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

Виконав:
Андреєв Д.Ю.
Група: ФБ-06
5 варіант

Київ - 2022

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 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 - 5.

Хід роботи

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.

Починаємо реалізовувати необхідні функції. Для початку реалізуємо розширений алгоритм Евкліда ext_gcd який окрім НСД знаходить також такі числа x та y що ax+by=НСД(a, b). Далі, використовуючи цю функцію пишемо іншу функцію inverse_mod яка знаходить обернений за множенням елемент до числа a за модулем n.

Далі реалізуємо функцію solve_mod_eq, використовуючи алгоритм дій з методичних вказівок, а також функції, реалізовані вище. Ця функція розв'язує лінійне порівняння і повертає всі корені у вигляді списку.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

Щоб виконати це завдання, було реалізовано функцію get_top_bigrams яка розбиває поданий текст на біграми, рахує їх та виводить відсортований у порядку спадання результат. Таким чином отримуємо 5 найчастіших біграм шифртексту.

Найчастіші біграми: **['вн', 'тн', 'дк', 'хщ', 'ун']**
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).

Це найважливіша частина роботи. Щоб зробити це, було спочатку реалізовано функцію bigrams_to_nums яка перетворює список біграм на список відповідних чисел за формулою:

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

Потім було написано функцію get_possible_keys, яка виконує всю основну роботу. Для початку беремо наші найпопулярніші табличні біграми російської мови, та топ 5 порахованих у попередньому пункті біграм. Потім перетворюємо їх на числа.

Далі ми формуємо можливі набори переходів, щоб на їх основі скласти системи рівнянь. Далі в цій же функції ми проходимося по цих наборах, розв’язуємо рівняння та отримуємо набори можливих ключів a та b. Всі обчислення виконувалися згідно формул та алгоритмів з методичних вказівок.

$$\begin{cases} Y^* \equiv aX^* + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

$$Y^* - Y^{**} \equiv a(X^* - X^{**}) \pmod{m^2}.$$

$$b = (Y^* - aX^*) \bmod m^2.$$

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

Для цього було реалізовано 3 функції:

- affine_decrypt - розшифровує текст з даним ключем
- text_detector - використовує декілька ознак, щоб перевірити чи є даний текст змістовним
- check_keys - об’єднує 2 попередні функції, перебирає всі можливі ключі, розшифровує текст цими ключами, та відкидає ключ, якщо текст не є змістовним та залишає у іншому випадку

Труднощі виникли з написанням функції text_detector. Було складно підібрати ознаки змістовного тексту, оскільки деякі з них не працювали з достатньою ефективністю, а деякі просто відсікали всі варіанти ключів. В кінці кінців вибір зупинився на підрахунку кількості літер, та порівняння з теоретичним значенням а також на індексі відповідності.
Принцип роботи розпізнавача:

1) спочатку розпізнавач рахує літери у даному тексті
2) далі перевіряється частота частих літер, тобто якщо найчастішою літерою не є “о” або “е”, то текст не змістовний
3) далі рахується індекс відповідності за алгоритмом з лабораторної роботи 2
4) значення індексу відповідності буде найближчим до теоретичного значення - **0.0553**

Язык	Индекс совпадений
русский	0.0553[1]

5) тепер порівнюємо значення індексу відповідності з теоретичним і робимо висновки, чи є текст змістовним

Таким чином було отримано єдиний можливий ключ **(654, 777)**. Коли шифртекст було розшифровано, то було виявлено, що літери “ы” та “ь” поміняні місцями, а також деякі інші неточності. Було зроблено спробу поміняти у алфавіті літери “ы” та “ь” місцями, і це допомогло. Було отримано змістовний відкритий текст.

Знайдене значення ключа - (654, 777)

Даний шифртекст

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнс
дуэммндтихкеюибщыцязкзхшвнос
ыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввцтнавпьгнуьввйнлхиьерддыцр
ихэкьзцэижцьехщмсэкжлрибуждэм
химьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщ
кщнфрхуюижсгцыззфрщихзтчщрихн
эпозтгфккчщкдмклыоьеынуййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництнду
ццоэивупхюфйчсьивйэютнрцшэбв
щншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндуз
йнкщнвнгоьцэииспьтуумщщшдекхнду
аошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьбиши
ыовдьезбтнмсэкжллрчсхщьрпьшв
шнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющьккюиеуяэзтьяяреурндуьцоэг
кмбобмщкскехюксдцтсывзтмсун
йьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйн
мсуншснхтуйнццмсяьмныонкцркч
ыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццв
нфиибхюпвиэислбиювинхыршьив
цнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюджджкеспьибубиюхщбуакикяеэ
дакаоццсвлбеилрлвцофкяяышвнун
хщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщм
бриввудябакфурщяэлчяздкаиьечслс
осэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихр
нфззфтнхщхиеуяэзтьяыуццыьбь
еелфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццс
ввныклрынпьювюсисцйвнихчщлр

акющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовяв
шньсйссцпрыоынчкццяьклхнщэюдри
исэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэик
зясусйнюйозвьтныэакосжцшншвюи
йдьяшншвосюсчязиьсунуллвихывхдсккламщубшскуаохщрнрцязакубсчфкяяосгйрщтнгб
фдзйьцэибусчжвавмнззфдыоиюшс
осюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмн
рншвйнввлвацшвьхаврщшнищюиьс
щожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшв
нюдцфвдыоияосунйпщнбкчзиввнмн
рьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуццщццспрчсэьлвзтк
лбулцшвюибщыцвивнуйвнакеи
чмывпвыэдчфкклццсвынуняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфь
модкчьяуфкойнкйдлцыцтнавчзфдыо
жяшсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсстгнхщщ
щфддбтьпнзкьеэдхнщьжвзтфрлцдкяяхь
овюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидроши
фкяяшнюдаоосунчзфпьцэилцмяэьсц
клжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвп
ьызмбйнвнцхпнуцязьсйядуулрибу
вдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпм
ьлриввеэяьхэфртгрулцузбщшьав
тулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфс
чсщьавпьскггыоющлхвииспьвиул
бутнзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрны
гщйеуйнзщшьявхщеуеидебупьесуз
ющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхчщмщявисчтжьамао
фисрябсчшижслбубщэнщфдэмсщябуб
чзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхсовпн
нчубакакхуямдкяяхсвнхбжсмкщн
щьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзй
ьцйныэвнхбрифкйыунрншьвнбкубье
бчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмсн
сибссвддцйнчсщнэпозцфибссщщ
убссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнх
щыглозфьцэидктнунэибунсхщав
ьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпн
оулцфрынщхыщмснфжврйвньркзскыщ
ссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьич
дрщдкикгбмщбущстссвйьшвоейу
лцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбццмсгцшвэр
зфвджяжвявшнмсчярщхьовюстымщкзищ
ссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнм
спбмщбущськмюннисдкдкцфжвйьдт
мщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщьккгнввшнивжврщрн
ыуоззнбкжлтьбцрныгйснжшдекцгеэ
юсрсхщньбиулбунхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлха
вьщсиеуобмбмщбущсфрмщчяовуп
мюосшнкуаохщмсэкццзтбьыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаих
щавиэжьчщоуобмблвыьрнунокпмшр

дцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзхщхурсунщхвввмдкорыус
нчзьяуиюшсвпнкурмщеувирсунсцць
блшэннбвамозмщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкию
щьккбыоскчицпьявицчзивяьочлц
свпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяякдункчзжсюсб
чкнбквьфзтнуноьюддкнхживнал
буыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщб
акксйнбжрисцвджцмнщькмыгьяье
хщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгьерынньэ
ьынавэкиютыннькиютноьакеишдщщ
швпвмндтихжцшнйнюирсыэьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвн
нстрсосщэтсяьяубщыцввяфжсюсунтс
чтгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнер
ссжофкеиябпвистнпвюскиосыр
ынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцу
фкщщцсунхдицяедьакхуумжсвнчр
лвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлс
иьпвтснфюирыюсцьаккнивжошижс
мкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяс
пнчкхуцфюижсшщязюсшсиэжьввшв
яэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнввв
вшнмьвврщозенйсуньейпфкаьтныо
еущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрь
йнвнцхмьакггмщшджсунлххэхьзт
лрэчбудквввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяьклхнг
цязвэкьзцэиьшсвмдьцюяусиебчду
ьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпьгбубсвй
навдьоспншсмкпрынкчмсхщнкой
щщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкриж
эпншнхщынгспнунрнгошддкяяфсшьыо
арфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккб
щшдекццжлывйквэпншнхщынгспныэ
рнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвюдцфю
ирыусунлрлцдкяяыуаокнввпьфзлц
внстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндц
вныкмбарбуябакфккчявпвлсзврщ
ьяшнынйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэяр
чсжвюсстибдцньтсюсстхщээрщьечщ
кзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуию
шннуяетнхщюиакфккчлспьыопьрц
мнрншбынлсюдризьяуфкшдвчсксчавзтрщхсщв

Відкритий текст

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепри
шлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснова
нииодинаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещ
енныйнарциссизмэтическаяценностьэтойдоброты этимнеоспаривается можетбытьэтовоо

бщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособенноясноп
тупающийвчрезвычайномслучаеобремененногосознаниясвоейвиныписателянетсомн
иячтоэтасимпатияпопричинеотождествлениярешительноопределилавыборматериалад
стоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступ
аполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступ
кукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмер
огонаследияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадосто
скийвгерманиибылобуреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадок
тологическойстрастикоторыйнеподдаетсяинойоценкенискакойсторонынебылонедост
кавоправданияхэтогостранногоинедостойногоповеденияучувствовиныкакэтонередкоб
аетуневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймого
овариватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсяврроссиюизбежав
аключенияявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточно
ницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавны
былаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрасс
ногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпокан
терялвсегоиграбыладлянеготакжесредствомсамонаказаниянесчетноеколичествораз
лонмолодойженесловоиличестноесловобольшенеиграть илинеиграть вэтотденьионна
шалэтословокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебя
едокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудов
ворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсяв
мчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестинаследу
щийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзаметилачто
отчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогдане
одвигалосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвя
ивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудовлетворенонаказани
иккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозволял
ебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодогописател
етрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорной
растиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтри
астеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтот
аленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляет
женщинаинакакиеудивительныедлянеесамойзакононарушенияеетолкаетнеожиданноеж
изненноевпечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкован
говоритоднакобезтакойоправдывающейтенденциигораздобольшепоказываетсовсемино
общечеловеческоеилискорееобщемужскоеитакоетолкованиестольявноподсказаночто
возможностиегонедопуститьдлясущностихудожественноготворчествахарактерночто
ательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждал
оупомянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтовр
сказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйслед
тойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпереж
ьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуж
далисьотказавшаясяоткакихбытонибылонадеждснасороквторомгодужизнионапопадает
овремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесреди
сехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственнос
юисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивого
юношиписательказкбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюда
щейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобыв
аркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинус
едоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочисле

ныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужд
енавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитье
гопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоивше
мусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетиграться снабжает
егоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуход
омпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожер
твоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпуте
шествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздыва
етнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущением
обнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушите
льдолгавернулсякигреонанапоминаетемуобегообещаниииноодержимыйстрастьюонбран
итсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыку
питьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсам
оубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправ
онасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпечатленияод
накопсихоанализучитчтоонавозникланаосновеумопостроямоговожденияпериодапол
овогосозреванияокаковомвожденииинекоторыевспоминаютсовершенносознательносог
ласноумопостроямомувожденииюматьдолжнасамаввестиюношувполовуюжизньдлясп
асенияегоотзаслуживающегоопасенияврединанизмастольчастыесублимирующиехудож
ественныепроизведенияывытекаютизтогожепервоисточникапороконанизмазамещаетсяпо
рокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательски
свидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляетсяэквив
алентомстаройпотребностивонанизмениоднимсловомкромесловаигранельзяназватьетее
аа

Висновки

В ході виконання комп’ютерного практикуму було виконано частотний аналіз афінного шифру, реалізовано допоміжні функції модулярної арифметики, а також розшифровано даний шифртекст за допомогою частотного аналізу. Також було побудовано примітивний розпізнавач мови, який дозволив автоматично відібрати ключ для розшифрування тексту.