Міністерство освіти і науки України

НТУУ «Київський політехнічний інститут»

Фізико-технічний інститут
Кафедра інформаційної безпеки

Криптографія

Лабораторна робота № 3

Виконали:

Студент
3 курсу ФТІ
групи ФБ-92
Сьомченко Дмитро

Студент
3 курсу ФТІ
групи ФБ-94
Стражник Богдан

Мета

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

Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

2. 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.

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

4. 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).

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

6. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

У ході роботи було реалізовано всі функції, що передбачались у завданнях. Було знайдено 5 найчастіших біграм шифрованого тексту, а саме ['еш', 'еы', 'шя', 'ск', 'до']. Біграми було переведено у числові значення згідно формули представленої у методичці до лабораторної роботи. Розглядаючи їх разом зі значеннями найчастіших біграм відкритого тексту було отримано деяку кількість ключів. Далі для кожного ключа було розшифровано текст. У ході розшифрування тексту для кожного ключа було перевірено вихідний текст на наявність у ньому заборонених біграм. Але заборонені біграми могли опинитися навіть у правильно розшифрованому тексті, таким чином, що перша літера біграми була кінцем слова а наступна літера була початком наступного слова, тому було створено додаткову перевірку на кількість таких біграм, тому що у відритому тексті таких біграми ну може бути багато. За допомогою даної перевірки ми отримали ключ для розшифрування та розшифрований текс.

Ключ: (390, 10)

Розшифрований текс:

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтое
гоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодоказатьэт
оневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогооб
ясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиунижений осуждениедостоевск
оговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпри
нялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгре
хпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместител
юотцаэтодаетнамнекотороепредставлениеопсихологическомоправданиинаказанийприсуждае
мыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверх
яизбавляясебятакимобразомотсамонаказанияготктознаетсложноеиизменчивоезначениеистери
ческихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсе
йполнотедостаточнотогочтоможнопредположитьчтоихпервоначальнаясущностьосталасьнеиз
меннойнесморянавсепоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосво
бодилсяотугрызенийсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопредел
илотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударственно
муавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюшкецарюооднаждыразы
гравшемуснимкомедиюубийствавдействительностинаходившуюстолькоразотражениевегопри
падкахздесьверхвзялопокаяниебольшесвободыоставалосьунеговобластирелигиознойпонедоп
ускающимсомненийсведениямондопоследнейминутысвоейжизнивсеколебалсямеждуверойиб
езбожиемеговысокийумнепозволялемунезамечатьтетрудностиосмысливаниякоторымпривод
итверавиндивидуальномповторениимировогоисторическогоразвитияоннадеялсявидеалехрист
анайтивыходиосвобождениеотгреховииспользоватьсвоисобственныестраданиячтобыпритязат
ьнарольхристаеслионвконечномсчетенепришелксвободеисталреакционеромтоэтообясняетсят
емчтообщечеловеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосв
ерхиндивидуальнойсилыинемоглабытьпреодоленадажееговысокойинтеллектуальностьюздесь
насказалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаип
одвергаемдостоевскогооценкеимеющейправонасуществованиелишьспристрастнойточкизрени
яопределенногомировоззренияконсерваторсталбынаточкузрениявеликогоинквизитораиоцени
валбыдостоевскогоиначеупрекправедливдляегосмягченияможнолишьсказатьчторешениедос
тоевскоговызваноочевиднозатрудненностьюегомышлениявследствиеневрозаедвалипростойсл
учайностьюможнообяснитьчтотришедеврамировойлитературывсехвременктрактуютоднуитуж
етемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскоговов
сехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсегоконеч
ноэтопредставленовдрамеоснованнойнагреческомсказаниииздесьдеяниесовершаетсяещесамим
героемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенноепризна
ниевнамеренииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбезан
алитическойподготовкивгреческойдраменеобходимоесмягчениеприсохраненииисущностимаст
ерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействительностькакчужд
ееемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамеренноиповсейвидим
остибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсяврасчеттаккаконможе
тзавоеватьцарицуматьтолькопослеповторениятогожедействиявотношениичудовищасимволиз
ирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокс
нятьеессебявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелая
винанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихологическиабсолютно
правильнованглийскойдрамеэтоизображеноболеекосвеннопоступоксовершаетсянесамимгеро

емадругимдлякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосудительныймот
ивсексуальногосоперничествауженщиныненуждаетсявзавуалированииравноиэдиповкомплекс
героямывидимкакбывотраженномсвететаккакмывидимлишьтокакоедействиепроизводитнагер
ояпоступокдругогоондолженбылбызаэтотпоступокотомститьностраннымобразомневсилахэто
сделатьмызнаемчтоегорасслабляетсобственноечувствовинывсоответствиисхарактеромневрот
ическихявленийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособностивып
олнитьэтозаданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуа
льнуюонпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпорк
ивэтомнаправлениироманрусскогописателяуходитнашагдальшеиздесьубийствосовершенодру
гимчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновнимиотношениямикакигер
ойдмитрийукоторогомотивсексуальногосоперничествооткровеннопризнаетсясовершенодруги
мбратомкоторомукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобыэ
пилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийц
аивотвречизащитниканасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодвухконца
хзавуалировановеликолепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшуюсущность
восприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознан
иясовершеннобезразличноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсяли
шьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьдоко
нтрастнойфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнас
лажденийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценав
высшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитри
йноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсявыра
жениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьсяпрезр
ениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевскогокпресту
пникудействительнобезграничнаонадалековыходитзапределысостраданиянакотороенесчастн
ыйимеетправоонанапоминаетблагоговениескоторымвдревностиотносилиськэпилептикуидуш
евнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругомслучаен
еслибыдругиеаа

Висновок: виконуючи дану лабораторну роботу ми отримали навички аналізу біграмного шифру афінної підстановки. Змогли знайти ключ, яким було зашифровано текс, та з його допомогою отримали відкритий текст. Згадали модульну арифметику та змогли реалізувати функції з цього розділу.