МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

з дисципліни

Криптографія

"Криптоаналіз афінної біграмної підстановки"

Варіант 21

Виконав студент групи ФБ-91

Олександр Чернов

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування 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 №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.

Біграми, що зустрічаються найчастіше у шифрованому тексті ['фт', 'йо', 'дт', 'шж', 'дж']

Знайдений ключ - (90, 91)

Розшифрований текст

Болезньнаташибылатаксерьезначтоксчастиюееиксчастиюродныхмысльовсемтомчтобыло
причинойееболезниеепоступокиразрывсженихомперешлинаворойпланонабылатакбольна
чтонельзябылодуматьотомнасколькоонабылавиноватавовсемслучившемсятогдакаконанее
ланеспалазаметнохуделакашлялаибылакакдаваличувствоватьдокторавопасностинадобы
лодуматьтолькоотомчтобыпомочьейдоктораездиликнаташеиотдельноиконсилиумамиговор
илимногопофранцузскипонемецкииполатыниосуждалиодиндругогопрописывалисамыеразн
ообразныелекарстваотвсехимизвестныхболезнейнониодномуизнихнеприходилавголовута
простаямысльчтоимнеможетбытьизвестнатаболезнькоторойстрадаланаташакакнеможетб
ытьизвестнаниоднаболезнькоторойодержимживойчеловекибокаждыйживойчеловекимеетс
воиособенностиивсегдаимеетособеннуюисвоюновуюсложнуюнеизвестнуюмедицинеболез
ньнеболезньлегкихпеченикожисердцанервовитдзаписанныхвмедициненоболезньсостоящу
юизодногоизбесчисленныхсоединенийвстраданияхэтихоргановэтапростаямысльнемоглап
риходитьдокторамтакжекакнеможетприйтиколдунумысльчтооннеможетколдоватьпотомучт
оихделожизнисостояловтомчтобылечитьпотомучтозатоониполучалиденьгиипотомучтонаэт
оделоонипотратилилучшиегодысвоейжизниноглавноемысльэтанемоглаприйтидокторампо
томучтоонивиделичтоонинесомненнополезныибылидействительнополезныдлявсехдомаш

нихростовыхонибылиполезнынепотомучтозаставлялипроглатыватьбольнуюбольшейчасть
ювредныевеществавредэтотбылмалочувствителенпотомучтовредныевеществадавалисьв
маломколичественоониполезнынеобходимынеизбежнобылипричинапочемувсегдаестьибу
дутмнимыеизлечителиворожеигомеопатыиаллопатыпотомучтооониудовлетворялинравстве
ннойпотребностибольнойилюдейлюбящихбольнуюониудовлетворялитойвечнойчеловеческ
ойпотребностинадеждынаоблегчениепотребностисочувствияидеятельностикоторыеиспыт
ываетчеловеквовремястраданияониудовлетворялитойвечнойчеловеческойзаметнойвребе
нкевсамойпервобытнойформепотребностипотеретьтоместокотороеушибленоребенокубьет
сяитотчасжебежитврукиматеринянькидлятогочтобыемупоцеловалиипотерлибольноеместо
иемуделаетсялегчекогдабольноеместопотрутилипоцелуютребенокневеритчтобыусильней
шихимудрейшихегонебылосредствпомочьегоболиинадежданаоблегчениеивыражениесочу
вствиявтовремякакматьтретегошишкуутешаютегодокторадлянаташибылиполезнытемчтоо
ницеловалиитерлибобоуверяячтосейчаспройдетежеликучерсездитварбатскуюаптекуивозь
метнарубльсемьгривенпорошковипилюльвхорошенькойкоробочкеиежелипорошкиэтинепр
еменночерездвачасаникакнебольшеинеменьшебудетвотварнойводепринимательбольнаячто
жебыделалисоняграфиграфинякакбыонисмотрелинаслабуютающуюнаташуничегонепредп
ринимаяежелибынебылоэтихпилюльпочасампитьятепленькогокуринойкотлеткиивсехподро
бностейжизнипредписанныхдокторомсоблюдатькоторыесоставлялозанятиеиутешениедля
окружающихчемстрожеисложнеебылиэтиправилатемутешительнеебылодляокружающихд
елокакбыпереносилграфболезньсвоейлюбимойдочериежелибыоннезналчтоемустоилатыс
ячирублейболезньнаташиичтооннепожалеетещетысяччтобысделатьейпользуежелибыонн
езналчтоежелионанепоправитсяоннепожалеетещетысячиповезетеезаграницуитамсделает
консилиумыежелибыоннеимелвозможностирассказыватьподробностиотомкакметивьеифе
ллернепонялиафризпонялимудровещелучшеопределилболезньчтобыделалаграфиняежел
ибыонанемоглаиногдассоритьсясбольнойнаташейзаточтоонаневполнесоблюдаетпредписа
нийдоктораэдакникогданевыздоровеешьговорилаоназадосадойзабываясвоегореежелитын
ебудешьслушатьсядоктораиневовремяприниматьлекарствоведьнельзяшутитьэтимкогдаут
ебяможетсделатьсяпневмонияговорилаграфиняивпроизношенииэтогонепонятногонедляне
еоднойсловаонауженаходилабольшоеутешениечтобыделаласоняежелибыунейнебылорад
остногосознаниятогочтоонанераздеваласьтриночипервоевремядлятогочтобыбытьнаготове
исполнятьвточностивсепредписаниядоктораичтоонатеперьнеспитночидлятогочтобынепро
пуститьчасывкоторыенадодаватьмаловредныепилюлииззолотойкоробочкидажесамойната
шекотораяхотяиговорилачтоникакиелекарстваневылечатееичтовсеэтоглупостииейбылора
достновидетьчтодлянееделалитакмногопожертвованийчтоейнадобыловизвестныечасыпри
ниматьлекарстваидажеейрадостнобылоточтоонапренебрегаяисполнениемпредписанного
моглапоказыватьчтоонаневеритвлечениеинедорожитсвоейжизньюдокторездилкаждыйден
ьщупалпульссмотрелязыкинеобращаявниманиянаееубитоелицошутилснейнозатокогдаонв
ыходилвдругуюкомнатуграфиняпоспешновыходилазанимионпринимаясерьезныйвидипока
чиваязадумчивоголовойговорилчтохотяиестьопасностьоннадеетсянадействиеэтогопослед
неголекарстваичтонадождатьипосмотретьчтоболезньбольшенравственнаянографинястар
аясьскрытьэтотпоступокотсебяиотдокторавсовывалаемуврукузолотойивсякийразуспокое
нныма