Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ No3
Криптоаналіз афінної біграмної підстановки

Виконали: Бойко Т. Я.

Хандрос А. В.

Група: ФБ-02

Київ – 2023

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 No1, 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.

- Знайдемо найчастіші біграми у шифротексті

Ними виявилися біграми ['ээ', 'вд', 'чф', 'цг', 'гн']

- У файлі rus.py реалізовано алгоритм перевірки того чи є набір символів змістовним текстом російською мовою
- Знайдемо всі можливі ключі, шляхом перебору з'ясовуємо, що наша шукана пара – це [314, 34]
- Розшифровуємо

Зашифрований текст:

```
ттгрэцрюфмнйбмйшугдээдэибггэдайжаищуикггуоитлчмтлвшаэвмхдвдлгцчцмбпврыэггзухлураятаиэншчфэчучкшт
фьээукщтбцнчфвшяфнрагрэцрцлцэюоксбмчфцгссошпруйедйгцгрэчсммцлжлочщетйсегрхчяэйекааэндвдэчбоцгзгдэ
ыуирщцээятглплычкчедйгцгчдфэучюшщясеплэнйфюфюбмйячвдогяфруопогшэпбмйячюоаэсмплизфрюбдукжюдээщшсву
рятаэггшйячбдйгьойсегммцшмэцгпмкаурюбщпдуяфйшлнрсээпблвтфцшкуцншмймщяээжсшшщятгдэцгчббйядогцоцггн
вриэоеканыклгнурюбдухжогууэчцдябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэаэнссрелуртукжэсфнйфгдэ
ээсглкчрзяаьйемщпмэумвдкгсгнчлщвшээалжвурдуопогруопогруопогрухсопогбггнчфьдечхшюбнргдфпчбфэкдчтйгг
йщнрдуиээдиэвнчфщзгрвштфвешыэшочйшяаяффдкчвчтшаиешшившэдечлфюфэнветйячыяюшмэсдггснаяээюгсеелфчкпо
гюггнодядкчешфчывээечогьоуэучжоьэхшгчэйжутйггдсэдшшветйячыяцгцлнрэссназвштэумэтогжлэеблэеишлтдгфш
врхлячщшцнбйесгнфртййбмйсстчжокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцдщркжцлураяючржапюфвштэчяьорэт
лурюфнрагкдээцгрэтлурфчычжлиекаэнчфьйзйлуирсмчфцгячьээйуиагшйдрйшиэпувдюшшишаыэмсвдхтгэкчьчэйыпнр
мйчсартйфдчстгщшаээйрэыэчйхялущшдуопогошээалжвурээыунрбдяуэчждэсетьдечнпзякяцггпмэтссхбмйячюцгд
эявжкйчггедоддэявжкаиягячеэюшуркйтеопечкгсшцлучщшазелурчбезвчпмцлуруйячэрдшртклуйлрфмйшймплэеггдб
уйишртгбцшнэгтждтхуэвчээгтждюгэдссммюфябцнчфцгфэшмйсссшвриэяэчэсеплэнэвээятрэаржуснцзшуснвдцэюои
эгмкаурмйцзнрушдуэчтоэчггаувймйсеябчфцньэцдогцояфюфтйкгюгогрэпутфээпбфэпутфаярссгжемйээрэврзюйдеч
дэллцявчяаиечмбэкдрэцрябмйэшфунчгфшйтеюнтйугюоибдуиэнгждятгльчькснтбитчйэчувюдгнцчыэлгвдфечфучжеу
ыкчяэьйусигджуиаяьожчвшлухжвдгэопогылээесвдлуэдэсвдцорэцгжехлвчкдбмюгягшшчфбэреапопечээжечбитоген
чфезфрюйэчлмэсглсгвдугггждцгврзюыщкдкгюдфбцдешймплндешйшуйэчлгкджлаыэшьяыэфпечрэюгеджчиюуруйогцэм
йэчычюшдчялкуггетгмвшеншигнвевшззумшутэкдцрйшкльчькирфпвддбэнушмэучжолвэшйфиэбдяучфзснчгнуявдшчпэ
фшуиуйягвдюбэеяукчыээээтждээнчячщшнфйшймэтвчимыщьдечвдэщезюнэнирхджбнряэаэзгэчвдэчучкшзьшчьччсыэф
печцгэчггауыщрэпмцдштйгвдкгучвдйэьоятцньюятчучфтйкгюгогттгтвштйндтгогьйьэуицэюохэнечмэечмлнчфишмб
мйээпуяищшсннрфмдуезггьоаягэрнщпчфурэвэжюдчсччусцэчяьогтччхштэйэссвшщзцлфчюрвууиыйтффедаюнчбтйиэг
нушкмээкчещфчкпечкмщпсгвштуйскбуяэдэйслцнэрдшбййббйьоээюоыэчскбцдечфучфширчяэлгыэумнрлвдлюмлсечиб
чфкдьовшябфэцрхчычялиелгвдячтчтогнуявдтчцчввэертдйфруцээщштфьюыэрзюбядгнпмшипчлмздцгопфсучтчайтею
нбпвчюегмьйцнкчдгяэтажюэеыэшоашсвйшураяплггйнчфныжвиявчяэцнсссгдяэсаэкгцгвдюгпдвшиэвнйсцэчйфшцлчд
ждвдгнеяждчслшнфцлогбшнфюгягйэдйсрхжртбаирэшлщюгфэщруиплггчзгрчдфэюдшдтлфруйетчзубээеяяауряэфэедт
гтгьйфпсгяэьэцдогыняцээлукчонвштбфэйэедмтяуазцдзсбшлвььсштфвравччмзвджмвштбдуйэедьоцнээяэынвежучф
пчлмплюйтеыщлунрбшьзчетйьчшнюйдшцнчфдльчггршезгршылныэнцээывтйячщшщяшчсчедиэяэщпвшфмтэцгкгюгогцой
эаэшшшимээйрэвчешшигггтлурйшшицгсепьплггнгээшсятаэьйфпдузйшнярснвшкдучяэээцмчфкчещурмйжчяныйтеышыс
щгьчдфэеьорнплмйыэйгемчмогвяыдючвшэдечвчклччгнярснээцузсжчцчяэжекуяукжкгфруыурипфэлсээзшмэфечфртм
сягджаиойтеазшчьфнрршоилуурюмаикдыэцулзнрзжзэюшзйкгнчывээцггэятьойэфэчдпфурэвкмчфкдыэцулзнрзжэшаз
шусндбвеюнюэрэвдядючдфэеьорночяэтгвчжокгойзйтеэшкгдуцггуцстечфтфщзгрплээретфойтфярснвшжемйэсайжаа
пзяэсглйчыэитшчюорстэцгдфцнцдибыядэцгкчяэюггнелчдждщртбнфуййшяфбпогюгждюбцнчфжеэжвдэьедискчщрхчкл
```

Розшифрований текст:

мамапошламыть посудуитомотправилсязанейкаждыйзвукзвонложкиилитарелкигулкораздавалсявзнойномвечерне
мвоздухепотомонимолчапошливбольшуюкомнатуснялисдиванаподушкивдвоемраскрылиегоиразложиливедьнасамо
мделеэтобылвовсенедиванашироченнаякроватьмамапостелилаимсдугласомпостельловковзбилаподушкитомнача
лбылорасстегиватьрубашкуноонасказалапогодиминуткутомпочемунадотыкакаяточуднаямамонаопустиласьнаст
улносразужевсталаподошлакдвериипозвалаоназваласноваисновадугласдугдуугееголосуплывалвдушнуютьмуит
онулвнейбезвсякогоотклikадажеэхонеотвечалодугласдугласдугласдуууглаааастомсиделнаполуиегопронизыва
лхолодновиноймомубылонемороженоеинезимаинелетнийзнойонвиделмаматорастерянноозираетсятозакрываетгл
азастоитинезнаетчтоделатьиоченьволнуетсядасразувиднорастерянаиволнуетсяонаоткрыладверьверандышагн
улавтемнотуспустилась поступенькампрошлаподорожкеподкустысиренитомприслушивалсякеешагамонаопять поз
валамолчаниеонапозвалаещедваразатомвсесиделвкомнатевотсейчассдлиннойдлиннойузкойулицыдонесетсягол
осдугласаидумамнебеспокойсяяидунодугласнеотвечалтомдолгиедвеминутысиделглядянараскрытуюпостельнам
олчащеерадиоимолчащийпатефонналюстругдекакнивчемнебывалопоблескивалистеклянныевисюлькинаковеррасп
исанныйпунцовымиифиолетовымизавитушкамипотомнарочностукнулногойокровать чтобыпоглядеть будетлибольн

ооказалосьбольнодверьверандысоскрипомотвориласьимамасказалапойдемтомпройдемсякудапростопоулицеиде
монвзялеезарукуонипошлипосентджеймсстритасфальтподногамибылвсеещетеплыйсверчкистрекоталигромчепре
жнеговсгущавшейсятьмеонидошлидоугласвернулиидвинулисьпонаправлениюкзападномуоврагугдетопроплылавт
омобильсверкнулвдалифараминаулицахникакихпризнаковжизнинисветанидвижениякоегдепозадимерцалислабоо
свещенныеквадратыоконвтойсторонеоткудаонишлиневсеещелеглиспатьнооченьоченьмногиедомаужестоялибезо
гнейиспалиапереднекоторымитожетемныминакрылечкахсиделиихобитателиивполголосавеливечернюбеседукое
гденаверандахпоскрипываликачелихотьбыотецбылдомасказаламамаонасжималавсвоейбольшойрукерукутомануп
остойдаймнетолькодобратьсядоэтогомальчишкидушегубопятьвышелнаохотуонубиваетлюдейвсемгрозитопаснос
тьниктонезнаетгдеикогдаонвдругпоявитсявотклянусьпустьтолькодугпридетдомойяеготакотколочувекбудетп
омнитьонипрошлиещекварталитеперьстоялипередчернымсилуэтомнемецкойбаптистскойцерквинауглучепелстри
тигленроквсотнешаговзацерковьюначиналсяоврагтомужечуялегооттудатянулоканализационнойтрубойсгнивши
милистьямидушнымивлажнымзапахомсплошныхзеленыхзарослейоврагбылширокийизвилистыйонперерезалгородим
амавсегдаговорилачтоэтоиднемтонепроходимыедебриаужночьюкнемулучшеиблизконеподходитьоттогочторядом
церковьстрахидолжныбырассеятьсянотомувсеравнобыложутковэтотчастемнаябезединогоогонькаонаказаласьх
олоднойибесполезнойразвалинойнакраюоврагатомубыловсегодесятьлетонничеготолкомнезналосмертистрахеу
жасесмертьэтовосковаякуклавящикеонвиделеевшестьлеттогдаумерегопрадедушкаилежалвгробуточноогромный
упавшийястреббезмолвныйидалекийникогдабольшеоннескажетчтонадобытьхорошиммальчикомникогдабольшенеб
удетспоритьополитикесмертьэтоегомаленькаясестренкаоднаждыутромемубыловтовремясемьлетонпроснулсяза
глянулвееколыбелькуаонасмотритпрямонанегозастывшимислепымисинимиглазамиапотомпришлилюдииунеслиеев
маленькойплетенойкорзинкесмертьэтокогдаонмесяцспустястоялвозлееевысокогостульчикаивдругпонялчтоон
аникогдабольшенебудеттутсидетьнебудетсмеятьсяилиплакатьиемууженебудетдосадночтоонародиласьнасветэ
тоибыласмертьиещесмертьэтодушегубкоторыйподкрадываетсяневидимкойипрячетсязадеревьямиибродитпоокру
геивыжидаетиразилидвавгодприходитсюдавэтотгороднаэтиулицыгдевечерамивсегдатемночтобыубитьженщинуз
апоследниетригодаонубилтрехэтосмертьносейчастутнепростосмертьвэтойлетнейночиподдалекимизвездамина
негоразомнахлынуловсечтооониспыталвиделислышалзавсюсвоюжизньионзахлебывалсяитонулонисошлистротуара
изашагалипопротоптаннойусыпаннойщебнемтропинкепообестороныгусторосласорнаятраваивнейгромконеумолч
нотрещалисверчкитомпослушношелзаматерьюбольшойхрабройпрекраснойегозащитницейотвсегосветатаквдвоем
онишлиишлиивотостановилисьнасамомкраюцивилизациивоврагздесьвэтойпропастипосредичернойчащобывдругсо
средоточилосьвсечегоонникогданеузнаетинепойметвсечтоживетбезыменноевнепрогляднойтенидеревьеввудуш
ливомзапахегниенияаведьонисматерьюздесьсовсемоднииеерукадрожитдадрожитемунепочудилосьноотчегомама
ведьбольшесильнееумнееегонеужелиионатожечувствуетэтунеуловимуюугрозутозловещеечтозатаилосьтамвниз
уисейчасвыползетизтемнотызначитможновырастиивсеравнонестатьсильнымзначитстатьвзрослымвовсенеутеше
ниезначитвжизнинетприбежищанеттакойнадежнойцитаделичтоустоялабыпротивнадвигающихсяужасовночисомне
нияразрывалиегомороженоевновьобожглоемухолодомгорловсевнутрипохолоделопоспинепошелморозоледенелир
укииногиемувдругсталоооченьзябкоточновновьналетелизпрошлогодекабрьскийветертаквотоночтозначитэтоуч
астьвсехлюдейкаждыйчеловекдлясебяодинединственныйнасветеодинединственныйсампосебесредивеликогомно
жествадругихлюдейивсегдабоитсявоткаксейчаснузакричишьстанешьзватьнапомощькомукакоеделотьмапоглоти
тводномгновеньеодночудовищноеледенящеемгновеньеивсеконченоещезадолгодорассветазадолгодотогокакпол
ицейскиеначнутпрощупыватьсвоимифонарикамитемнуюрастревоженнуютропинкуинанейзашуршитщебеньподногам
илюдейкоторыевсмятенииикинутсянапомощьидажееслионисейчастольковпятистахшагахоттебяаужнавернотаконо
иестьтемныйприбойможетзахлестнутьзатрисекундыиотнятьутебявсетвоидесятьлетижизньэтоодиночествовнез
апноеоткрытиеобрушилосьнатомакаксокрушительныйудариопзадрожалмаматожеодинокавэтуминутуейнечегонад
еятьсянинасвятостьбраканиназащитулюбящейсемьининаконституциюсоединенныхштатовнинаполициюейнеккому
обратитьсякромесобственногосердцаавсердцесвоемонанайдетлишьнеодолимоеотвращениеистрахвэтуминутупе
редкаждымстоитсвоятолькосвоязадачаикаждыйдолженсамеерешитьтысовсемодинпоймиэторазинавсегдатомпрог
лотилкомокзастрявшийвгорлеиприжалсякматеригосподинедайейумеретьмолилоннеделайнамничегоплохогопапа
придетссобраниячерезчасиеслидоманикогонебудетматьдвинуласьпотропинкевдикуючащумамтызадуганебойсяд
рожащимголосомсказалтомснимничегонеслучилосьтызанегонебойсяснимничегонеслучилосьонвсегдавозвращае
тсяэтимпутемголосматеризвенелотнапряженияясторазговорилаемуходидругойдорогойноэтипроклятыемальчиш
кивсеравнолезутнапроломкогданибудьонпойдеттудаибольшеневернетсябольшеневернетсяэтоможетозначатьчт
оугоднобродягипреступникитьманесчастныйслучайаглавноесмертьодинвовсейвселеннойнасветемиллионтаких
городишекивкаждомтакжетемнотакжеодинококаждыйтакжеотвсегоотрешенвкаждомсвоиужасыисвоитайныпронзит
ельныезаунывныезвукискрипкивотмузыкаэтихгородишекбезсветаносомножествомтенейакакоенеобятноенепоме
рноеодиночествоаневедомыеоврагичтозасасываюткактрясинажизньвэтихгородишкахпоночамоборачиваетсялед
енящимужасомразумусемьедетямсчастьюсовсехсторонгрозитчудищеимякоторомусмертьматьсноваргромкопозвал
автемнотудугласдугивдругобапочувствовaличтотослучилосьсверчкиумолклисталосовсемтихоонинезналчтобы
ваеттакаятишинабеспредельнаябездыханнаятишинаотчегозамолчалисверчкиотчегокакаяэтомупричинапреждео
ниникогданеумолкалиникогдазначитзначитсейчасчтотослучитсяказалосьоврагнапрягаетсвоичерныемышцывби
раетвсебявсесилыспящихгородковифермнамногиемиливокругвеликаятишинапропитанныхросойлесовидолининак
атывающихсякакприбойхолмовгдесобакизадравмордывоютналунувсясобираласьстекаласьстягиваласьводнуточ
куивсамомсердцетишиныбылионимамаитомвотсейчассиюминутучтотослучитсячтотослучитсясверчкивсемолчатз
вездыопустилисьтакнизкочтокажетсяпротянирукуинапальцахостанетсяпозолотаихнесчестьзвездонижаркиеко
лючиевсерастетразбухаеттишинавсеострейнапряженнейожиданиеохкактемнопустыннокакбесприютноивдругдал
екодалекозаоврагомголосяздесьмамидумамаисновамамамамидушлепшлепшлепмчатсяногивтеннисныхтуфляхподн
уоврагасхохотомнесутсятроемальчишекбратдугласчарливудмениджонхафбегутхохочутзвездывзвилисьвверхто
чнодесятьмиллионовужаленныхулитоквтянулисвоирожкисверчкизастрекоталитемнотаотступалаиспуганнаяоша
рашеннаязлобнаяотступилапотеряваппетитведьонасовсемужесобраласьпоживитьсяивдругейтакгрубопомешали
икогдатемнотаотхлынулаточноволнавовремяотливаизнеевозниклисмеясьтроемальчишекмамтомприветисразуво
кругзапахлодугласомведьотнеговсегдапахнетпотомтравойдеревьямиветвямииручьемвампредстоитпоркамолод
ойчеловекобявиламамаотеестраховиследанеосталосьтомзналонаникогдавжизиникомупроэтонерасскажетнико
гданострахэтотнавсегдаостанетсяунеевдушеивдушетоматожетемнойлетнейночьюонишлидомойспатькакхорошоч
тодугласживойкакхорошоанаоднусекундутамнакраюоврагаемуподумалосьгдетодалекопосмутномуозаренномулу
нойлесунадвиадукомпотомвнизуподолинепрогрохоталпоездонотчаянносвистелточнобезыменныйжелезныйзверь
заблудилсявночитомулегсявпостельрядомсбратомвесьдрожаонприслушивалсякэтомусвистуидумалдалекодалек

отамгдесейчасмчитсяпоезджилихдвоюродныйбратиумеротвоспаленияслегкихмноголетназадвотвтакуюженочьдуг
ласлежалрядомотнегопахлопотомиэтобылокакволшебствотомпересталдрожатьтолькодвевещиязнаюнавернякаду
гпрошепталонкакиеодначтоночьюужаснотемноадругаяеслимистерауфманкогданибудьвсамомделепостроитмашин
усчастьясоврагомейвсеравнонесовладатьдугласнемногоподумалповторичтотысказалониумолклинаулицевнеза
пнораздалисьшагиближеближевотониужеподдеревьямивозледоманатротуаремамасосвоейкроватинегромкосказа
лапапаидетинеошибласт

Висновок:

Виконуючи цю лабораторну роботу, були закріплені навички частотного аналізу тексту на прикладі шифру афінної підстановки. Також був розроблений механізм розпізнавання російської мови.