Звіт до лабораторної роботи 3 з Симетричної Криптографії

ФІ-03 Буржимський Ростислав, Недождій Максим

Варіант 3

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 розширенного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь необхідно 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, труднощі і їх розв'язання

Слідуючи методичним вказівкам і порядку виконання роботи, ми реалізували усі допоміжні функції, після чого розв'язали поставлену задачу дешифрування афінного шифру. В можливі проблеми можна враховувати пошук змістовних текстів, адже надана у методичних вказівках рекомендація не дуже добре працює для текстів такого розміру, як у наданих варіантах. Застосування індексу відповідності дало кращі результати.

Найчастіші біграми

За допомогою комп'ютерного практику №1, було знайдено, що найчастіші біграми шифротексту будуть 'кд', 'щю', 'во', 'рб', 'тд' (начебто біграми подані у порядку зростання частот). Їх ми і компонували з біграмами 'ен', 'на', 'то', 'но', 'ст' для отримання ключів.

Структура розпізнавача змістовного тексту

Розпізнавач робився аналогічно до розпізнавача з комп'ютерного практикуму №2, адже це був точний і ефективний метод знаходження наближених до природної мови по розподілу символів текстів. Його коректність доведена як теоретично, у відомостях до комп'ютерного практикуму №2, так і практично у комп'ютерних практикумах №2, №3.

Шифротекст і його розшифрування

Наданий шифротекст (згідно варіанта):

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоыомхзотхэтоовцлшвуджозчх йбжькткибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзю жмьгнхщюзншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозо ихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдвоэомюфожхетжютдцюгршшкд эйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстуд вежюнхэджядшищвччощщвуноййхзозпцэфтмефпшхтдпощщщыкдвуозеойбдэзэстсдоожмиврбгхнойхзозпцэцэфпэтщющюэоео хсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмшшзцтй ищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднт жхщюжощщцыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвцхндн шбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншшвуйжышьтджфицхеогбшшан жхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэ стйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесдвейхаирбтюзсжжйб щддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотддншддцбаабжукцеочтйхвюеыдйрббдфхдйыжщщуогбажбфьащелбхшзцтйищцюнхктсдждайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюко стщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбво тдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщтокшеронцчшццнджфитджюкцтй вмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыо эозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжх кйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхетжютдхшкдысбхьнэл жхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхзэтихшцтжбфоилсуюыяшшеокоящелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбд шшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтждждцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухвцщоыояо етктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждннььгррщюцйюгдткуюгаюет мютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоыыйбсунбцюэозоихщюмолесбсуммяюепдэйх сбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвххкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужь кюдурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсййбргшзцтйищцюжхинфиывйу гнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзюшкшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэщитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужхщююует нобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхытцодгжабйбхфйужцбретщюуд шшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцч шццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгх чощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфо човсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыощучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытц ончхшхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетидйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкц жхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбр щюэтсдбоцпштмыкдохьбгцфпиб-

шшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдри анлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднттюхлдшшш итщостжошсзхтдьжрбгхмюлбпзажкбжьхыэцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощйекд ютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуожхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдве атлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсштввюлтднт нойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвщщохсгтфдньзюэшкчаюйхцпвоыойсвцхндн шблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдух вцщоыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэочоьбгцфпчочо боацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйшюыхнцхтидретыбрущоыыйбрбитшхыошсзхтдстнтыбюлпюыыеоьыювюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньще чощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпкдьоицжувундэыдйлдюойхфб пойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэю цнсесдверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцси тцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияжьзвотдучяоехфдвукдюткй тцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюкоушнбднеокодйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьюворнтнтфддйкдютгцит сдвейхагкцжуружхеогсослфчхшщщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюггжнб гхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбй щтцпвотдучвцйудйпрэвщдшдэыдйут

Отриманий розшифрований текст (згідно варіанта):

отцеубийствокакизвестнооснобноеиизначальноепреступлениечеловечестваиотдельногочеловека
вовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлиисследованиямнеудал
осьещеустановитьдушевноепроисхождениевиныипотребностиискупленияноотнюдьнесущественноед
инственныйлиэтоисточникпсихологическоеположениесложноинуждаетсявобъясненияхотношениемал
ьчикакотцукакмыговоримамбивалентнопомимонеенавистиизза которойхотелосьбыотцакаксоперника
устранитьсуществуетобычнонекоторая доля нежностикнемуобаотношенияслываются видентификацию
сотцомхотелосьбызанятьместоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотому
чтохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймоментребено
кначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказание
черезкастрациюизстрахакастрацииитоестьвинтересахсохранениясвоеймужественностиребенокотк
азываетсяотжеланияобладатьматерьюиотустраненияотцапоскольку этожеланиеостаетсявобластиб
ессознательногооноявляетсяосновойдляобразованиячувствавинынамкажетсячтомыописалинормал
ьныепроцессыобычную судьбутакназываемогоэдиповакомплексаследуетоднаковнестиважноедополн
ениевозникаютдальнейшиеосложненияеслиуребенкасильнееразвитконституционный факторназывае
мыйнамибисексуальностьютогдаподугрозойпотериму жественностичерезкастрациюукрепляетсяте
нденцияуклонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместоматериипе
ренятьеероль какобекталюбвиотцаоднали шьбоязньюкастрациделаетэтуразвязкуневозможнойребен
окпонимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщината
кобрекаютсянавытеснениеобапорыванеенавистькотцуивлюбленностьвотцаизвестнаяпсихологичес
каяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследствиестрахаперед внешне
йопасностьюкастрацией влюбленностьжевотцавоспринимаетсякаквнутренняяопасностьпервичног
опозывакоторая посутисвоейсновавозвращаетсяктойжевнешнейопасностистрахпередотцамделает
ненавистькотцунеприемлемойкастрацияужаснакаквкачествекарытакиценылюбвиизобоихфакторо
ввытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияикастрацииследуетназва
тьнормальнымпатогеническоеусилениепривноситсякаккажетсялишьдругимфакторомбоязньюженст
веннойустановкиярковыраженнаябисексуальнаясклонностьстановитсятакимобразомодним изусло
вийилиподтвержденийневрозаэтусклонностьочевидноследу етпризнатьиудостоевскогоионалатен
тнаягомосексуальностьпроявляетсявдозволенномвидевтомзначениикакоеимелавегожизнидружбас
мужчинамивегодостранностинежномотношениикоперникамвлюбвиивегопрекрасномпониманииполо
женийобяснимыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленныепример
ыизегопроизведенийсожалеюноничегонемогуизменитьеелиподробностионенавистиилюбвикотцуи
обихвидоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанализечитателюпокажутс
ябезвкуснымиималовероятнымипредполагаючтоименнокомплекскастрациибудетотклоненсильнее
всегоносмеюуверитьчтопсихоаналитическийопыт ставитименноэтиявленияявневсякогосомнения и
находитвнихключклюбомуневрозуиспытаемжеговслучаетакназываемойэпилепсиинашегописател
янонашемусознаниютакчуждытеявленияявластикоторыхнаходится нашабессознательнаяпсихиче
скаяжизньуказаннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытесненияненависти
котцуновымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянное
местоэтоотождествлениевоспринимается нашимяноп редставляетсобойвнемособуюинстанциюпроти
востоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашимсверхяиприписыва
емейнаследницеродительскоговлиянияна иважнейшиефункцииеслиотецбылсуровнасильственжест
окнашесверхяперенимаетотнегоэтикачестваивегоотношениикясновавозникаетпассивностькото
ройкакразнадлежалобыбытьвытесненнойсверхяталосадистическимястановитсямазохистскимто

естьвосновесвоейженственнопассивнымвнашемявозникаетбольшаяпотребностьвнаказаниииятч
астиотдаетсебякактаковоевраспоряжениесудьбыотчастиженаходитудовлетворениевжестокомоб
ращенииснимсверхсознаниевиныкаждаякараявляетсяведьвосновесвоейкастрациейикактаковая
осуществлениемизначальногопассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяп
роекцияотцанормальныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаописан
ныездесьанормальныенамещенеудалосьустановитьразграниченияміжднимизамечаетсячтонаибо
льшаярольздесьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженственности и
ещекакслучайныйфакторимеетзначениеявляетсяливнушающийстрахотецивдействительностиособ
еннонасильственнымэтоотноситсякдостоевскомуфактегоисключительногочувствавиныравнокак
имазохистскогообразажизнимысводимкегоособенноярковыраженномукомпонентуженственностид
остоевскогоможноопределитьследующимобразомособенносильнаябисексуальнаяпредрасположен
ностьиспособностьсособойсилойзащищатьсяотзависимостиотчрезвычайносуровогоотцаэтотхар
актербисексуальностимыдобавляемкранееузнаннымкомпонентамегосуществараннийсимптомприп
адковсмертиможнорассматриватькакотождествлениесвоегоясотцомдопущенноевкачественаказа
ниясосторонысверхятызахотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйобы
чныймеханизмистерическихсимптомовиктомужетеперьтебяубиваетотецдлянашегоясимптомсмерт
ияявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазохистскимпосредствомн
аказанияэтоестьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшевобщемотно
шениемеждуличностьюиобектомотцаприсохраненииегосодержанияперешловотношениемеждуяисве
рхяноваяинсценировканавторойсценетакиеинфантильныереакцииэдиповакомплексамогутзаглох
нутьеслидействительностьнедаетимвдальнейшемпищинохарактеротцаостаетсятемжесамымнетон
ухудшаетсясгодамитакимобразомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиес
мертиэтомузломуотцустановитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделеф
антазиясталареальностьювсемерызащитытеперьа

Значення ключа

Отримане значення ключа $k = (199, 700)$

Висновки

Робота з біграмами дало можливість розшифрувати текст, зашифрований так званим 'афінським' (не трейдмарк) шифром. Повідомлення містило явні натяки на неврози, психози, поради каструвати людей, вбивати батьків і ставати гомосексуалістами. Я не можу сказати, що я згоден з повідомленням, але змістовну інформацію текст містить.