НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:
студенти групи ФБ-32
Кошикова Дар'я
Сажко Олена

Мета роботи:

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

Порядок виконання роботи:

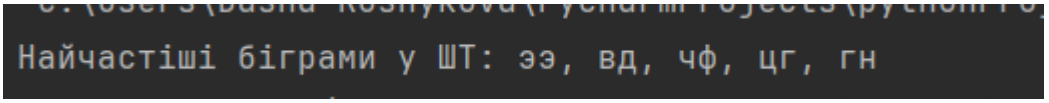
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно 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).

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

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 (варіант 9)

1) ШТ знаходиться у text.txt. Першим кроком розбиваємо текст на біграми (що не перетинаються) та знаходження п'яти найчастіших:



Відомі п'ять найчастіших біграм російської мови: ст, но, то, на, ен.

Таким чином, під час атаки розглядалися всі можливі зіставлення між цими двома множинами (5×5 = 25 комбінацій біграм, у кожній перевірялися перестановки — всього 400 пар X/Y).

Далі виконувалось відновлення параметрів ключа афінного шифру — коефіцієнтів a та b.

Для кожної пари біграм (однієї з мови та відповідної з шифртексту) програма розв'язувала систему конгруенцій:

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

На основі цієї системи обчислювались можливі значення a та b, що описують афінне перетворення для даних біграм.

У лог-файлі steps.txt зберігаються усі обчислення:

```
A=934, B=667 → a_solutions=[438]
fail (a=438, b=351)
A=934, B=48 → a_solutions=[105]
fail (a=105, b=207)
A=934, B=627 → a_solutions=[831]
fail (a=831, b=469)
A=934, B=750 → a_solutions=[79]
fail (a=79, b=875)
A=934, B=619 → a_solutions=[333]
fail (a=333, b=829)
A=934, B=913 → a_solutions=[856]
fail (a=856, b=250)
A=934, B=579 → a_solutions=[726]
fail (a=726, b=947)
A=934, B=171 → a_solutions=[314]
pass (a=314, b=34)
```

Після повного перебору всіх комбінацій (5×5 пар біграм і їх перестановок) було:

```
Перебрано пар X/Y: 400, отримано кандидатів ключів: 174
Знайдений ключ: a=314, b=34
```

Для кожного кандидата (a, b) виконувалося дешифрування шифртексту.
Програма перевіряла, чи схожий результат на російську мову — за такими критеріями:

- частота «о» > 10%, «а» > 7%;
- відсутні заборонені біграми (аь, оь, ьь, иь, йй тощо).

Як видно з логу:
pass (a=314, b=34) - цей ключ успішно пройшов перевірку — отже, дешифрований текст є осмисленим.

Розшифрований текст:

мамапошламытьпосудуитомотправилсязанейкаждыйзвукзвонложкиилитарелкигулкор аздавалсявзнойномвечернемвоздухепотомонимолчапошливбольшуюкомнатуснялисдиван аподушкивдвоемраскрылиегоиразложиливедьнасамомделеэтобылвовсенедиванашироче ннаякроватьмамапостелилаимсдугласомпостельловковзбилаподушкитомначалбылора сстегиватьрубашкуноонасказалапогодиминуткутомпочемунадотыкаякаяточуднаямам онаопустилась настулносразужевсталаподошлакдвериипозвалаоназваласноваисноваду гласдугдуугееголосуплывалвдушнуютьмуитонулвнейбезвсякогоотклика дажеэхонеотве чалодугласдугласдугласдуууглааастомсиделнаполуиегопронизывалхолодновиной томубы лонемороженоеинезимаинелетнийзнойонвиделмаматорастерянноозираетсятозакрыв аетглазастоитинезнаетчтоделатьиоченьволнуетсядасразувиднорастерянаиволнуетс яонаоткрыладверьверандышагнулавтемнотуспустилась поступенькам прошлаподорож кеподкустысиренитомприслушивалсякеешагамонаопятьпозвалам олчаниеонапозвалаещ едваразатомвсесиделвкомнатевотсейчассдлинной длинной узкой улицыдонесетсяголосду гласаидумамнебеспокойсяяидунодугласнеотвечалтомдолгиедвеминутысиделглядянарас крытуюпостельнамолчащеерадиоимолчащийпатефонналюстругдекакнивчемнебывало поблескивалистеклянныевисюлькинаковерраспи санныйпунцовымиифиолетовымизавит ушкамипотомнарочностукнулногойокроватьчтобыпоглядетьбудетлибольнооказалось больнодверьверандысоскрипомотвориласьимамасказалапойдемтомпройдемсякудапрос топоулицеидемонвзялеезарукуонипошлипосентджеймсстритасфальтподногамибылвс еещетеплыйсверчкистрекоталигромчепрежнеговсгущавшейсятьмеонидошлидоугласве рнулиидвинулисьпонаправлениюкзападномуоврагугдетопроплылавтомобильсверкнулвда лифараминаулицахникакихпризнаковжизнинисветанидвиженияко егдепозадимерцалисл абоосвещенныеквадратыоконвтойсторонеоткудаонишлиневсеещелеглиспатьнооченьо ченьмногиедомаужестоялибезогнейиспалиапереднекоторымитожетемнымина крылеч кахсиделиихобитателиивполголосавеливечернююбеседукоегденаверандахпоскрипывали качелихотьбыотецбылдомасказаламамаонасжималавсвоейбольшойрукерукутоманупос тойдаймнетолькодобратьсядоэтогомальчишкидушегубопятьвышелнаохотуонубивает людейвсемгрозитопасностьниктонезнаетгдеикогдаонвдругпоявитсяворотклянусьпусть толькодугпридетдомойяеготакотколочувекбудетпомнитьонипрошлиещеквартали теперьстоялипередчернымсилуэтомнемецкойбаптистскойцерквинауглучепелстритигленр оквсотнешаговзацерковьюначиналсяоврагтомужечуялегооттудатянулоканализационн ойтрубойсгнившимилистьямидушнымивлажнымзапахомсплошныхзеленыхзаро слейовр агбылширокийизвилистыйонпереререзалгородимамавсегдаговорилачтоэтоиднемтонепр оходимыедебриаужночьюкнемулучшеиблизконеподходитьоттогочторядомцерковьстр ахидолжныбырассеятьсянотомувсеравнобыложутковэтотчастемнаябезединогоогонь каонаказаласьхолоднойибесполезнойразвалинойнакраюоврагатомубыловсегодесятьлет онничеготолкомнезналосмертистрахеужасесмертьэтовосковаякуклавящикеонвиделее вшестьлеттогдаумерегопрадедушкаилежалвгробуточноогромныйупавшийястреббезм олвныйидалекийникогдабольшеоннескажетчтонадобытьхорошимма льчикомникогдабо льшенебудетспоритьополитикесмертьэтоегомаленькаясестренкаоднаждыутромемуб ыловтовремясемьлетонпроснулсязаглянулвееколыбелькуаонасмотритпрямонанегозаст ывшимислепымисинимиглазамиапотомпришлилюдииунеслиеевмаленькойплетенойкорз инкесмертьэтокогдаонмесяцспустястоялвозлееевысокогостульчикаивдругпонялчтоон

аникогдабольшенебудеттутсидетьнебудетсмеятьсяилиплакатьиемуужененебудетдоса
дночтоонародиласьнасветэтоибыласмертьиещесмертьэтодушегубкоторыйподкрады
ваетсяневидимкойипрячетсязадеревьямиибродитпоокругеивыжидаетиразилидвавгодп
риходитсюдавэтотгороднаэтиулицыгдевечерамивсегдатемночтобыубитьженщинуза
последниетригодаонубилтрехэтосмертьносейчастутнепростосмертьвэтойлетнейно
чиподдалекимизвездаминанегоразомнахлынуловсечтоониспыталвиделислышалзавсюсв
оюжизньионзахлебывалсяитонулонисошлистротуараизашагалипопротоптаннойусып
аннойщебнемтропинкепообестороныгусторосласорнаятраваивнейгромконеумолчнотр
ещалисверчкитомпослушношелзаматерьюбольшойхрабройпрекраснойегозащитницейо
твсегосветатаквдвоемонишлишишлишвотостановилисьнасамомкраюцивилизациивоврагз
десьвэтойпропастипосредичернойчащобывдругсосредоточилосьвсечегоонникогданеузн
аетинепойметвсечтоживетбезыменноевнепрогляднойтенидеревьеввудушливомзапахег
ниенияаведьонисматерьюздесьсовсемодниеерукадрожитдадрожитемунепочудилосьн
оотчегомамаведьбольшесильнееумнееегонеужелиионатожечувствуетэтунеуловимуюу
грозутозловещеечтозатаилосьтамвнизуисейчасвыползетизтемнотызначитможновы
растиивсеравнонестатьсильнымзначитстатьвзрослымвовсенеутешениезначитвжизн
инетприбежищанеттакойнадежнойцитаделичтоустоялабыпротивнадвигающихсяуж
асовночисомненияразрывалиегомороженоевновьобожглоемухолодомгорловсевнутрипох
олоделопоспинепошелморозоледенелирукииногиемувдругсталоченьзябкоточновновьна
летелизпрошлогодекабрьскийветертаквотоночтозначитэтоучастьвсехлюдейкаждый
человекдлясебяодинединственныйнасветеодинединственныйсампосебесредивеликогомн
ожествадругихлюдейивсегдабоитсяводкаксейчаснузакричишьстанешьзватьнапомощь
комукакоеделотьмапоглотитводномгновеньеодночудовищноеледенящеемгновеньеивсек
онченоещезадолгодорассветазадолгодотогокакполицейскиеначнутпрощупыватьсвоим
ифонарикамитемнуюрастревоженнуютропинкуинанейзашуршитщебеньподногамилюд
ейкоторыевсмятенишикинутсянапомощьидажееслионисейчастольковпятистахшагахо
ттебяаужнавернотаконоиестьтемныйприбойможетзахлестнутьзатрисекундыиотн
ятьутебявсетвоидесятьлетижизньэтоодиночествовнезапноеоткрытиеобрушилосьна
томакаксокрушительныйударионзадрожалмаматожеодинокавэтуминутуейнечегонад
еятьсянинасвятостьбраканиназащитулюбящейсемьининаконституциюсоединенныхши
татовнинаполициюейнеккомуобратитьсякромесобственногосердцаавсердцесвоемонан
айдетлишьнеодолимоеотвращениеистрахвэтуминутупередкаждымстоитсвоятолькос
воязадачаикаждыйдолженсамеерешитьтысовсемодинпоймиэторазинавсегдатомпрогл
отилкомокзастрявшийвгорлеиприжалсякматеригосподинедайейумеретьмолилоннедел
айнамничегоплохогопапапридетссобраниячерезчасиеслидоманикогонебудетматьдвину
ласьпотропинкевдикуючащумамтызадуганебойсядрожащимголосомсказалтомснимнич
егонеслучилосьтызанегонебойсяснимничегонеслучилосьонвсегдавозвращаетсяэтимпут
емголосматеризвенелотнапряженияясторазговорилаемуходидругойдорогойноэтипрок
лятыемальчишкивсеравнолезутнапроломкогданибудьонпойдеттудаибольшеневернется
большеневернетсяэтоможетозначатьчтоугоднобродягипреступникитьманесчастный
случайаглавноесмертьодинвовсейвселеннойнасветемиллионтакихгородишекивкаждом
такжетемнотакжеодинококаждыйтакжеотвсегоотрешенвкаждомсвоиужасыисвои
тайныпронзительныезаунывныезвукискрипкивотмузыкаэтихгородишекбезсветаносом
ножествомтенейакакоенеобятноенепомерноеодиночествоаневедомыеоврагичтозасас

ываюткактрясинажизньвэтихгородишкахпоночамоборачиваетсяледенящимужасомра
зумусемьедетямсчастьюсовсехсторонгрозитчудищеимякоторомусмертьматьсновагр
омкопозвалавтемнотудугласдугивдругобапочувствовваличтотослучилосьсверчкиумолкл
исталосовсемтихоонинезналчтобываеттакаятишинабеспредельнаябездыханнаятиши
наотчегозамолчалисверчкиотчегокакаяэтомупричинапреждеонининикогданеумолкалиник
огдазначитзначитсейчасчтотослучитсяказалосьоврагнапрягаетсвоичерныемышцывб
ираетвсебявсесилыспящихгородковифермнамногиемиливокругвеликаятишинапропитан
ныхросойлесовидолининакатывающихсякакприбойхолмовгдесобакизадравмордывоютн
алунувсясобиралась стекалась стягивалась воднуточкуивсамомсердцетишиныбылионим
амаитомвотсейчассиюминутучтотослучитсячтотослучитсясверчкивсемолчатзвезды
опустилисьтакнизкочтокажетсяпротянирукуинапальцахостанетсяпозолотаихнесчес
тьзвездонижаркиеколючиевсерастетразбухаеттишинавсеострейнапряженнейожида
ниеохкактемнопустыннокакбесприютноивдругдалекодалекозаоврагомголосяздесьмами
думамаисновамамамамидушлепшлепшлепмчатсяногивтеннисныхтуфляхподнуоврагас
хохотомнесутсятроемальчишекбратдугласчарливудмениджонхафбегутхохочутзвезды
взвилисьверхточнодесятьмиллионовужаленныхулитоквтянулисвоирожкисверчкизаст
рекоталитемнотаотступалаиспуганнаяошарашеннаязлобнаяотступилапотеряваппе
титведьонасовсемужесобраласьпоживитьсяивдругейтакгрубопомешалиикогдатемно
таотхлынулаточноволнавовремяотливаизнеевозниклисмеясьтроемальчишекмамтомпр
иветисразувокругзапахлодугласомведьотнеговсегдапахнетпотомтравойдеревьямивет
вямиручьемвампредстоитпоркамолодойчеловекобявиламамаотеестраховиследанеост
алосьтомзналонаникогдавжизниникомупроэтонерасскажетникогданострахэтотнавсе
гдаостанетсяунеевдушеивдушетоматожетемнойлетнейночьюонишлидомойспатькакх
орошочтодугласживойкакхорошоанаоднусекундутамнакраюоврагаемуподумалосьгдет
одалекопосмутномуозаренномулуной лесунадвиадукомпотомвнизуподолинепрогрохотал
поездонотчаянносвистелточнобезыменныйжелезныйзверьзаблудилсявночитомулегсяв
постельрядомсбратомвесьдрожаонприслушивалсякэтомусвистуидумалдалекодалекот
амгдесейчасмчитсяпоезджилихдвоюродныйбратиумеротвоспалениялегкихмноголетна
задвотвтакуюженочьдугласлежалрядомотнегопахлопотомиэтобылокакволшебствот
омпересталдрожатьтолькодвевещиязнаюнавернякадугпрошепталонкакиеодначтоноч
ьюужаснотемноадругаяеслимистерауфманкогданибудьвсамомделепостроитмашинусч
астьясоврагомейвсеравнонесовладатьдугласнемногоподумалповторичтотысказалониу
молклинаулицевнезапнораздалисьшагиближеближевотониужеподдеревьямивозледоман
атротуаремамасосвоейкроватинегромкосказалапапаидетинеошибласьа

Висновки

У цій роботі ми ознайомилися з принципом роботи афінного шифру біграм та навчилися проводити його криптоаналіз за допомогою частотного методу. Під час виконання завдання повторили, як знаходити обернені елементи за модулем за допомогою розширеного алгоритму Евкліда, і розв’язували лінійні рівняння. Також створили програму, яка автоматично знаходить ключ і розпізнає змістовний текст. У результаті вдалося знайти правильний ключ *(a = 314, b = 34)* та розшифрувати шифртекст.