КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Стеденти групи ФБ-11 Шестак Максим та Тирнавська Єлизавнта

Мета роботи:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи:

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

Щоб розпізнати змістовний текст, ми використали критерій заборонених l-грам. Спочатку ми визначити біграми, які неможливо зустріти в російській мові:

```
# Неможливі біграми
bad_bigrams = ['иь', 'юь', 'йь', 'оь', 'йы', 'яь', 'ыю',
               'ыь', 'ьь', 'аы', 'юы', 'еь', 'еы', 'хь',
               'аь', 'ць', 'ыы', 'яы', 'оы', 'эы', 'кь',
               'уь', 'йй', 'уы', 'иы', 'эь']
```

Якщо у нашому розшифрованому тексті з’являться такі сполучення букв, то це буде свідчити про те, що текст розшифровано неправильно і ми перейдемо до іншого ключа.

Ключ `Ключ: (13, 151)`

Зашифрований текст:

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысе
чамнмпывйвфяжтинфвйвйвсжнпчнмпгущзкыфвйвутсюцзкыкынмотзщбйьыбшхо
луычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаыч
йдбцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйп
рйжклечаккяжюыщяояфскчбяызрчйзчвгзжзычэявсшчтщлжочшызюшхачрнтмнку
фйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщя
лчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеа
рчэяицкятчрогцфэкыпэзтйпчаэеэявахыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэт
ыычлчокбцккузбнинепжвининачрнсджяццаиятчщтецрнбяшквдиабцотияьацційв
ычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнкся
бяешщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэ
вячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырцсоу
шрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюр
чньаччквсеокяяорнбччнйцнбшзикзчшклзпеепаопниашчеквдзеязэгцеккьызаццнк
шчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытн
щрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящ
яцзэклтвсбцяыыцлтбцдйрцецкзвзвычяквсойюшххолуычннйвбнзеевсоцзпахышчг
зючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвцяучрнкейп
рцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярач
ыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйз
твйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыцзыэ
щрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдч
екеэгызнзтчнпнивучппжкнкэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэй

когхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойз
ьялчуцднеэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыб
шнрчнмпмэхчйцбйвсчнмпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнкт
ейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиащзфтногзаашятч
фяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщя
ебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхо
инхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутсюцзкыфпцеэярнкецз
кышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаю
ьукфвецыогзбшучяпхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолп
аццнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшб
йчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччекиабшфя
яцмнкыбэкгхчтыгшшчкгнккршчтчиншчияцзывьяючбятьюьюаыыкьзаучйзтысюие
бчщзечучючьквяднеэльачрнвязарчтчйдбйеплюрбучэтийшчрнвцебтцузйджчутеэь
ьсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчне
зучлчмыбшхыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзов
йдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебчочьвеслеяздчюзюабйчыик
фтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфт
лзньхярнбяшкжкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйацц
еяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцььэтнкфякэцтзыхынмлзещккмвинз
тчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпн
кэофяйтмпдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыи
чнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычицнввдевинзтсолчспейцаыячыб
шйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоеч
еклнжшдэпаычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзацц
ицхкпцкяхыозбятчызякиащзфяеыюччажсчащзьянвшхьягнлжчцеофлшххобятчьы
дсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзое
ыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыьке
эиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзкеэзщйхчащзднеэшдшызюуфач
штвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтч
сжлжыяызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшриф
шчучлжияшкрбнитятнрцшчрнгятчлаэтмэщяшкиабшсеотбяющузрчычьышсепьке
йуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпац
ытыызкьццзтьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшр
йкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпйкщтыызззэкицбчичжеиа
жчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнку
ффтчавяюзаояалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйф
чыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчучючцяцзицтллфвычялкшяюаэк
йпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрн
яыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрн
зтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмзынк
щфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчт

чнасжнпоебччцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыы
зйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцотцяьнщммпуэфтцежскыназебч
ечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцп
ажэецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчв
ырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкыозрнотмусзщяхаэбычпабшкытн
щммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжцз
еотлжееинеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзсси
аычицнввджкйсиахыычяктзфятыыяькоыечзнзтчхучычньбнзежкфэкксяйцщцккяж
жагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Розшифрований текст:
многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписател
якакневротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносму
щающейнассложностинаименееспоренонкакписательместоеговодномрядусшекспир
омбратьякарамазовывеличайшийроманизвсехкогдалибонаписанныхалегендаовелико
минквизитореодноизвысочайшихдостиженийимировойлитературыпереоценитькоторо
еневозможноксожалениюпередпроблемойписательскоготворчествапсихоанализдолж
енсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяегочеловек
омвысоконравственнымнатомоснованиичтотолькототдостигаетвысшегонравственно
госовершенствактопрошелчерезглубочайшиебездныгреховностимыигнорируемодно
соображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспыт
ываемоеискушениеприэтомемунеподдаваяськтожепопеременнотогрешиттораскаива
ясьставитсебевысокиенравственныецелитоголегкоупрекнутьвтомчтоонслишкомудоб
нодлясебястроитсвоюжизньоннеисполняетосновногопринципанравственностинеобх
одимостиотречениявтовремякакнравственныйобразжизнивпрактическихинтересахвс
егочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварваровубива
вшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромрасчи
щавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюхарак
тернаярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыдостоев
скогопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозывовинд
ивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинени
юмирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскому
мелкодушномунационализмукчемуменеезначительныеумыпришлисгораздоменьшим
иусилиямичемонвэтомслабоеместобольшойличностидостоевскийупустилвозможнос
тьстатьучителемиосводителемчеловечестваиприсоединилсяктюремщикамкультур
абудущегонемногимбудетемуобязанавэтомповсейвероятностипроявилсяегоневрозиз
закоторогоонибылосужденнатакуюнеудачупомощипостиженияисилелюбвиклюдяме
мубылоткрытдругойапостольскийпутьслужениянампредставляетсяотталкивающимр
ассматриваниедостоевскоговкачествегрешникаилипреступниканоэтоотталкиваниене
должноосновыватьсянаобывательскойоценкепреступникавыявитьподлиннуюмотива
циюпреступлениянедолгодляпреступникасущественныдвечертыбезграничноесебялю
биеисильнаядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляихпроя
влениййвляетсябезлюбовностьнехваткаэмоциональнооценочногоотношениякчелове

кутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотребнос
тьвлюбвииегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозвол
явшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьимститьнапримерпоот
ношениюкегопервойженеиеелюбовникунотогдавозникаетвопросоткудаприходитсоб
лазнпричислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреиму
щественнонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосущест
вованиитакихсклонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизн
истрастиегоказартнымиграмможетбытьсексуальногорастлениянезрелойдевочкииспо
ведьэтопротиворечиеразрешаетсяследующимобразомсильнаядеструктивнаяустремле
нностьдостоевскогокотораямоглабысделатьегопреступникомбылавегожизнинаправл
енаглавнымобразомнасамогосебявовнутрьвместотогочтобыизнутриитакимобразомв
ыразиласьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчерт
выявляющихсявегораздражительностимучительстванетерпимостидажепоотношени
юклюбимымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиство
вневажномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайший
добродушнейшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомыв
ыделилитрифактораодинколичественныйидвакачественныхегочрезвычайноповышен
нуюаффективностьегоустремленностькперверзиикотораядолжнабылапривестиегокс
адомазохизмуилисделатьпреступникомиегонеподдающееесяанализутворческоедарова
ниетакоесочетаниевполнемоглобысуществоватьибезневрозаведьбываютжестопроце
нтныемазохистыбезналичияневрозовпосоотношениюсилпритязаниипервичныхпозы
вовипротивоборствующихимторможенийприсоединяясюдавозможностисублимиров
аниядостоевскоговсеещеможнобылобыотнестикразрядуимпульсивныххарактеровно
положениевещейзатемняетсяналичиемневрозанеобязательногокакбылосказаноприда
нныхобстоятельствахновсежевозникающеготемскореечемнасыщенноеосложнениепо
длежащеесостороныческогояпреодолениюневрозэтотолькознактогочтоятакой
синтезнеудалсячтоонприэтойпопыткепоплатилосьсвоимединствомвчемжевстрогом
смыслепроявляетсяневроздостоевскийназывалсебясамидругиетакжесчиталиегоэпиле
птикомнатомосновании чтоонбылподвержентяжелымприпадкамсопровождавшимися
потерейсознаниясудорогамиипоследующимупадочнымнастроениемвесьмавероятноч
тоэтатакназываемаяэпилепсиябылалишьсимптомомегоневрозакоторыйвтакомслучае
следуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтоспо
лнойуверенностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихп
рипадковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныавовторых
потомучтопониманиесвязанныхсэпилептоидными припадкамиболезненныхсостояни
йостаетсянеясныма

Висновок:

В ході лабораторної роботи ми здобули навички частотного аналізу. Ми зрозуміли, що цей шифр складніше зламати аніж шифр Віженера, бо існує велика кількість потенційних ключів, за допомогою яких ми можемо розшифрувати текст та перевірити його на змінстовність.

Після виконання відповідних кроків ми отримали фрагмент п’єси «Буря» В.Шекспіра.