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

Лабораторна робота №3

Виконали:
студенти ФІ-04

Кравченко Антон

Давидюк Данил

Київ – 2023

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 шифротексту (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,b) шляхом розв’язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

Хід роботи, опис труднощів, що виникали, та шляхів їх розв’язання

Ми розпочали з вивчення методичних вказівок та алгоритму розшифрування афінного шифру. Здійснили реалізацію необхідних допоміжних функцій для визначення ключа та розшифрування тексту. Зіткнулися з труднощами, пов'язаними із автоматичним розпізнаванням тексту, оскільки отриманий текст мав певні недоліки та помилки. Виявили шляхи вирішення цієї проблеми, використовуючи інші підходи до визначення ключа та аналізу тексту. У результаті успішно розшифрували текст та отримали змістовний результат.

Знайдені п’ять найчастіших біграм шифротексту

Була використана програма, що була реалізована для комп’ютерного практикуму №1. Результати для нового вхідного тексту (нашого варіанту) такі:

[("тд", 0.027353463587921848),
("рб", 0.018827708703374777),
("во", 0.01847246891651865),
("щю", 0.015985790408525755),
("кд", 0.01492007104795737)....]

Результати роботи

Зашифрований текст:

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоыом
хзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлх
йостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщюзншбхюэотйбавотдцюэшшылх
щюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозоихщюкцз
оюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдвоэо
мюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйб
ышкдэйюейосежхюбгцэюубйутодткдвощхщюющцяюстудвежюнхэджядшищвччощщвунойхзозпц
эфтмефпшхтдпощщщыкдвуозеойбдээстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзс
двеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэдохех
воубпзшбчхлыйбсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдют
етэтфтщютздйирэттднттюрюецтйвмшшзцтйищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцх
нрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднтжхщюжощщщыгцщоцпь
сждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвц
хндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеы
аншшвуйжышьтджфицхеогбшшанжхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрб
йекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэстйуэлетмюшюыхнцхтцпвотду
чеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесдвейхаирбтюзсжжйбщдд
ццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотддншддцбаабжукцеочтйхвюеыдйрббдфхд
йыжхшшшщаышиткчсняощщуогбажбфьащелбхшзцтйищцюнхктсджданершецшмбзнбрфоюбол
охехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощцвуэ
тегрбыюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбвотдбнкдютр
ртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщтокшеронцчшц
цнджфитджюкцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывю
щючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшц
лшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхбжйуолэттднттю
зсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхетжютдх
шкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруате
оахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбв
онстднбансюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсу
рржцзожюдюяюэоддтххгнхщюжбзнкофтждждцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухв
цщоыояоетктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшш

шухсугжднньыгррщюцйюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжу
ьжгажюпннъхыохзйзцвоыыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгц
фпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужь
кюдурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюа
бгххсййбргшзцтйищцюжхинфиывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажан
дйщеябруеыохпыыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкбьхвцньйбгц
шхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужх
щюююетнобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпю
шбхфньхытцодгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетшт
ехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцчшццнйиеыанвущоьылхн
цэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрб
гхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяе
вокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошу
чберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдйнищдгждцщоыо
ьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшммыдйрбс
учхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретхжвг
ажщаиашдбншдкцжхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбн
гцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбоцпштмыкдохьбгцфпибшшернбцюйек
длттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдрианлххнэйрбгхщгк
цеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднттюх
лдшшшитщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйб
яхщоцщаняюепмтцпжхофюекйухощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннб
цючотхтдэиыжюбдыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйе
рййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсд
веатлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеь
жкхшцтжпнгсштввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшщ
лшйотдухвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпоойерягрр
щюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюб
покйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэ
очоьбгцфпчочобоацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнт
фддйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбрущоьыйбрбитшхыошсзхтдстнтыбюлпюыы
еоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньщечощщвуйоюсзхыбух
ушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпкдьоицжувундэыдй
лдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнч
хеойхшисеетщхыощцсучдвукудйэюцнсесдверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогб
анохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцситцэюмхэшсурианлххнэйрбгхфодт
ююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияжьзвотдучяоехфдвукдюткйтцюмнт
жхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюкоушнбднеокоацях
жхитсюююйянбэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвот
кбфичхэюенмтцпжхофйуфюьювортнтфддйкдютгцитсдвейхагкцжуружхеогсослфчхшцщцыомтм
юитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюггжнбгхкудйэюждв
удрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдер
йетдажбйщтцпвотдучвцйудйпрэвщдшдэыдйут

Розшифрований текст:

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловек
авовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлиисследованиямне
удалосьещеустановитьдушевноепроисхождениевиныипотребностиискупленияноотнюдьнесуще
ственноединственныйлиэтоисточникпсихологическоеположениесложноинуждаетсявобяснения
хотношениемальчикакотцукакмыговоримамбивалентнопомимоненавистиизакоторойхотелосьб
ыотцакаксоперникаустранитьсуществуетобычнонекотораядолянежностикнемуобаотношениясл
иваютсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызываетвосхищение
хотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятств
иевопределенныймоментребенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстр
етилабысостороныотцанаказаниечерезкастрациюизстрахакастрациитоестьвинтересахсохранени
ясвоеймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустраненияотцапоск
олькуэтожеланиеостаетсявобластибессознательногооноявляетсяосновойдляобразованиячувства
винынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбутакназываемогоэдиповако
мплексаследуетоднаковнестиважноедополнениевозникаютдальнейшиеосложненияеслиуребенк
асильнееразвитконституционныйфакторназываемыйнамибисексуальностьютогдаподугрозойпот
еримужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсторонуженственностиб
олеетоготенденцияпоставитьсебянаместоматериилиперенятьееролькакобекталюбвиотцаодналишь
боязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчтоондолженвзятьнасебяикас
трированиееслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснениеобапорыв
аненавистькотцуивлюбленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоо
тненавистикотцуотказываютсявследствиестрахапередвнешнейопасностьюкастрацией влюбленн
остьжевотцавоспринимаетсякаквнутренняяопасностьпервичногопозывакотораяпосутисвоейсно
вавозвращаетсяктойжевнешнейопасностистрахпередотцамделаетненавистькотцунеприемлемой
кастрацияужаснакаквкачествекарытакиценылюбвиизобоихфактороввытесняющихненавистькот
цупервыйнепосредственныйстрахнаказанияикастрациисследуетназватьнормальнымпатогеничес
коеусилениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойустановкиярков
ыраженнаябисексуальнаясклонностьстановитсятакимобразомоднимизусловийилиподтвержден
ийневрозаэтусклонностьочевидноследуетпризнатьиудостоевскогоионалатентнаягомосексуальн
остьпроявляетсявдозволенномвидевтомзначениикакоеимелавегожизнидружбасмужчинамивегод
остранностинежномотношениихсоперникамвлюбвиивегопрекрасномпониманииположенийобяс
нимыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизего
произведенийсожалеюноничегонемогуизменитьеелиподробностионенавистиилюбвикотцуиоби
хвидоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанализечитателюпокажутся
безвкуснымиималовероятнымипредполагаючтоименнокомплекскастрациибудетотклоненсильне
евсегоносмеюуверитьчтопсихоаналитическийопытставитименноэтиявленияневсякогосомнени
яинаходитвнихключклюбомуневрозуиспытаемжеговслучаетакназываемойэпилепсиинашегопи
сателянонашемусознаниютакчуждытеявленияповластикоторыхнаходитсянашабессознательнаяп
сихическаяжизньуказаннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытеснени
яненавистикотцуновымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемя
постоянноеместоэтоотождествлениевоспринимаетсянашимянопредставляетсобойвнемособуюи
нстанциюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнаш
имсверхяиприписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецбы
лсуровнасильственжестокнашесверхяперенимаетотнегоэтикачестваивегоотношениикясноваво
никаетпассивностькоторойкаразнадлежалобыбытьвытесненнойсверхяталосадистическимяст
ановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашемявозникаетбольшаяпо
требностьвнаказанииияотчастиотдаетсебякактаковоевраспоряжениесудьбыотчастиженаходитуд

овлетворениевжестокомобращениинаснимсверхясознаниевинынаждаякараявляетсяведьвосновесв оейкастрациейикактаковаяосуществлениемизначальногопассивногоотношениякотцуисудьбавко нцеконцовлишьдальнейшаяпроекцияотцанормальныеявленияпроисходящиеприформированиис овестидолжныпоходитьнаописанныездесьанормальныенамещенеудалосьустановитьразграниче ниямеждунимизамечаетсячтонаибольшаярольздесьвконечномитогеприписываетсяпассивнымэл ементамвытесненнойженственностиищекакслучайныйфакторимеетзначениеявляетсяливнуша ющийстрахотецивдействительностиособеннонасильственнымэтоотносится кдостоевскомуфакте гоисключительногочувствавиныравнокакимазохистскогообразажизнимысводимкегоособеннояр ковыраженномукомпонентуженственностидостоевскогоможноопределитьследующимобразомос обенносильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяотза висимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкранееузнанн ымкомпонентамегосуществараннийсимптомприпадковсмертиможнорассматриватькакотождест влениесвоегоясотцомдопущенноевкачественаказаниясосторонысверхятызахотелубитьотцадабы статьотцомсамомутеперьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовикто мужетеперьтебяубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфантазиимужс когожеланияиодновременномазохистскимпосредствомнаказаниятоестьсадистическимудовлетво рениемобаяисверхяиграютрольотцаидальшевобщемотношениемеждуличностьюиобектомотцап рисохраненииегосодержанияперешловотношениемеждуяисверхяноваяинсценировканавторойсц енетакиеинфантильныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедает имвдальнейшемпищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитакимобраз омпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузломуотцустановит сяопаснымеслитакиевытесненныежеланияосуществляютсянаделефантазиясталареальностьювс емерызащитытеперьа

Ключ: (199, 700)

Опис розпізнавача:

Програма працює на основі аналізу індексу співставлення, який є метрикою схожості символів у тексті. Індекс співставлення обчислюється для розшифрованого тексту і порівнюється з нормованим значенням для кожної мови.

Основні кроки програми:

1. Задається зашифрований текст `text.txt`.
2. Визначається список символів алфавіту ALPH, які використовуються для розшифрування.
3. Функція `coi` обчислює індекс співставлення для розшифрованого тексту. Для цього проходиться по кожному символу зі списку ALPH і підраховує кількість його появ у тексті. За допомогою цих значень обчислюється індекс співставлення k за певною формулою.
4. Існує список ключів keys, які будуть використовуватись для розшифрування тексту.

5. Програма проходиться по кожному ключу зі списку keys і розшифровує текст за допомогою функції `decrypt_text`. Отриманий розшифрований текст зберігається у змінній `decoded`.
6. Перевіряється, чи є розшифрований текст порожнім. Якщо так, програма переходить до наступного ключа.
7. Обчислюється індекс співставлення для розшифрованого тексту `decoded` за допомогою функції `coi`.
8. Розраховується різниця між обчисленим індексом співставлення та нормованим значенням norm_I.
9. Якщо різниця менша за певне порогове значення, вважається, що мова розшифрованого тексту співпадає зі знайденою мовою, і виводиться розшифрований текст та відповідний ключ. Виконання програми завершується.
10. Якщо жоден з розшифрованих текстів не відповідає умовам, програма продовжує своє виконання до кінця без виведення результатів

Висновок:

В ході виконання цієї лабораторної роботи ми успішно набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки. Цей прийом аналізу допоміг нам відновити змістовний текст з зашифрованого повідомлення, використовуючи частотну структуру мови та статистику появи окремих символів.

Також, ми опанували прийоми роботи в модулярній арифметиці, зокрема знаходження оберненого елемента за модулем та розв'язування лінійних порівнянь за модулем. Ці навички дозволили нам виконувати обчислення з використанням арифметичних операцій над числами у модульному просторі, що є важливим у криптографії.

Отримані навички частотного аналізу та роботи в модулярній арифметиці допоможуть нам у подальших криптографічних дослідженнях та розв'язанні задач забезпечення безпеки даних. Ми освоїли необхідні інструменти та методи для аналізу та розкриття шифрів, що робить нас більш компетентними в галузі криптографії.