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

Криптографія

Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки

Варіант №5

Виконали:
Студенти III курсу
Групи ФБ-95
Пашинський М.О.
Бурчак Б.Ю.
Перевірила:
Селюх П.В.

Київ – 2021

Мета роботи:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; оволодіння 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 No1, 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, 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 виконання роботи:

Для початку з шифротексту було утворено **масив біграм** (без перетину) і знайдено **по 5 найчастіших біграм в російській мові** та самому **шифротексті**. Отримані біграми було переведено у числові значення за формулою: **B1 * 31 + B2**

Далі з отриманих даних було створено **списки можливих пар елементів** для кожного з масивів, що містять **числові значення найчастіших біграм**. Це було зроблено для зручності знаходження можливих ключів **(a, b)**. Описати даний процес можна як розв'язок системи рівнянь де:

(1) - Знаходяться значення різниць елементів пар біграм:

P = (p1 – p2)mod961

C = (c1 – c2)mod961

(2) **-** Ці значення використовуються для знаходження ключа **a**:

a = ((P^-1) * C)mod961

(3) **-** Знаючи значення ключа **a** знаходиться ключ **b:**

b = (c1 – a * p1)mod961

Для знаходження ключа було написано ф-ї знаходження **НСД** та **оберненого елемента до a**.

Згодом було отримано **список розшифрованих текстів** за допомогою кожного відомого ключа. Розшифрування здійснювалось за формулою: **P = (a^-1 * (C - b))mod961.**

Потім для кожного отриманого тексту ми знайшли **індекси відповідності** (Опираючись при цьому на твердження, що індекс коректного тексту буде найбільш наближеним до теоретичного значення індексу відповідності російської мови ~ **0.0553**).

Таким чином було знайдено текст розшифрований ключем **(654, 777)**. Він виявився майже досконалим. В ньому на місці де мала би стояти буква **'ь'** стояла буква **'ы'** та навпаки. Також це вплинуло і на інші розшифровані букви.

Коректний, змістовний текст було отримано коли ми поміняли в алфавіті місцями букви **'ь'** та **'ы'**.

Шифротекст:

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэммндтихкеюибщыцязкзхшвнос
ыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввцтнавпьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэм
химьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсгцыззфрщихзтчщрихн
эпозтгфккчщкдмклыоьеынунййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивупхюфйчсьивйэютнрцшэбв
щншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшдекхнд
у
аошдвдеигебуявюсшьйдроццвнфиибжлакцввбвываккчслтьхщзйьцжьбрьецфтспьбишиыовдьезбтнмсэкжллрчсхщьрпьшв
шнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющькккюиеуяээтьяяреурндуьцоэгкмбобмщкскехюксдцтсывзтмсун
йьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйнмсуншснхтуйнццмсяьмныонкцркч
ыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьив
цнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюджджкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяышвнун
хщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщмбриввудябакфурщяэлчяздкаиьечслс
осэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбь
еелфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсисцйвнихчщлр
акющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовявшньсйссцпрыоынчкццяьклхнщэюдри
исэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюи
йдьяшншвосюсчязиьсунуллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгйрщтнгбфдзйьцэибусчжвавмнззфдыоиюшс
осюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшнищюиьс
щожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшвнюдцфвдыоияосунйпщнбкчзиввнмн
рьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуцццщццспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеи
чмывпвыэдчфкклццсвынуняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыо
жяшсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсстгнхщщщфддбтьпнзкьеэдхнщьжвзтфрлцдкяя
хь
овюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьсц
клжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвпыызмбйнвнцхпнуцязьсйядуулрибу
вдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьав
тулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншпвихэхаорщибясфсчсщьавпьскггыоющлхвииспьвиул
бутнзцнулцяьжцюсчвввймюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшьявхщеуеидебупьесуз
ющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхчщмщявисчтжьамаофисрябсчшижслбубщэнщфдэмсщяб
уб
чзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхсовпннчубакакхуямдкяяхсвнхбжсмкщн
щьжвэкссщьккдктнфифсбвддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьвнбкубье
бчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщ
убссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглозфьцэидктнунэибунсхщав
ьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпноулцфрынщхыщмснфжврйвньркзск
ыщ
ссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьичдрщдкикгбмщбущстссвйьшвоейу
лцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщ
кзищ
ссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнмспбмщбущськмюннисдкдкцфжвйьдт
мщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщькккгнввшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэ
юсрсхщньбиулбунхнчйдпнввкцйнушвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавыщсиеуобмбмщбущсфрмщчяовуп
мюосшнкуаохщмсэкццзтбыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихщавиэжьчщоуобмблвыьрнунокпмшр
дцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсцць
блшэннбвамозмщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтзскиющькккбыоскчицпьявицчзивяьочлц
свпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяякадункчзжсюсбчкнбквьфзтнуноьюддкнхживнал
буыодкеиочоьлхэфдкфпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщбакксйнбжрисцвджцмнщькмыгьяье
хщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгьерынньэьынавэкиютынькиютноьакеишдщщ
швпвмндтихжцшнйнюирсыэьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунт
с
чтгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпвюскиосыр
ынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщцсунхдицяедьакхуумжсвнчр
лвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлсиьпвтснфюирыюсцьаккнивжошижс
мкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяспнчкхуцфюижсшщязюсшсиэжьввшв
яэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнвввввшнмьвврщозенйсуньейпфкаьтныо
еущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхмьакггмщшджсунлххэхьзт
лрэчбудквввзнввшнжьжврщунынжвжрццисчцэиаьмчввршищссркжэжвмндтфрлцяьклхнгцязвэкьзцэиьшсвмдьцюяусиебчду
ьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпьгбубсвйнавдьоспншсмкпрынкчмсхщнкой
щщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшь
ыо
арфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекццжлывйквэпншнхщынгспныэ
рнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдициввспьгсунмщпвюдцфюирыусунлрлцдкяяыуаокнввпьфзлц
внстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщ
ьяшныннйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчсжвюсстибдцньтсюсстхщээрщьечщ
кзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуиюшннуяетнхщюиакфккчлспьыопьрц
мнрншбынлсюдризьяуфкшдвчсксчавзтрщхсщв

Відкритий текст (K => 654, 777):

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлосьбыубиватьсамомуэтонеодноли
шьдобroесостраданиеэтоотождествлениенаосновании одинаковыхимпульсовкубийствусобственноговорялишьвминимально
йстепенисмещенныйнарциссизмэтическаяценностьэтойдобротыэтимнеоспариваетсяможетбытьэтовообщемеханизмнашегод
оброгоучастияпоотношениюкдругомучеловекуособенноясноступающийвчрезвычайномслучаеобремененногосознанияев
оейвиныписателянетсомнениячтоэтасимпатияпопричинеотождествлениярешительноопределилавыборматериаладостоевско
гоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступникаполитическогоирелигиозногопреждечемкко
нцусвоейжизнивернутьсякпервопреступникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопос
мертногонаследияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманиибылобуреваем
игорнойстрастьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеподдаетсяинойоценкенискакойст
оронынебылонедостаткавоправданияхэтогостранногоинедостойногоповеденияучувствовиныкакэтонередкобываетуневротик
овнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймоготговариватьсятемчтоонпривыигрышеполучилбывоз
можностьвернутьсяврассиюизбежавзаключенияявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточнопр
оницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавнымбылаиграсамапосебевсеподробност
иегообусловленногопервичнымипозывамибезрассудногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспо
каивалсяпоканетерялвсегоиграбыладлянеготакжесредствомсамонаказанияснесчетноеколичествораздавалонмолодойженеслов
оиличестноесловобольшеиграть или неиграть вэтотденьионнарушалэтословокаконарассказываетпочтивсегдаеслионсвоими
проигрышамидоводилсебяиеедокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудовлетворени
емонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешник
аипослевсейэтойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзамети
лачтотоотчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшечем
послепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудо
влетворенонаказаниямиккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозволялсебеделатьне
сколькошаговнапутикуспехурассматриваярассказболеемолодогописателянетрудноугадатькакиедавнопозабытыедетскиепере
живаниянаходятвыявленияивигорнойстрастиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтр
имастеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываеткакбу
дтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеудивительныедлянеесамойзакононарушенияеетолк
аетнеожиданноежизненноевпечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобез
такойоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилискореебщемужскоеитакоетолк
ованиестольявноподсказаночтонетвозможностиегонедопуститьдлясущностихудожественноготворчествахарактерночтописа
тельскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждоиво
всеневходиловегонамерениянесмотрянаточтоврассказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнат
айныйследвэтойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережитьболеедвадцатилеттому
назадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуждалисьотказавшаясяоткакихбытонибылонадежднасороквтор
омгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредивсехдиков
инеевниманиеприковываютдверукикоторыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенесчастн
ымигрокомчувстварукиэтирукикрасивогоюноши писателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанабл
юдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаянииипокидающегозалчтобывпаркепокончитьсосвоеюбезнаде
жнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетееза
однуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужденавконцеконцо
ввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойлюбовнойно
чионавелитказалосьбыуспокоившемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетиграть снабжаетег
оденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуж
даетсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимв
местевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезн
увшемуюношеонасноваприходитвигорныйдомисвозмущениемобнаруживаеттамтежерукинакануневозбудившиевнейтакуюг
орячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещаниионодержимыйстрастьюонбранитсорвав
шуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаетгородавпоследс
твииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконеч
ноправонасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпечатленияоднакопсихоанализучитчтоона
возниклаонаосновеумопострояемоговожделенияпериодаполовогосозреванияокаковомвожделениинекоторыевспоминаютсове
ршенносознательносогласноумопострояемомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотз
аслуживающегоопасенияврединаонизмастольчастыесублимирующихудожественныепроизведенияивытекаютизтогожеперво
источникапороконанизмазамещаетсяпорокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательс
кисвидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивонани
зменионимсловомкромесловаигранельзяназватьетееаа

Висновок:

В ході виконання даної лабораторної роботи ми отримали навички криптоаналізу шифру афінної біграмної підстановки, застосували їх для знаходження ключа і розшифрування повідомлення знаючи лише шифротекст.