Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки

Роботу виконали:

Біла Анастасія і Лета Яна,

студенти 3 курсу ФТІ НТУУ «КПІ»,

спеціальність «Кібербезпека», група ФБ-02

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 (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.

Варіант завдання: 3

Хід роботи:

1.Реалізуємо програми з такими математичними операціями: знаходження НСД, обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язування лінійних порівнянь, які потрібно буде обчислювати для кожної утвореної системи кандидатів (a,b) на ключ.

2.Використаємо функцію для обчислення 5 найчастіших біграм даного шифртексту за варіантом, і отримаємо:

['тд', 'рб', 'во', 'щю', ,ет']

Відповідно 5 найчастіших біграм російської мови відкритого тексту нам відомо:

['ст', 'но', 'то', 'на', 'ен']

3.Потім співставляємо знайдені біграми шифртексту із біграмами відкритого тексту (користуємося тільки 5 найчастішими) і знаходимо кандидатів на ключ шляхом розв’язування системи.

Отримаємо такі можливі кандидати на ключ:

[(954, 533), (199, 700), (854, 256), (446, 625), (923, 130), (943, 762), (792, 411), (911, 904), (305, 590), (802, 727), (269, 29), (199, 700), (199, 700), (246, 71), (708, 63), (363, 693), (7, 526), (206, 664), (861, 220), (453, 589), (38, 929), (20, 168), (830, 778), (949, 310), (656, 469), (497, 634), (925, 897), (855, 607), (762, 359), (47, 829), (509, 821), (164, 490), (762, 899), (755, 870), (655, 593), (247, 1), (18, 837), (941, 405), (810, 686), (929, 218), (159, 872), (464, 900), (428, 339), (358, 49), (715, 567), (914, 705), (462, 68), (117, 698), (107, 149), (100, 120), (306, 287), (553, 212), (169, 955), (131, 523), (151, 194), (119, 336), (692, 376), (36, 404), (533, 541), (891, 514), (253, 342), (452, 480), (499, 812), (616, 473), (515, 110), (508, 81), (714, 248), (408, 765), (50, 792), (12, 360), (32, 31), (842, 641), (762, 35), (106, 63), (603, 200), (70, 463), (598, 42), (797, 180), (844, 512), (345, 504), (897, 342), (172, 913), (120, 494), (371, 576), (282, 210), (83, 547), (192, 261), (17, 200), (64, 717), (236, 107), (184, 649), (435, 731), (679, 849), (762, 834), (871, 548), (696, 487), (789, 686), (725, 466), (909, 618), (199, 700), (878, 91), (199, 700), (109, 751), (895, 690), (841, 872), (777, 652), (52, 262), (251, 886), (769, 144), (90, 753), (852, 129), (786, 743), (590, 159), (526, 900), (762, 510), (710, 91), (944, 535), (265, 183), (66, 520), (175, 234), (370, 342), (327, 913), (27, 494), (588, 576), (778, 489), (672, 578), (223, 819), (265, 820), (591, 717), (918, 107), (618, 649), (218, 731), (183, 570), (855, 586), (406, 827), (448, 828), (634, 686), (43, 466), (661, 618), (261, 700), (289, 60), (106, 948), (512, 317), (554, 318), (934, 872), (343, 652), (300, 262), (561, 886), (738, 547), (555, 474), (449, 563), (42, 805), (373, 159), (743, 900), (700, 510), (400, 91), (696, 876), (513, 803), (407, 892), (919, 172), (491, 655), (182, 252), (641, 748), (292, 128), (470, 404), (652, 94), (150, 590), (762, 931), (779, 386), (309, 479), (459, 572), (110, 913), (320, 618), (811, 711), (502, 308), (612, 184), (669, 607), (199, 700), (851, 297), (349, 793)]

4. За допомогою кожного кандидата на ключ розшифровуємо текст та знаходимо правильний ключ із функції перевірки змістовності розшифрованого тексту, використовуючи порівняння значення ентропії відкритого тексту російської мови і ентропії розшифрованого тексту.

Отримана пара (a, b), що є ключем до афінного шифру: **(199, 700)**

Шифротекст :

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоыомхзотхэтоовцлшву
джозчхйбжькткибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужхриажгцфхзхжцитво
жюфпксщхибухкйзюжмыгнхщюзншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюжд
зютдлзщюаыпюнозоуюмхэшухэозоихщюкцзоюбзюгсвичхшцщнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтму
фьанэйсужушюстлхэдвоэомюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцх
еоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстудвежюнхэджядшищвччощщвуной хзозпцэфтмеф
пшхтдпощщщыкдвуозеойбдэзэстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрстднтщюфпвцукео
етитмшпнчхшщабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлыйбсуодмзеоэотэкшфстднтщ
юфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмшшзцтйищщюеокцфпж
юэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднтжхщю
жощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсв
цхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбфчшсшпвситуберончхфоыойиеыаншшвуйжышь
тджфицхеогбшшанжхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйерж
юкшйбтдщдзщяоыбэлгтфдэйетзэстйуэлетмюшюыхнцхтцпвотдучеощицынийькосотыкддйсуюгкцхнрбвотдьздйир
эттднттющсзйэысесдвейхаирбтюзсжжйбщддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотддншддцбаабжу
кцеочтйхвюеыдйрббдфхдйыжхшшшщаышиткчсняощщуогбажбфьащелбхшзцтйищщюнхктсджданершецшмбзнбр
фоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбью
етитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбвотдбнкдютрртхтдетмыпюнозоуюмхэш
юентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщтокшеронцчшщцнджфитджюкцтйвмщыдйфиибшфжхмоатс
бгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонт
мыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгх
бжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхетжютдхш
кдысбхьнэлжхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшухжцл
жрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюы
хнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтждцжжйбв
отдромхжюгбгцлхкссдкйрретфпасйотдухвцщоыояоетктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшцщнйовныжрбв
оенэизнеожретмхщюдшшшухсугждннььгррщюцйюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчоб
хдбдшжуьжгажюпнньхыохзйзцвоыыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгцфпюшш
шетждрсэтзэстудобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькюдурбщдфхгжеыникоь
бгцэюйбрбдntцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсййбргшзцтйищцюжхинфиывйугнрцн
мттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзюшхыбфшвуйжышэшзцтйищц
ювснхеокшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцн
жхвцлшжьгцвужхщюююетнобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыювцислтсдшшетзэстйуолсылжэып
юшбхфньхытцодгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпе
тмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмрыонцчшццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетж
ютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдм
кеокдьгнхтдьжрбгхооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитц
пвохсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдйнищдг
ждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшммыдйрбсучхеояб
ньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкцжхыбо
линдйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйу
цнбрщюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлтт
дкгрбвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкц
оохлэттднттюхлдшшшитщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбях
щоцщаняюепмтцпжхофюекйухощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбд
ыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшц
взеоетйаыжтфюекоцппикцбнщожхвбвущджьэыювюфюнэстсдвеатлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюг
хзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсштввюлтдntнойхтюмихлтджюйхцпвотдяочоехыбйбзцл
ждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпоо
йерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюбпокйфигж
щддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэочоьбгцфпчочобоацлжолфт
ьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйшюыхнцхтцпвотдсуыищаднсейузйнбьхд
ретыбрущоьыйбрбитшхыошсзхтдстнтыбюлпюьыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщ

юкцооньщечощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпкдьои цжувундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеой хшисеетщхыощцсучдвукудйэюцнсесдверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцш цсюьыгцохэцхнвуетэтфтщюбдухтддцситцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнща зхфоябсфрбгхшхвияжьзвотдучяоехфдвукдютккйтцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююинд йчевостююхцяхщюкоушнбднеокоацяхжхитсюоюйянбэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфх джэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфддйкдютгцитсдвейхагкцжуружхеогсослфчхшцщц ыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюггжнбгхкудйэюждвудрзохскд ыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбйщтцпвотдучвцйуд йпрэвщдшдэыдйут

Розшифрований текст :

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекавовсякомслучаео ноглавныйисточникчувствавинынеизвестноединственныйлииссследованиямнеудалосьещеустановитьдушевноепро исхождениевиныипотребностиискупленияноотнюдьнесущественноединственныйлиэтоисточникпсихологическое положениесложноинуждаетсявобъясненияхотношениемальчикакотцукакмыговоримамбивалентнопомимоненавист иизакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекотораядолянежностикнемуобаотнош ениясливаютсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызываетвосхищениехотелосьб ыбытькаконипотомучтохочетсяегоустранитьвсеэтоналкивается накрупноепрепятствиевопределенныймоментре бенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказаниечерезкастр ациюизстрахакастрациитоестьвинтересахсохраненияс воеймужественностиребенокотказываетсяотжеланияоблад атьматерьюиотустраненияотцапоскольку этожеланиеостается вобластибессознательногооноявляетсяосновойдляо бразованиячувствавинынамкажетсячтомыописалинормальныепроцессыобычную юсудьбутакназываемогоэдиповак омплексаследуетоднаковнестиважноедополнениевозникаютдальнейшиеосложненияеслиуребенкасильнееразвитк онституционныйфакторназываемыйнамибисексуальностьютогдаподугрозойпотеримужественностичерезкастрац июукрепляетсятенденцияуклонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместоматериип еренятьеероллькакобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчт оондолженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснение обапорываненавистькотцуивлюбленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотненави стикотцуотказываютсявследствиестрахаперед внешнейопасностьюкастрацией влюбленностьжевотцавосприниме тсякаквнутренняяопасностьпервичногопозывакотораяпосутисвоейсновавозвращаетсяктойжевнешнейопасностис трахпередотцамделаетненавистькотцунеприемлемойкастрацияужаснакаквкачествекарытакиценылюбвиизобоих фактороввытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияикастрациисследуетназватьнорма льнымпатогеническоеусилениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойустановкиярк овыраженнаябисексуальнаясклонностьстановитсятакимобразомоднимизусловийилиподтвержденийневрозаэтуск лонностьочевидноследу етпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвид евтомзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежномотношениихсоперникамвлюбв иивегопрекрасномпониманииположенийобъяснимыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываютмн огочисленныепримерыизегопроизведенийсожалеюноничегонемогуизменитьеелиподробностионенавистиилюбвик отцуиобихвидоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанализечителюпокажутсябезвкусн ымиималовероятнымипредполагаючтоименнокомплекскастрациибудетотклоненсильнеевсегоносмеюуверитьчтоп сихоаналитическийопытставитименноэтиявленияв невсякогосомненияинаходитвнихключклюбомуневрозуиспыта емжеговслучаетакназываемойэпилепсиинашегописателянонашемусознаниютакчуждытеявленияв ластикоторы хнаходитсянашабессознательнаяпсихическаяжизньуказаннымвышенеисчерпываютсявэдиповомкомплексепослед ствиявытесненияненавистикотцуновымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяп остоянноеместоэтоотождествлениевоспринимаетсянашимянопредставляетсобойвнемособуюинстанциюпротивос тоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашимсверхяиприписываемейнаследнице родительскоговлияниянаиважнейшиефункцииеслиотецбылсуровнасильственжестокнашесверхяперенимаетотнег оэтикачестваивегоотношениикяснова возникаетпассивностькоторойкакразнадлежалобыбытьвытесненнойсверхяс талосадистическимястановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашемявозникаетбольш аяпотребностьвнаказанииияотчастиотдаетсебякактаковоевраспоряжениесудьбыотчастиженаходитудовлетворени евжестокомобращениисниммсверхясознаниевиныкаждаякараявляетсяведьвосновесвоейкастрацией икактаковаяосу ществлениемизначальногопассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяпроекцияотцанорма льныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаописанныездесьанормальныенамещенеу

далосьустановитьразграниченияміждунимизамечаетсячтонаибольшаярольздесьвконечномитогеприписываетсяпа ссивнымэлементамвытесненнойженственностиищекакслучайныйфакторимеетзначениеявляетсяливнушающийс трахотецивдействительностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключительногочувс твавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраженномукомпонентуженственнос тидостоевскогоможноопределитьследующимобразомособенносильнаябисексуальнаяпредрасположенностьиспосо бностьсособойсилойзащищатьсяотзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдоб авляемкранееузнаннымкомпонентамегосуществараннийсимптомприпадковсмертиможнорассматриватькакотожд ествлениесвоегоясотцомдопущенноевкачественаказаниясосторонысверхятызахотелубитьотцадабыстатьотцомса момутеперьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужетеперьтебяубиваетотецдл янашегоясимптомсмертиявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазохистскимпосре дствомнаказаниятоестьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшевобщемотношениеме ждуличностьюиобектомотцаприсохраненииегосодержанияперешловотношениемеждуяисверхяноваяинсценировк анавторойсценетакиеинфантильныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедаетимвда льнейшемпищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитакимобразомпродолжаетоставатьс яиненавистьдостоевскогокотцужеланиесмертиэтомузломуотцустановитсяопаснымеслитакиевытесненныежелани яосуществляютсянаделефантазиясталареальностьювсемерызащитытеперьа

Висновки:

У ході виконання комп’ютерного практикуму при розшифруванні тексту російської мови афінною підстановкою, використовуємо набуті навички частотного аналізу при порівнянні ентропій ВТ і ШТ для перевірки тексту на змістовність, а також опановуємо прийоми роботи в модулярній арифметиці для знаходження кандидатів ключа.