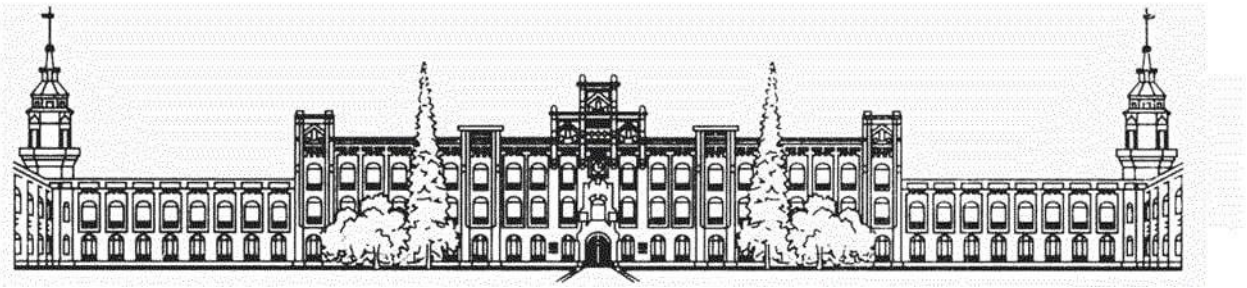

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали роботу:

студент ФБ-23 Хоменко Гліб

студент ФБ-23 Ткачук Андрій

Варіант 3

Київ 2024

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

Постановка задачі:

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.

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

Найчастіші біграми шифротексту

Біграма	**Кількість у шифротексті**
тд	77
рб	53
во	52
щю	45
кд	42

Пари популярних біграм

	тд	рб	во	щю	кд
тд		тд, рб	тд,во	тд,щю	тд,кд
рб			рб,во	рб,щю	рб,кд
во				во,шю	во,кд
щю					щю,кд
кд					

	ст	*но*	*то*	*на*	*ен*
ст		*ст,но*	*ст,то*	*ст,на*	*ст,ен*
но			*но,то*	*но,на*	*но,ен*
то				*то,на*	*то,ен*
на					*на,ен*
ен					

Пари популярних біграм

	тд	рб	во	щю	кд
тд		562,497	562,76	562,804	562,314
рб			497,76	497,804	497,314
во				76,804	76,314
щю					804,314
кд					

	ст	*но*	*то*	*на*	*ен*
ст		545,417	545,572	545,403	545,168
но			417,572	417,403	417,168
то				572,403	572,168
на					403,168
ен					

Приклад знайдених a та b

a	b
954	533
199	700
854	256
62	407
206	664
861	220
69	371
655	593
824	744
169	955
923	130
943	762
792	411
62	407

Потрібний ключ обирається за таким алгоритмом:

1. Розшифровуємо текст за кожним ключем
2. Порівнюємо найпоширеніші літери тексту і російської мови
3. Порівнюємо найпоширеніші біграми тексту і російської мови
4. Відкидаємо ключ, якщо менше 2 спільних букв та менше 3 спільних біграм

Після перевірок залишається ключ (199,700)

Зашифрований текст:

кдяхэаюлтдооэтсювнкцябпосбанвоюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоы
омхзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцю
лцлхйостщюшужхриажгцфхзххцитвожюфпксщхибуххйзюжмьгнхщюзншбхюэотйбаводтдцюэшшыл
хщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозоихщюкцзо
юбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдвоэомюфож
хетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэй
юейосежхюбгцэюубйутодткдвощхщющцяюстудвежюнхэджядшищвччощщвуноййхзозпцэфтмефпш
хтдпощщщыкдвуозеойбдээзстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрс
тднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэдохехвоубпзш
бчхлыйбсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфт
щютздйирэттднттюрюецтйвмшшзцтйищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвот
дмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднтжхщюжощщщыгцщоцпьсждьггж
нбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвцхнднш
бчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншш
вуйжышьтджфицхеогбшшанжхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюа
йбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэстйуэлетмюшюыхнцхтцпвотдучеощицы
нийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесдвейхаирбтюзсжжйбщддццнтдэ
ййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотддншддцбаабжукцеочтйхвюеыдйрббдфхдйыжхш
шшщаышиткчсняощщуогбажбфьащелбхшзцтйищцюнхктсдждайершецшмбзнбрфоюболохехвоаый
бсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбью
етитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбвотдбнкдютрртхтдетм
ыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщтокшеронцчшццнджфитд

жюкцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэтк
нгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзн
жхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхбжйуолэттднттюзсзтсбш
шшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхетжютдхшкдысбхьнэлжх
эоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшухж
цлжрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщо
дэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсурржцзожюдюяюэоддт
ххгнхщюжбзнкофтждцжжйбвотдромхжюгбгцлххсдкйрретфпасйотдухвцщоыояоетктйхэдет
эьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждннььгррщюц
йюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпннъхыохзйзцво
ьыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэсту
добжьлзтцлхыбвххйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькюдурбщдфхгжеынико
ьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсййбргшзцтйищцюжхинф
иывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзю
шхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзк
цсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужхщююютнобюхнщютшкчншкчбохсжхыйбр
кююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхытцодгжабйбхфйужцбретщюудшшй
свишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфт
ыбрудэщхжхтцмхрыонцчшццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысв
одэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбух
шхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитц
щвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюиц
тхшмююкйеытцончхшхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщц
эьцайанетпюцптдтхнгкцеоубхфкцтхшммыдйрбсучхеоябньмкэюэтмхтдстпннъпоябсфрбцюде
сбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкцжхыболиндйчетдажгцс
итцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйу
цнбрщюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгр
бгхшсшпцэкдлттдкгрбвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжю
чээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднттюхлдшшшитщостжошсзхтдьжрбгхмюлбпза
жкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощйекдютво
эуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвхпик
цутвоэуажкбвхетшхзххриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйа
ыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдвеатлцпнчэсклхшхэджудэйхсбрбвочгрбтдт
хыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсштввюлтднтнойхтюмихлтд
жюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдньзюэшкчаюйхцпв
оыойсвцхндншблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтих
ыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюбпокйфигжшддцлххсввсущантсофочоехы
бгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэочоьбгцфпчочобоацлжолфтьюжтфпвекд
фтжюпюфотдяобзохвнщзтлвошскооыокдютждкдртнтфддйшюыхнцхтцпвотдсуыищаднсейузйн
бьхдретыбрущоьыйбрбиташхыошсзхтдстнтыбюлпюьыеоьывюатошанкудйэюфоюбэйзцкуодвюст
фпэтщоеовикцхнлхщюкцооньщечощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдп
рвмкдгжэащдрощщсиюасцитфпкдьоицжувундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмю
тддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсес
дверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнву
етэтфтщюбдухтддцситцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщ
азхфоябсфрбгхшхвияжьзвотдучяоехфдвукдютккйтцюмнтжхщюгхыочонххгнбйебхохвжанкдво
щхщюйувгксююиндйчевостююхцяхщюкоушнбднеокоацяхжхитсююйянбэюцпчэдйщтощцюйиеыа
ншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфд
дйкдютгцитсдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпв
ешбрбднтцфпйотдухвцщоыощощщюггжнбгхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщд
шшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбйщтцпвотдучвцйудйпрэвщ
дшдэыдйут

Відкритий текст:

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельног
очеловекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлии
сследованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностиискупл
енияноотнюдьнесущественноединственныйлиэтоисточникпсихологическоеположениесло

жноинуждаетсявобъяснениихотношениемальчикакотцукакмыговоримамбивалентнопомимон
енавистииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекотор
аядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосьбызанятьм
естоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоу
странитьвсеэтоналкиваетсянакрупноепрепятствиевопределенныймоментребенокначи
наетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказа
ниечерезкастрациюизстрахакастрациитоестьвинтересахсохранениясвоеймужественнос
тиребенокотказываетсяотжеланияобладатьматерьюиотустраненияотцапосколькуэтожел
аниеостаетсявобластибессознательногоооноявляетсяосновойдляобразованиячувствави
нынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбутакназываемогоэдиповак
омплексаследуетоднаковнестиважноедополнениевозникаютдальнейшиеосложненияеслиу
ребенкасильнееразвитконституционныйфакторназываемыйнамибисексуальностьютогдап
одугрозойпотеримужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсто
ронуженственностиболеетоготенденцияпоставитьсебянаместоматерииперенятьеероль к
акобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпо
нимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщи
натакобрекаютсянавытеснениеобапорываненавистькотцуивлюбленностьвотцаизвестная
психологическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследст
виестрахапередвнешнейопасностьюкастрацией влюбленностьжевотцавоспринимаетсякак
внутренняяопасностьпервичногопозывакотораяпосутисвоейсновавозвращаетсяктойжев
нешнейопасностистрахпередотцамделаетненавистькотцунеприемлемойкастрацияужасна
каквкачествекарытакиценылюбвиизобоихфактороввытесняющихненавистькотцупервыйне
посредственныйстрахнаказанияикастрациисследуетназватьнормальнымпатогеническоеу
силениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойустановкиярко
выраженнаябисексуальнаясклонностьстановитсятакимобразомоднимизусловийилиподтв
ерждений невроза этусклонностьочевидноследуетпризнатьиудостоевскогоионалатентна
ягомосексуальностьпроявляетсявдозволенномвидевтомзначенииикакоеимелавегожизнид
ружбасмужчинамивегодостранностинежномотношенииксоперникамвлюбвиивегопрекрасно
мпониманииположенийобъяснимыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываю
тмногочисленныепримерыизегопроизведенийсожалениюничегонемогуизменитьеелиподро
бностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозыкастрациинесве
дущемувпсихоанализечитателюпокажутсябезвкуснымиималовероятнымипредполагаючтои
меннокомплекскастрациибудетотклоненсильнеевсегоносмеюуверитьчтопсихоаналитиче
скийопытставитименноэтиявленияявневсякогосомненияинаходитвнихключклюбомуневроз
уиспытаемжеговслучаетакназываемойэпилепсиинашегописателянонашемусознаниютакч
уждытеявленияявластикоторыхнаходитсянашабессознательнаяпсихическаяжизньуказа
ннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытесненияненавистикотцун
овымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянное
местоэтоотождествлениевоспринимаетсянашимянопредставляетсобойвнемособуюинстан
циюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашимс
верхяиприписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецб
ылсуровнасильственжестокнашесверхяперенимаетотнегоэтикачестваивегоотношениикя
сновавозникаетпассивностькоторойкакразнадлежалобыбытьвытесненнойсверхясталоса
дистическимстановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашем
явозникаетбольшаяпотребностьвнаказанииияотчастиотдаетсебякактаковоевраспоряже
ниесудьбыотчастиженаходитудовлетворениевжестокомобращенииснимсверхясознаниеви
ныкаждаякараявляетсяведьвосновесвоейкастрациейикактаковаяосуществлениемизнача
льногопассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяпроекцияотцано
рмальныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаописанныезде
сьанормальныенамещенеудалосьустановитьразграниченияміжду нимизамечаетсячтонаиб
ольшаярольздесьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженств
енностиищекакслучайныйфакторимеетзначениеявляетсяливнушающийстрахотецивдейст
вительностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключительн
огочувствавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраже
нномукомпонентуженственностидостоевскогоможноопределитьследующимобразомособен
носильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяот
зависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкра
нееузнаннымкомпонентамегосуществованнийсимптомприпадковсмертиможнорассматрива
ткакотождествлениесвоегоясотцомдопущенноевкачественаказанияссторонысверхяты
захотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйобычныймеханизми

стерическихсимптомовиктомужетеперьтебяубиваетотецдлянашегоясимптомсмертиявляе
тсяудовлетворениемфантазиимужскогожеланияиодновременномазохистскимпосредством
наказанияэтоестьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшево
бщемотношениемеждуличностьюиобектомотцаприсохраненииегосодержанияперешловотно
шениемеждуяисверхяноваяинсценировканавторойсценетакиеинфантильныереакцииэдипо
вакомплексамогутзаглохнутьеслидействительностьнедаетимвдальнейшемпищинохаракт
еротцаостаетсятемжесамымнетонухудшаетсясгодамитакимобразомпродолжаетоставатьс
яиненавистьдостоевскогокотцужеланиесмертиэтомузломуотцустановитсяопаснымеслит
акиевытесненныежеланияосуществляютсянаделефантазиясталареальностьювсемерызащи
тытеперьа