Криптографія

Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки

Виконали
Студенти 3-го курсу
Групи ФБ-02
Замрій Денис та
Гнатюк Максим

Мета роботи:

Набуття навичок частотного аналізу на шрикладі 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 шифротексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a, в) 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. **Реалізували функції для знаходження НСД та оберненого елементу. Для цього використали алгоритм Евкліда.**

2. **За допомогою функції Prime5() знайшли 5 біграм які найчастше зустрічаються в тексті. ['вм', 'мь', 'кч', 'жг', 'йв']**
3. **Співставили наші найчастіші біграми з найчастіші біграми, які були вказані в теоретичних відомостях ['ст', 'но', 'то', 'на', 'ен']. Та реалізували функції які знаодять всі можливі пари ключів a та b, шляхом розв'язання системи.**

4. **Підставили отримані ключі a = 35, b = 219 в формули, та отримали змістовний текст.**

В результаті отримали ось такий вивід:

```
--------------------------------------------------------------------------------------------------------------
Freq: {'ь': 330, 'г': 323, 'в': 308, 'ц': 278, 'ч': 256, 'м': 256, 'п': 230, 'и': 230, 'д': 222, 'к': 19
--------------------------------------------------------------------------------------------------------------
The most frequent bigrams: ['вм', 'мь', 'кч', 'жг', 'йв']
Encrypt text: коетоеюгчвцпйжжиддкгвцщпоемьрвваетьчвыынюкетдашьццрвфвиьдьзьвмьцщцынржгяэцаиуксгюччевцыкгк
--------------------------------------------------------------------------------------------------------------
Key: a =  35
Key: b =  219
--------------------------------------------------------------------------------------------------------------
Decrypt text: агодышлидашлибыстроинеслышнокакподснежныеводыпротекаламолодостьеленывбездействиивнешнемвов
--------------------------------------------------------------------------------------------------------------

Process finished with exit code 0
```

Encrypt text:

**коетоеюгчвцпйжжиддкгвцщпоемьрвваетьчвыынюкетдашьццрвфвиьдьзьвмьцщцынржгяэц
аиуксгюччевцыкгктрддкчвцнжудчжегддюкдонаетярйрвцкчэжяпкгуьгиушэцшгуафишййкуг
втоувмяшгккшпчхчпиэефвмсжгэьжчлзшьбгццусшлйюьпыирсжгаьчтхчрмжохмипхчлтипкч
лзыипцвмэврэьмфпрмвцгьяьцдыисвпчыисвфвфьымьигктцзчгяйкьихуцьэвдвйгфвэьяиуккч
мьаияьэщйгтччщмьйгтччщетцчмллзбцнрквыдоягьйвфвмсщадоыиупцьбгмьаьпчижфпыивл
тлщмбэйкэпрмхцтлщцэлцчэжяппчулбьвцвмпияющцегжгемпчсрэцпыккупцьэвлкупыиагбьв
гфвмспчргмьчтыифуыиэжсчнапчхууплтныэжгюфвмснвиьаиэжектцымрьгдьыупжцзлояупф
иьцычрмвжпиыужищцлчаувцбьвцфьяюачаурвцыэмчжгяхщнкивхщфгрсвцаьгьнршвфвпчр
гвмйвшчфисвмьшгдьмсжзхмпмашнриьсхыгньдруцжгокфийуэврэьмфпрмпчвбкмечсрюцхпц
ьшядьрвлцвмфцлчлзюгньйвглщахмлютцлчэззьфимьпвжгекпиьцльмохчпяиьгатгшьхнитудг
кэзулоцрлтззьчопчйудояайвшгрспюфьщпатжгпищцхныьщцтчсгибгяюгэваьвцрчрьццзцщц
ынжгаьфвюкынгибцуцвцрцуьрпвжщцжгчмнпаьпвдьрцкчодпвзгмьчтмцюатгньбгдьтонпгкр
ббьпчныипмцмбяохмьбяопчулбьвцецфврмьбйужгемпчйужиюгукзцдьядфицгщахмоупчэрыг
```
```

ювфвчвецыуююфвмсэвливжлзрцяацбмьчдгкетфплткчюялтвцзчгквцдвучьббьбьцгусмьэжгя
аусчмьпилциьэвэььплтрмечсрюцфвсвщгдвщгевдьючжзсвщгчддифифпфишкедпврспюэвярхрж
дияшашьньбгфвтайирвюгмсйисвтнкчюкрпрмюкугзлзнуссчтаудфктхыгвцвжньбгюгмсжзчв
шьдлтлпчхчьисвйвфвмсвцннчврсбьгьымгквцюашььиньбгдьбьшлйкжкнпмьпвлчлзнругшл
ояфкупыишкнвиьюцкчщдьымьмифьаьаиуксгыдетынбццбыибьйнюгбайвфцфьйгшврсспцб
фуюрбгьпчмкимгвцфьжгшврсбцвмйвлчфиццокэцьсшлхмуддопчвбуппюэвэдыишлояипкчлт
нптельйнячгккчмьгьвцхмньбгфвхммлэвпчфумьгьнршвфввжодтцьсюклькжцлдоягьяьоць
чхуфьддэжмьвмшкдвчгццчйьцуаэсгяьтчулмцукпккяьивцвжньбгиьвмчщвжпикцпгрстцгдр
ммьвмагбищцзьпвжгоквмйвццэглцшлашвжфввмышчдйкфпечудыичдатипчмагуфудшвлгоь
чдоуоещцлчкшйвцдижхмрвзгоцйрюгшьпврсцчйьцуаэйщнпгбмьвмккэьвдйукчмьиьийпиукк
чвбупгкфидумтпичмкшгьзьвдыиыуьмтгпврмпюрвячвбупечэзырилэлдочвэьлгупеччцчдхмп
ипнутйумлйвыглцшлашвмйвэвпаоудоюгяащцвмьищодьлвусмьаирмаштлодгкфьюгыглцшл
тзжпыдачшаьбфцэвярпцжгфайвкбипгкзлшаудетфпрсорудувжгдвлгдштлодгкэуыитцвмйвку
ыдшаьбыгетмьвдйукчмьюцвццбйудвгьчхыгждзагнэяэвюгчдиппирсэьддщтжглцвмпваштпк
чжияьыьжчрьшукчккупьиагэцругбодгяэвлгпчупеччцждхчбэнбыибьфьблйвэцлчауевшьцюэ
тищчгщжписпьмынртфизррлцццщйьлчлзтцыгвцшлнпвлтатгпгмьксатцчккугмсэупиццстип
упхувынрэвшьжчэзаькачщццччэзйвежлзщцуохумтжзвмфцлчаумьннрмушмьдьэгьиияячвлен
цыьщцйуюйынегэцпцннзлоудсумодедояшгыгзлоуоржгрвлгртцюпккясгюцдтдчщдетындшщ
дтлццэисвбтщдбьервмхчгкщцлчкшддхчьчаэчьэвусынвгаыыаудаэкювгбатгхэщабцвмгпдеыт
пвшгчвшошьвнйвшлзныгегшгзьпяюцвцжгатхчынрдыигдзмнцчвлчкшчдатфьфвуврмыммл
оукмфикржвычкгюгфьщпфэипкчшайвьпкчынвтжзвмшгаисвюгжкпиццрицнщпцчйьцуаэсг
пмхмшгжчщдсекчкюгиддцбмцеисчргыьщццбыибьфьщпатвмшгрудокмйнрснвцнодояынбц
щпщашшейкчццдиэлжгэгяайвяьфчулхчтлхмудцщфьддвбкчаупиьэедижхмцтпичмаььпгтжзб
ьдполнпщцемккзвдмудгкпммльмыиддчфргфьццтгиьйрукедныьмкиекпнпюжввтнпфвшьяь
жчтлжцщпулжгувьыегитхчьметфисвбьфчнпдекищцялшазыидэмиашшэмэмипмгйвбирвдврс
фикрпглейупюяьхтипкчгкфиццпооярмьгюгфьццщцшгэцжграшшэмэмипдузырмстипьмвлж
гшцфцюгаьщцучщщоцэпфуеьлцьспвочцщцчйьцуаэйщвжодяомцороьддыигдзмкючдатвмйкц
юумпкаткчкюнпгтышьибьтгйжнпгяжгогмсшвэьвмгюжгцилцбьсклвиляшетэваьфьзчкчйщцы
ьусщьгьпгщпыикцлгупьибьерждияяпгбмьвмьискаткчнцдлоудсумодгкфисвюгмсэвбьяысрш
ьючегдмоуецэьвмгюжггббьмтрьзеыдмьгььифьусуьпвжггхэускаткчнцгигкоцюцлчоувгоцзртг
сувмхчгкэмпюгиэжнпбцпвочлзйнвмшьйвжкккищуцаитьддыиусцшиянзвмпвзьньхнхмзртгсу
ыисвмьсюеиекнымьзбыирсбкупумынпафизрспкчтзяьзчдоашвмйвэврдояшгыгрмидпяшвяа
фивжвмеррмшьвмеьийпиуккчмьгьчдкгжкетвмпввпрбпцжгдцгьвмяремидедфизрчдкгжкетэ
мипечфиыгддщтйкоумьэгньддыицююхаьмьвгщгчвецвцхуэщчгйлзртгсузалюиьгьхммьпцжг
рувынрэвшьжчжцзртгвмшлжцфьддэжщцжгпиыгорюгяррмзчдоьбьищцлччцжлпчоугбпищгн
ашьзцбивьэлзнпвьйнцзьфьгчэмипеччцзнилмтцючдетбллгцчрмидьиеищгньддыищцаиияячвп
вчмйунвцнорщпгккюдпхдфисвчдкгжкетвмпвгиьхыгщвемудцтипищддояшгыгегбтйиддсгзрт
гсуцьлцьспвочаудпциддхчяаодушетыннмщаоужлпчоуулнцпчоугбпищгрмяржчфиыгаьбьзнн
аодвыккищсхыггьгрчвэиукхчйудокмвцшлояьмкисчэршьючодояшгыгчмидпяшвмьчдихбьд
лнычвциддхчргюцрмпхбьиьачэекчсгпквщяафэяфулоэипытхчмьядижхмедыиыухмоцрсщаш
ьхчуппяыдгкьмжьмохчпяаэйщзртгвмшллзэцчмипечфиыггиддхчпикцоцньжчауыгфьшхаьм
ьвгщгэвчдхуодюккчждсгючвбуподыиыуьмтгпвумпюццудрмулоурметгбпищгнанпзыкчкюьи
щпатгкхчкюдвццэтмцеитьзцилщдояюгфчкшщвемудгкйвжкэмкюцчнрвмтгэмидпяшвфцаотг
щатгшьжчудпиидьчэзжрусзрччкгвмудгбпищгхгцчмдыиддблзрччэзфьццхэивалоуспзльчжцз
ртгвмшлжцйвььжгшьпвжгатупбцчдгкетэмпюхчуппяэьвдйукчмьгьэьвмгюжгмгбтйиддсгзртг
суйккчждсгбцхмэцусынйлоуфьвцсмгкэвйьвцвжуцгьидгкяюжлпчоугбпиаьгьйвжкэмкювмйв
ынчврмпющэкчрвэьлгупечбхаьмьвглцшллзшьюгцчнрвмтгэмидпяшвпхаьмьвгхцфцаотгсгц
ятлхщлцжгнашьяьбгеитьийтзхчуппяудувжгдвлгэмидьиеиаьртююццусмьвмкквмйвэвсикцоц
ньжчауыгфьшхаьмьвгщгяьиййукккчждсгкбыиачфиыгфцаокючдцчлтщцавдиддхчфуяаодуш
етыннмщаоужлпчоуулсгюцрмццзчйукчбцяафэяфгбпищгцбодпнаьбьзнльюпгбищццльхтярэг
сиддхчпмдохмщайкхммьпцжгыдояшгыгмгбтйиддсгзртгсуцььчгкмьбмтллзлцюмлзекцюрмп
юбьымхмидпяыккчждсгйвжкккмцеишрецчвючжцпцючвбупатпврэьмдогкзлйкпмлзвмйввц
щпзыфпьилмйвбглгпчынрмидьиеищгписюнгзртгсуекцюрмпюпвочлзхмйвщпчщэвшьжчдош

шиянзвмпвэьвдйукчмьоккчждсгаьюглцвмяьцчфиддхчынтмидьибьбафишйищчгаккчждйщ
йввмрмпягьчвтоетбьорвцшвдьяафивжвмеррмыьувцциетзжрусзрччкгвмудгбпищгхгчдыдет

Decrypt text:

Бачимо, що текст змістовний, і можна легко прочитати його.

А|годы|шли|да|шли|быстро|и|не|слышно|как|подснежные|воды|протекала|молодостье|ленывб
ездействиивнешнемвовнутреннейборьбеитревогеподругунеенебылоизовсехдевицпосещавши
хдомстаховыхонанесошласьнисоднойродительскаявластьникогданетяготеланаделенойасшес
тнадцатилетнеговозрастаонасталапочтисовсемнезависимаоназажиласобственнойсвоеюжизн
ьюножизньюодинокойеедушаиразгораласьипогасалаодинокоонабиласькакптицавклеткеакл
еткинебылониктонестеснялееиниктонеудерживалаонарваласьитомиласьонаиногдасамасебя
непонималадажебоялась самойсебявсечтоокружалоееказалосьейнетобессмысленнымнетонеп
онятнымкакжитьбезлюбвиалюбитьнекогодумалаонаистрашностановилосьейотэтихдумотэт
ихощущенийвосемнадцатилетоначутьнеумерлаотзлокачественнойлихорадкипотрясенныйдо
основаниявесьееорганизмотприродыздоровыйикрепкийдолгонемогсправитьсяпоследниесле
дыболезниисчезлинаконецноотецеленыниколаевнывсеещенебезозлобленияТолковалобеенер
вахиногдаейприходиловголовучтоонажелаетчеготочегониктонежелаеточемниктонемыслитв
целойроссиипотомонаутихаладажесмеяласьнадсобойбеспечнопроводиладеньзаднемновнезап
ночтотосильноебезымянноесчемонасовладетьнеумелатакизакипаловнейтакипросилосьвырв
атьсянаружугрозапроходилаопускалисьусталыеневзлетевшиекрыльянопорывыэтинеобходи
лисьейдаромкаконанистараласьневыдатьтогочтовнейпроисходилотоскавзволнованнойдуши
сказываласьвсамомеенаружномспокойствииироднымееечастобыливправепожиматьплечамиу
дивлятьсяинепониматьеестранностейвденьскоторогоначалсянашрассказеленадольшеобыкн
овенногонеотходилаотокнаонамногодумалаоберсеньевеосвоемразговореснимпотребностьвза
щитеинформациивозникаетвсвязиснеобходимостьюобеспечитьсекретностьисследованийвст
ратегическихобластяхправильнораспределятьинформациюопромышленныхразработкахире
гулироватьинформациюоличностивсовременномобщественачаловосьмидесятыхгодоврассма
триваетсякакначальныйпунктогдасоциальныепротестывдемократическихстранахпомогли
сплестисьглобальнойсетихакеровполитическийфлиртнапочвенарушенияправчеловекапород
илтьмуорганизацийхакероввмассестранмирапочтиодновременноменеечемзагодэтигруппыуз
налипрелестьсотрудничестваихчленысвободнообменивалисьидеямичерезнациональныегран
ицычастопоукраденнымпаролямдающимбесплатныйдоступктелефоннойсетинесколькоприч
инобъединившисьвместесделалимеждународныйкомпьютерныйразбойлегкимидейственным
новыетехнологиисоздавшиеболеемощныеидешевыекомпьютерыразвитиекоммуникацийдля
связиимеждународныйхарактерстандартовустановленныхтранснациональнымикорпорация
мивпринципеестьлишьдвавидаугрозыраскрытиеивидоизмененияданныхраскрытиеданныхп
редполагаетчтокомутослучайноилипослеценаправленныхдействийстализвестенсмыслинф
ормацииэтотвиднарушенияВстречаетсянаиболеечастопоследствиямогутбытьсамыеразныеес
липохищентексткнигисправочниканакоторуюпотраченымесяцыработыдесятковлюдейтодля
коллективаавторовэтокатастрофаипотеримогутвыражатьсявтысячахдоллароводнакоесликн
игаужеизданатодостаточнолишьслегкапожуритьпохитителяирассказатьослучившемсявотде
леновостейгазетыилипотелевидениюпохитительможетсделатькнигевеликолепнуюрекламуо
ченьважнуюинформациюоберегаемуюотраскрытияпредставляютсведенияолюдяхисториибо
лезниписьмасостоянияСчетоввбанкаходнакопомнениюбольшогочисласпециалистовугрозыл
ичностисведениемкомпьютеровостались натомжеуровнеивтомжесостоянииЧтоидообширног
оиспользованияэвмведениевсовременномМиретуризмстановитсявсеболееважнойбыстрораз
вивающейсяотрасльюхозяйствадоходыоттуризмастановятсяважнойчастьювалютныхпоступ
ленийвомногихстранахразвитиетуризмаспособствуетростуобщественногопроизводстваулуч
шениюегоструктурыроступроизводительноститрудавомногихотрасляхэкономикидаженеиме
ющихктуризмупрямогоотношениямеждународноетуристскоепотреблениестимулируетмного
численныеэкономическиепроцессыоткрывающиедополнительныерынкидляпродукциинету

ристскихотраслейсоздаваятемсамымусловиядлярастапроизводствавсеэтифакторыделаютраз витиеиндустриитуризмаоченьважнымдлястранспереходнымтипомэкономикиеономическиет рудностикоторыепереживаютэтигосударстванемогутнесказатьсянауровнеразвитиятуризман оприэтомкаждаястранаимеетвэтомотношениисвоюспецификуцельданнойработырассмотрет ьипроанализироватьорганизациютуристскойдеятельностивстранепереходнымтипомэконом икинапримеревенгриивначалерассматриваютсятеоретикометодическиеположенияисследова ниязатемдаетсяоценкаразличныхфакторовразвитияиндустриитуризмавенгрииприродноресу рсныйкультурноисторическийиинфраструктурныйпотенциалкомплексноетуристскоерайон ированиедалеепроводитсяанализсовременногосостоянияиндустриитуризмавенгриииеотдель ныхкомпонентовнафонеобщегоуровняэкономическогоразвитиястраныдаетсяоценкасоциаль ноэкономическойролииндустриитуризмавэкономикевенгриииивзаключениепроводитсяобщи йанализорганизациитуристскойдеятельностивстранахпереходнымтипомэкономикивобщем ивенгриивчастностивенгияпринадлежакстранамспереходнымтипомэкономикиимееттемнем енееспецификиечертыкоторыеотличаютееотдругихстранэтоготипавотношенииразвитияи ндустриитуризмаосновнойтакойчертойявляетсяточтотуризмвенгрииразвиваетсяужедавное шевначаледвадцатоговекавэтойстранесложилисьтрадиционныетуристскиесвязитуризмявля етсяважнойотрасльюнародногохозяйствасовременнойвенгрииколичествоиностранныхтурис товпосещающихвенгриюрастетизгодавгодтомунемалоспособствуетбогатейшийкультурноист орическийиприрод

Висновок:

В ході виконання цієї лабораторної роботи ми отримали практичні навички частотного аналізу на прикладі розкриття моноалфавітної підстановки. Розшифрували зашифрований текст, за допомогою Афінного шифру.