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

ЛАБОРАТОРНА РОБОТА №3
«Криптоаналіз афінної біграмної підстановки»

Варіант 9

Виконали:
студенти групи ФБ-04
Кравченко Владислав
та
Жмур Назар

Перевірив:
Чорний О.

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).

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. Написали необхідний функціонал, залучивши стандартні бібліотеки Пітона.
2. Найчастіші біграми шифротексту: тд, рб, во, щю, кд.
   В якості перевірки текст на змістовність взяли недопустимі біграми, оскільки це найлегший і найефективніший метод.

   Ключ a = 199, 700

   Зашифрований текст

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпво
ыомхзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжц
юлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщюзншбхюэотйбавотдцюэш
шылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозоихщ
юкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэд
воэомюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэ
вбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстудвежюнхэджядшищвччощщвунойхз
озпцэфтмефпшхтдпощщщыкдвуозеойбдээзстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоеохсгдю
млзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэд
охехвоубпзшбчхлыйбсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэ
кдютетэтфтщютздйирэттднттюрюецтйвмшшзцтйищщюеокцфпжюэддйкцвмчоьйнбрбйеинухяу
югкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднтжхщюжощщщыгц
щоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойеранн
бйейсвцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфо
ыойиеыаншшвуйжышьтджфицхеогбшшанжхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгц

зоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэстйуэлетмюшюыхнцхт
цпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесдвейхаирбтюзсж
жйбщдддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотдднщддцбаабжукцеочтйхвюеыдй
рббдфхдйыжхшшшщаышиткчсняощщуогбажбфьащелбхшзцтйищцюнхктсджданершецшмбзнб
рфоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюк
эфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбвот
дбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщток
шеронцчшццнджфитджюкцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкд
ютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоохлсбанднб
рыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхбжйуо
лэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжх
етжютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуа
жкбруатеоахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучих
хцхнрбвонстднбансюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантс
офогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтжджцжжйбвотдромхжюгбгцлхкссдкйрретфпас
йотдухвцщоыояоетктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмх
щюдшшшухсугждннььгррщюцйюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобх
дбдшжуьжгажюпнньхыохзйзцвоыыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцыш
шсажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьз
ньйбйужькюдурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюф
мэощняюабгххсййбргшзцтйищцюжхинфиывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэ
мюсуажандйщеябруеыохпыыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкбьх
вцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшж
ьгцвужхщюююетнобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсыл
жэыпюшбхфньхытцодгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищ
двеештехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцчшццнйиеыанвущ
оьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгн
хтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдв
еетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчет
щхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдйнищдгжд
цщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшмм
ыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзй
еретхжвгажщаиашдбншдкцжхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсю
пдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбоцпштмыкдохьбгцфпибшшер
нбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдрианлххнэй
рбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэт
тднттюхлдшшшитщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшп
дтушйбяхщоцщаняюепмтцпжхофюекйухощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэ
умйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднб
анщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэыв
юфюнэстсдвеатлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцре
тмхщюбеьжкхшцтжпнгсштввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеок
двопюшцлшйотдухвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпо
ойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщо
ыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбг
цфптцэочоьбгцфпчочобоацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютжд
кдртнтфддйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбрущоьыйбрбитшхыошсзхтдстнтыбю
лпюыыеоыывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньщечощщвуйоюс
зхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпкдьоицжуву
ндэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпй

хлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсесдвериалххнэйрбгхыянбитйюсуюгэшжььггж
нбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцситцэюмхэшсуриалххнэйр
бгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияжьзвотдучяоехфдвукдюткй
тцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюкоушнбднео
коацяхжхитсюююйянбэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюй
хцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфддйкдютгцитсдвейхагкцжуружхеогсослфчхшцщ
цыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюггжнбгхкуд
йэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнх
лхгтэдерйетдажбйщтцпвотдучвцйудйпрэвщдшдэыдйут

Розшифрований текст

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногоче
ловекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлиисследова
ниямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностиискупленияноотню
дьнесущественноединственныйлиэтоисточникпсихологическоеположениесложноинуждаетсяв
обясненияхотношениемальчикакотцукакмыговоримамбивалентнопомимоненавистииззакото
ройхотелосьбыотцаксоперникаустранитьсуществуетобычнонекотораядолянежностикнемуо
баотношениясливаютсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызы
ваетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтонаталкиваетсянак
рупноепрепятствиевопределенныймоментребенокначинаетпониматьчтопопыткаустранитьотц
акаксоперникавстретилабысостороныотцанаказаниечерезкастрациюизстрахакастрациитоесть
винтересахсохранениясвоеймужественностиребенокотказываетсяотжеланияобладатьматерь
юиотустраненияотцапосколькуэтожеланиеостаетсявобластибессознательногооноявляетсяосно
войдляобразованиячувствавинынамкажетсячтомыописалинормальныепроцессыобычнуюсудь
бутакназываемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдаль
нейшиеосложненияеслиуребенкасильнееразвитконституционныйфакторназываемыйнамибис
ексуальностьютогдаподугрозойпотеримужественностичерезкастрациюукрепляетсятенденцияу
клонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместоматерииперенять
ееролькакобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребено
кпонимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщ
инатакобрекаютсянавытеснениеобапорыванеНавистькотцуивлюбленностьвотцаизвестнаяпсих
ологическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследствиестрахапе
редвнешнейопасностьюкастрациейвлюбленностьжевотцавоспринимаетсякаквнутренняяопасн
остьпервичногопозывакотораяпосутисвоейсновавозвращаетсяктойжевнешнейопасностистрах
передотцамделаетненавистькотцунеприемлемойкастрацияужаснакаквкачествекарытакицены
любвиизобоихфакторовВытесняющихненавистькотцупервыйнепосредственныйстрахнаказани
яикастрациисследуетназватьнормальнымпатогеническоеусилениепривноситсякаккажетсялишь
другимфакторомбоязньюженственнойустановкиярковыраженнаябисексуальнаясклонностьста
новитсятакимобразомоднимизусловийилиподтверждений неврозаэтусклонностьочевидносле
дуетпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвиде
втомзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежномотношении
ксоперникамвлюбвиивегопрекрасномпониманииположенийобяснимыхлишьвытесненнойгом
осексуальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведенийсожалеюнон
ичегонемогуизменитьеелиподробностионенавистиилюбвикотцуиобихвидоизмененияхподвли
яниемугрозыкастрациинесведущемувпсихоаналисудьбавконцеконцовлишьдальнейшаяпроек
цияотцанормальныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаопис
анныездесьанормальныенамещенеудалосьустановитвляетсяливнушающийстрахотецивдейств
ительностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключительногочувс
твавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраженномукомп
онентуженственностидостоевскогоможноопределитьследующимобразомособенносильнаяби

сексуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяотзависимостиотчре звычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкранееузнаннымкомпонент амегосуществараннийсимптомприпадковсмертиможнорассматриватькакотождествлениесвое гоясотцомдопущенноевкачественаказаниясосторонысверхятызахотелубитьотцадабыстатьотцо мсамомутеперьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужете перьтебяубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфантазиимужского желанияиодновременномазохистскимпосредствомнаказаниятоестьсадистическимудовлетвор ениемобаяисверхяиграютрольотцаидальшевобщемотношениемеждуличностьюиобектомотца присохраненииегосодержанияперешловотношениемеждуяисверхяноваяинсценировканавтор ойсценетакиеинфантильныереакцииэдиповакомплексамогутзаглохнутьеслидействительность недаетимвдальнейшемпищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитак имобразомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузломуот цустановитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделефантазиясталаре альностьювсемерызащитытеперьа

Висновки:

В лабораторній роботі освоїли та закріпили навички програмування в модульній алгебрі, дослідили алгоритм взламу біграмної афінної підстановки.