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

Симетрична криптографія
Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки
Варіант 3

Виконали:
студенти групи ФІ-94
Коробан Ольга

Перевірив:
Чорний О.М.

Київ 2022

ЗАГАЛЬНІ ВІДОМОСТІ

Мета роботи

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

Постановка задачі

Написати програму для шифрування та розшифрування тексту шифром Віженера, а також обчислення індексу відповідності тексту.

Хід 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 No1, знайти 5 найчастіших біграм запропонованого шифротекст у (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифротекст у (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).

Труднощі, що виникали:

1) Не очевидним, хоча і природнім при відсутності результату було збільшити кі-сть біграм для співставлення, а не спроба перебрати усі варіанти (що, до речі дало правильну відповідь, хоча і заняло багацько часу). В цілому проблем дана задача не викликала.

Результат:

```
max bigrams for language
0.0167 17 18
0.0151 16 0
0.0142 13 8
0.0133 5 13
0.0123 0 13
0.0119 13 0
0.0111 14 2
0.0108 13 14
0.0106 16 5
0.0101 10 14
max bigrams for crypt text
0.0274 18 4
0.0188 16 1
0.0185 2 14
0.0160 25 29
0.0149 10 4
0.0146 5 18
0.0128 3 22
0.0128 6 21
0.0128 3 22
0.0128 6 21
```

```
199 700
отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекавовсякомслучае

Process finished with exit code 0
```

Для відсікання точно не коректних результатів перевірялася наявність у тексті біграм виду голосна+м’який знак та приголосна+’й’(ці дві комбінації гарантовано не існують у мові) - що було досить ефективно навіть при повному переборі усіх ключів (31^4) - на екран було виведено близько 200 відповідей, що є досить малою кі-стю.

Шифрований текст:

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднх
цпвоыомхзотхэтоовцлшвуджозчх
йбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужхр
иажгцфхзхжцитвожюфпксщхибухкйзю
жмьгнхщюзншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэля
юждзютдлзщюаыпюнозоуюмхэшухэозо
ихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсу
жушюстлхэдвоэомюфожхетжютдцюгршшкд
эйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэйюейосежх
юбгцэюубйутодткдвощхщющцяюстуд
вежюнхэджядшищвччощщвунойхзозпцэфтмефпшхтдпощщщыкдвуозеойбдэээстсдоож
миврбгхнойхзозпцэцэфпэтщощюэоео
хсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнх
лхыбэлфошхэдохехвоубпзшбчхлыйб
суодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщ
ютздйирэттднттюрюецтйвмшшзцтй
ищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдих
ктщюжонжсиодгуоддйучяожстднт
жхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхш
цжосбанолхжжоойераннбйейсвцхндн
шбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыой
иеыаншшвуйжышьтджфицхеогбшшан
жхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхд
йержюкшйбтдщдзщяоыбэлгтфдэйетзэ
стйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднт
тющсзйэысесдвейхаирбтюзсжжйб
щддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотдднщддцбаабжукцеочтйхвюе
ыдйрббдфхдйыжхшшшщаышиткчсняо
щщуогбажбфьащелбхшзцтйищцюнхктсджданершецшмбзнбрфоюболохехвоаыйбсучхбз
еойбйотгрбарбдкбзцбаююэттдвюко
стщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюц
одтэоаэстжхетжютдхшкдыспнкчнжрбво
тдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющ
ощщтокшеронцчшццнджфитджюкцтй
вмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдве
эткнгстйрбмежоатсбгцфпбхьньзвоыо
эозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохй
ощщжунхктсджхетжютдхшкдысжх
кйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеок
ояншдкцмеввнмжхетжютдхшкдысбхьнэл

жхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщ
юмхэшухжцлжрбгхкйпнвопюшцлшшш
этихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюы
хнцхтцпетщцжжйбвотддцитвожюшцбд
шшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтжджцжжйбвотдромхжюгб
гцлхкссдкйрретфпасйотдухвцщоыояо
етктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшш
шухсугждннььгррщюцйюгдткуюгают
мютхыойотдntыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоыыйб
сунбцюэозоихщюмолесбсуммяюепдэйх
сбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсудйхюххыокйз
ювнфирбюлчозтлхтбйбьзньйбйужь
кюдурбщдфхгжеыникоьбгцэюйбрбдntцэюлжгажющощщкющанмжюйорршхжхщюфмэ
ощняюабгххсййбргшзцтйищцюжхинфиывйу
гнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдз
юшхыбфшвуйжышэшзцтйищцювснхео
кшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыб
мкэюцнлхщюцнжхвцлшжьгцвужхщююует
нобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпю
шбхфньхытцодгжабйбхфйужцбретщюуд
шшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшю
еыюлбссэтфтыбрудэщхжхтцмхрыонцч
шццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдл
зеоушйбяхщоцщанкдьгнхтдьжрбгх
чощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвее
тнюяевокйфитдднсесдчобоэнжхфо
човсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошучберончхпджьмтжд
кюхцитцщвчетнюицтхшмююкйеытц
ончхшхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэ
ьцайанетпюцптдтхнгкцеоубхфкцтхшммы
дйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйо
лэтзйеретхжвгажщаиашдбншдкц
жхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхину
хчгрбтдтхыбхызцпюибруибхфйуцнбр
щюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюы
эйсгрбгхшсшпцэкдлттдкгрбвмнищдри
анлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхш
поосбанкцоохлэттдnттюхлдшшш
итщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйб
яхщоцщаняюепмтцпжхофюекйухощйекд
ютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкб
уофюьтыбвхпикцутвоэуажкбвхетшхзх
жхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппик
цбнщожхвбвущджьэывюфюнэстсдве

атлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмх
щюбеьжкхшцтжпнгсштввюлтднт
нойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвцщохсг
тфдньзюэшкчаюйхцпвоыойсвцхндн
шблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвуч
швуэожхэдюгрбтдтхыбгцэюйотдух
вцщоыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохц
йзцэозоихыбгцфптцэочоьбгцфпчочо
боацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйш
юыхнцхтцпвотдсуыищаднсейузйнбьх
дретыбрущоыйбрбитшхыошсзхтдстнтыбюлпюыыеоыывюатошанкудйэюфоюбэйзцкуод
вюстфпэтщоеовикцхнлхщюкцооньще
чощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсию
асцитфпкдьоицжувундэыдйлдюойхфб
пойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчх
еойхшисеетщхыощцсучдвукудйэю
цнсесдверианлххнэйрбгхыянбитйюсуюгэшжьыггжнбйеяогбанохшхыбвуерюмтцшцсюь
ыгцохэцхнвуетэтфтщюбдухтддцси
тцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгх
шхвияжьзвотдучяоехфдвукдюткй
тцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюко
ушнбднеокоацяхжхитсюоюйянбэюцпчэ
дйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенм
тцпжхофйуфюьювортнтфддйкдютгцит
сдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбр
бднтцфпйотдухвцщоыощощщюггжнб
гхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывк
цхнсеудвеетнхлхгтэдерйетдажбй
щтцпвотдучвцйудйпрэвщдшдэыдйут

Розшифрований текст:

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельного
человекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлии
сследованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностииску
плениянооотнюдьнесущественноединственныйлиэтоисточникпсихологическоеположен
иесложноинуждаетсявобъясненияхотношениемальчикакотцукакмыговоримамбивалентн
опомимоненавистииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобыч
нонекотораядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотел
осьбызанятьместоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотому
чтохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймом

ентребенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысосто
роныотцанаказаниечерезкастрациюизстрахакастрациитоестьвинтересахсохранениясвое
ймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустраненияотцап
оскольку этожеланиеостаетсявобластибессознательногооноявляетсяосновойдляобразов
аниячувствавинынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбутакна
зываемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдальней
шиеосложненияеслиуребенкасильнееразвитконституционныйфакторназываемыйнамиб
исексуальностьютогдаподугрозойпотеримужественностичерезкастрациюукрепляетсяте
нденцияуклонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместом
атериипереняттьеероликакобекталюбвиотцаодналишьбоязнькастрациидолаетэтуразвязк
уневозможнойребенокпонимаетчтоондолженвзятьнасебяикастрированиеслионхочетб
ытьлюбимымотцомкакженщинатакобрекаютсянавытеснениеобапорываненавистькотцу
ивлюбленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотненави
стикотцуотказываютсявследствиестрахапередвнешнейопасностьюкастрациейвлюбленн
остьжевотцавоспринимаетсякаквнутренняяопасностьпервичногопозывакотораяпосутис
воейсновавозвращаетсяктойжевнешнейопасностистрахпередотцамделаетненавистькот
цунеприемлемойкастрацияужаснакаквкачествекарытакиценылюбвиизобоихфакторовв
ытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияикастрацииследу
етназватьнормальнымпатогеническоеусилениепривноситсякаккажетсялишьдругимфак
торомбоязньюженственнойустановкиярковыраженнаябисексуальнаясклонностьстанов
итсятакимобразомоднимизусловийилиподтверждений неврозаэтусклонностьочевиднос
ледуетпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволен
номвидевтомзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежн
омотношениихсоперникамвлюбвиивегопрекрасномпониманииположенийобяснимыхли
шьвытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизего
произведенийсожалеюноничегонемогуизменитьеелиподробностионенавистиилюбвико
тцуиобихвидоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанализечит
ателюпокажутсябезвкуснымиималовероятнымипредполагаючтоименнокомплекскастра
циибудетотклоненсильнеевсегоносмеюуверитьчтопсихоаналитическийопытставитимен
ноэтиявленияявневсякогосомненияинаходитвнихключклюбомуневрозуиспытаемжеегов
случаетакназываемойэпилепсиинашегописателянонашемусознаниютакчуждытеявлени
явовластикоторыхнаходитсянашабессознательнаяпсихическаяжизньуказаннымвышене
исчерпываютсявэдиповомкомплексепоследствиявытесненияненавистикотцуновымявля
етсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянноеместоэт
оотождествлениевоспринимаетсянашимянопредставляетсобойвнемособуюинстанциюп
ротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашим
сверхяиприписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслио
тецбылсуровнасильственжестокнашесверхяперенимаетотнегоэтикачестваивегоотноше
ниикясновавозникаетпассивностькоторойкакразнадлежалобыбытьвытесненнойсверхяс
талосадистическимястановитсямазохистскимтоестьвосновесвоейженственнопассивны
мвнашемявозникаетбольшаяпотребностьвнаказанииияотчастиотдаетсебякактаковоевра
споряжениесудьбыотчастиженаходитудовлетворениевжестокомобращенииснимсверхя
сознаниевиныкаждаякараявляетсяведьвосновесвоейкастрациейикактаковаяосуществле
ниемизначальногопассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяп

роекцияотцанормальныеявленияпроисходящиеприформированиисовестидолжныпоход
итьнаописанныездесьанормальныенамещенеудалосьустановитьразграниченияміждуни
мизамечаетсячтонаибольшаярольздесьвконечномитогеприписываетсяпассивнымэлеме
нтамвытесненнойженственностиищекакслучайныйфакторимеетзначениеявляетсяливн
ушающийстрахотецивдействительностиособеннонасильственнымэтоотносится кдостое
вскомуфактегоисключительногочувствавиныравнокакимазохистскогообразажизнимыс
водимкегоособенноярковыраженномукомпонентуженственностидостоевскогоможноо
пределитьследующимобразомособенносильнаябисексуальнаяпредрасположенностьиспо
собностьсособойсилойзащищатьсяотзависимостиотчрезвычайносуровогоотцаэтотхарак
тербисексуальностимыдобавляемкранееузнаннымкомпонентамегосуществараннийсим
птомприпадковсмертиможнорассматриватькакотождествлениесвоегоясотцомдопущенн
оевкачественаказаниясосторонысверхятызахотелубитьотцадабыстатьотцомсамомутепе
рьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужетеперьтеб
яубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфантазиимужскогож
еланияиодновременномазохистскимпосредствомнаказаниятоестьсадистическимудовле
творениемобаяисверхяиграютрольотцаидальшевобщемотношениемеждуличностьюиоб
ектомотцаприсохраненииегосодержанияперешловотношениемеждуяисверхяноваяинсц
енировканавторойсценетакиеинфантильныереакцииэдиповакомплексамогутзаглохнуть
еслидействительностьнедаетимвдальнейшемпищинохарактеротцаостаетсятемжесамым
нетонухудшаетсясгодамитакимобразомпродолжаетоставатьсяиненавистьдостоевскогок
отцужеланиесмертиэтомузломуотцустановитсяопаснымеслитакиевытесненныежелания
осуществляютсянаделефантазиясталареальностьювсемерызащитытеперьа

Висновки:

Під час виконання лабораторної роботи набула навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, опанувала прийоми роботи в модулярній арифметиці. Афінний шифр виявився більш стійким ніж шифр Віженера, але для алфавітів з відносно невеликою кількістю букв його ключ можна підібрати. Якщо говорити не про рішення “в лоб” - афінний шифр достатньо легко розв’язується простими методами, що не вимагають багато пам’яті та часу.