвобожденияэпилептическогоотводараздраженияэпи
лептическаяреакциякаковымименемможноназватьвсеэтовместевзятоенесомненнотакж
епоступаетиврасполяжениеневрозасущностькотороговтомчтобыликвидироватьсомати
ческимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилептичес
кийприпадокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидоизмен
яетсяподобнотомукакэтопроисходитпринормальномтеченииисексуальногопроцессатак
имобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпракт
ическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающ
ийвторойневротиквпервомслучаедушевнаяжизньподверженанарушениюизвневоворо
мслучаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятночтоэпил
епсиядостоевскогоотносится яковторомувидуточнодоказатьэтонельзятаккаквтакомслуч
аенужнобылобывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследу
ющиевидоизмененияэтихприпадковадляэтогоунаснедостаточноданныхописаниясамих
припадковничегонедаютсведенияосоотношенияхмеждуприпадкамииипереживаниямин
еполныичастопротиворечивывсеговероятнеепредположениечтоприпадкиначалисьудос
тоевскогоужевдетствечтоонивначалехарактеризовалисьболееслабымисимптомамиито
лькопослепотрясшегоегопереживаниянавосемнадцатомгодужизниубийстваотцаприня
лиформуэпилепсиибылобывесьмауместноеслибыоправдалосьточтоониполностьюпрек
ратилисьвовремяотбыванияимкаторгивсибириноэтомупротиворечатдругиеуказанияоч
евиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадостоевскогобро
силасьвглазанеодномубиографудостоевскогоипослужилаимуказаниемнаизвестноесовр
еменноепсихологическоенаправлениепсихоанализтаккакподразумеваетсяименноонскл
оненвидетьвэтомсобытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпун
ктегоневрозаеслияначнуобосновыватьэтуустановкупсихоаналитическиопасаюсьчтоок
ажусьнепонятнымдлявсехтехкомунезнакомыучениеивыраженияпсихоанализаунасоди
ннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдостоевскоговегоюно
шескиегодызадолгодопоявленияэпилепсииуэтихприпадковбылоподобиесмертиониназ
ывалисьстрахомсмертиивыражалисьвсостоянииле таргическогоснаэтаболезньнаходила
нанеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяподавленностьчувст
вокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейча

сжеумеретьивсамомделенаступалосостояниесовершеннподобноедействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемкакзаснутьоставлялзаписькичтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестнысмыслинамерениетакихприпадковсмертиониозначаютотождествлениесумершимчеловекомкоторый действительноумерилисчеловекомживымещенокоторомумыжелаемсмертивторойслучайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожелалисмертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучение утверждаетчтоэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокявляетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Висновок

Виконуючи лабораторну роботу, ми опанували навички і методи роботи з модульною арифметикою, зробили програму для розшифрування біграмного афінного шифру, проаналізували його, закріпили навички частотного аналізу