КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Варіант 4

Виконали: ФБ-12 Карабінський Василь, ФБ-12 Мосейко Олег

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 дотi, доки дешифрований текст не буде змістовним.

1.Реалізували 3 підпрограми, кожна з яких виконує свою роль.
`def extended_gcd_2(a, b)` реалізовує розширенийф алгоритм Евкліда.
`inverse(a, m):` реалізує інверсію елемента по модулю, в цій функції ми використовуємо функцію з розширеним алгоритмом Евкліда.
`def congurence(a, b, m):` ця функція розв'язує лінійну конгуренції та повертає усі розв'язки.

2.Модифікуваши програму для підрахунку біграм з 1 лаби ми знайшли, що найчастішими біграмами нашого шифртесту є ['еш', 'еы', 'шя', 'ск', 'до']

3. за формулою

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

знаходимо a, і для кожного можливого значення a знаходимо b за формулою

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

4. `def decrypt_text(text, a, b)` в цій функції ми спочатку перетворюємо біграми у числові значення по формулі:

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

а потім декодуємо кожну біграму за формулою

$$X_i = a^{-1}(Y_i - b) \bmod m^2$$

Також була написана програма для розпізнавання змістовного російського тексту, ми перевіряди текст по критерію частоти 1-грам.
найдений ключ: a =390, b = 10

Розшифрований шфиртекст:

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждался когдабылкараеминымобразомнодоказатьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогообясняется яточтоонпрошелнесломленнымчерезэтигодыбедствийиунижениййосуждениедостоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказаниятоткто знаетсложноеиизменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчтоихпервоначальнаясущностьосталасьнеизменнойнесморянавсеследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюшкецарюоднаждыразыгравшемусним комедиюубийствавдействительностинаходившуюстолькоразотраженноевегоприпадкахздесьверхвзялопокаяниебольшесвободыоставалосьуне говобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвоейжизнивсеколебалсямеждуверойибезбожиемеговысокий умнепозволялемунезамечатьтетрудностиосмысливанияккоторымприводитверавиндивидуальномповторениимировогоисторическогоразвитияонна деялсявидеалехристанайтивыходиосвобождениеотгреховииспользоватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконечномсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойсилыинемоглабытьпреодолена дажеговысокойинтеллектуальностьюздесьнасказалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдостоевскогооценкеимеющейправонасуществованиелишьспристрастнойточкизренияопределенногомировоззренияконсерваторсталбынато чкузренияевеликогоинквизитораиоценивалбыдостоевскогоиначеупрекс

праведливдляегосмягченияможнолишьсказатьчторешениедостоевского
вызваноочевиднозатрудненностьюегомышленияв следствиеневрозаедва
липростойслучайностьюможнообяснитьчтотришедеврамировойлитерату
рывсехвременктрактуютоднуитужетемутемуотцеубийствацарьэдипсофок
лагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраскрыв
аетсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсег
оконечноэтопредставленовдрамеоснованнойнагреческомсказанииздес
ьдеяниесовершаетсяещесамимгероемнобезсмягченияизавуалированияп
оэтическаяобработканевозможнаоткровенноепризнаниевнамеренииуби
тьотцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбез
аналитическойподготовкивгреческойдраменеобходимоесмягчениеприс
охранениисущностимастерскидостигаетсятемчтобессознательныймоти
вгерояпроецируетсявдействительностькакчуждоеемупринуждениенавя
занноесудьбойгеройсовершаетдеяниенепреднамеренноиповсейвидимос
тибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсявр
асчеттаккаконможетзавоеватьцарицуматьтолькопослеповторениятого
жедействиявотношениичудовищасимволизирующегоотцапослетогокакоб
наруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьеес
себявзвалитьеенапринуждениесостороныСудьбынаоборотвинапризнает
сяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянеспра
ведливымнопсихологическиабсолютноправильнованглийскойдрамеэтои
зображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимд
лякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосудит
ельныймотивсексуальногосоперничествауженщиныненуждаетсявзавуал
ированииравноиэдиповкомплексгероямывидимкакбывотраженномсветет
аккакмывидимлишьтокакоедействиепроизводитнагеропоступокдругог
оондолженбылбызаэтотпоступокотомститьностраннымобразомневсилах
этосделатьмызнаемчтоегорасслабляетсобственноечувствовинывсоотв
етствииихарактеромневротическихявленийпроисходитсдвигичувствов
иныпереходитвосознаниесвоейнеспособностивыполнитьэтозаданиепоя
вляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивнду
альнуюонпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпоза
слугамктоуйдетотпоркивэтомнаправлениироманрусскогописателяуход
итнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочелов
екомсвязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитр
ийукоторогомотивсексуальногосоперничествооткровеннопризнаетсяс
овершенодругимбратомкоторомукакинтереснозаметитьдостоевскийпер
едалсвоюсобственнуюболезньякобыэпилепсиютемсамымкакбыжелаясдел
атьпризнаниечтомолэпилептикневротиквомнеотцеубийцаивотвречизащ
итникапасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодву
хконцахзавуалировановеликолепнотаккакстоитвсеэтоперевернутьина
ходишьглубочайшуюсущностьвосприятиядостоевскогозаслуживаетнасм
ешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершеннобезраз
личноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсял

ишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветствов
алипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныд
вижимыйпервичнымипозывамиискательнаслажденийполныйскепсисацини
киэпилептическийпреступниквбратьяхкарамазовыхестьсценаввысшейс
тепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпост
игаетчтодмитрийноситвсебеготовностькотцеубийстваибросаетсяпере
днимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноознач
атьчтосвятойотстраняетотсебяискушениеисполнитьсяпрезрениемкуби
йцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевско
гокпреступникудействительнобезграничнаонадалековыходитзапредел
ысостраданиянакотороенесчастныйимеетправоонанапоминаетблагогов
ениескоторымвдревностиотносилиськэпилептикуидушевнобольномупре
ступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругомслу
чаенеслибыдругиеаа

Висновок

В ході виконання даної лабораторної роботи ми опанували навички частотного аналізу афінного шифру. маючи лише шифртекст ми спромоглися знайти ключі шифрування та отримати відкритий текст. Важливою частиною цієї лабораторної було опанування модулярної арифметики, використовувався розширений алгоритм Евкліда для розв’язання лінійних конгуренцій.