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 11

Виконав:
Студент III курсу ФТІ
Групи ФБ-06
Сулима Олексій
Перевірила:
Селюх П.В.

**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 шляхом розв’язання системи (1). ) ,(ba
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 роботи**

Зашифрований текст був взятий 11 варіанту(text_utf.txt).

5 найчастіших біграм шифротексту:

[('сг', 62), ('жэ', 60), ('нг', 59), ('ям', 56), ('цр', 53)]

Ключ: (300, 400)

Частина розшифрованого тексту:

поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябылоразглядетьврем яотвременионвосклицалагаилииэтотожезначитемувголовуприходилоещечтонибудьподходящееедляег оспискапотомдверьчутьстукнулаточновсеткуотмоскитовудариласьночнаябабочкалинашепнулауфман онаселарядомснимнакачеливоднойночнойсорочкенетоненькаякаксемнадцатилетняядевочкакоторуюе щенелюбятинетолстаякакпятидесятилетняяженщинакоторуюуженелюбятноскладнаяикрепкаяименно такаякакнадотаковыженщинывовсякомвозрастееслионилюбимыонабылаудивительнаяеетелокакиегос обственноевсегдадумалозанеетолькоподругомуоновынашивалодетейиливходиловпередилеовкаждую комнатучтобынеуловимоизменитьтамсамыйвоздухподстатьнастроениюмужаказалосьонаникогданеза думываетсянадолгомысльтотчаспередаваласьотееголовыплечампальцамипретворяласьвдействиетакн езаметноиестественночтолеонесмогбыдаинехотелизобразитьэтокакимилибочертежамиэтамашинаска залаонанаконецненужнаонанамдаотозвалсяонноиногданужнопозаботитьсяиодругихявотвседумаючто тудавставитькинокартинырадиоприемникистереоскопическиеочкиеслисобратьвсеэтовместевсякийче ловекпощупаетулыбнетсяискажетдадаэтоиестьсчастьесочинитьтакуюхитруюмеханикудумалончтопу скайучеловекапромоклиногиилиноетязваилиегомучаетбессонницаионворочаетсявпостеливсюночьна пролетидушуегогрызутзаботыавсеравнотвоямашинадастемусчастьекактамагическаякрупинкасоличто брошенавокеанивечнорождаетсольиобратилавсеморевсолянойрастворктонерасшибсябывлепешкули шьбыизобрестиатакуюмашинупустьемуответитнаэтотвопросцелыймирпустьответитвесьгородокпусть ответитженалинасмущенномолчаласидярядомснимнакачеляхиеемолчаниеговорилояснеевсякихсловл еотожеумолкзапрокинулголовуислушалкаксвищетветервгустойлиствемогучеговязанезабывайговори лонсебеиэтотшелестлистьевтоженужендлятвоеймашинычерезминутуверандаопустелапустыекачелин еподвижноповисливтемнотедедушкаулыбнулсявоснеонпочувствовалэтуулыбкуудивилсяейипроснулс

яполежалнемногоприслушалсяксебеипонялоткудаонавзяласьибоонуслышалнечтогораздоболееважно
ныхкараулитьросттравынамиллионахлужаекиллинойсаогайоилиайовыикакзаметятчтоонасозреладляс
енокосавтосамоеутровместофейерверковфанфарикриковпустьначинаетсявеликаябурнаясимфониякос
илоксрезающихсвежиетравынанеобятныхлуговыхпросторахвтотединственныйденьвгодукоторыйпон
астоящемузнаменуетсобойначалолюдямнадобыбросатьдругвдруганеконфеттиинесерпантинапригорш
нисвежескошеннойтравыдедушкахмыкнулчтотоужбольнодолгуюфилософиюразвелвсталподошелкок
нуивысунулсявласковыйсолнечныйсветтакиестьфорестерновыйжилецмолодойгазетчиккакраззаканчи
ваетряддоброеутромистерсполдингтакеехорошенькобиллсжаромкрикнулдедушкаивскореужесиделвн
изуиуплеталприготовленныйбабушкойзавтракширокоеоконобылораскрытоижужжаньекосилкисловно
подпевалозавтракуотэтойкосилкинадушестановитсяспокойнеезаметилдедушкатытолькопослушайтеп
ерьужнедолгонамееслушатьотозваласьбабушкаипоставиланастолгоркупшеничныхлепешекбиллфоре
стерпосеетсегодняновыйсорттравыеененадобудеткоситьнепомнюкактамонаназываетсяноонакаквыра
стетскольконужнотаксамаиостановитсяибольшенерастетдедушкасизумлениемуставилсянаженудовол
ьноглупаяшуткасказалоннаконецидипосмотрисамбиллфорестерговоритэтоземленапользусказалабабу
шкаонужепривезновыесеменаонисложенызадомомвмаленькихкорзинкахнужновразныхместахвырыть
ямкиизасыпатьтудасеменакконцугодановаятраваубьетвсюстаруюитогдаможешьпродаватьсвоюкосил
куонатебебольшенепонадобитсядедушкасорвалсясостулаимигомвыскочилводворбиллфорестеростан
овилкосилкуижмурясьотсолнцасулыбкойподошелкнемуваттактосказалонвчеракупилновыесеменадай
думаюзасеювамлужайкупокаясвободенаменяпочемунеспросилилужайкатовсетакимоязакричалдедуш
каядумалвыбудетедовольнымистерсполдингничегоянедоволенпокажитемнеэтучертовутравуонистоял
ивозлемаленькихчетырехугольныхкорзиноксновомоднымисеменамидедушкаподозрительнопотыкало
днуизнихноскомбашмакапомоемуэтосамаяобыкновеннаятраваавыуверенычтовасненадулиявкалифор
ниивиделкаконарастетвотнастольковырастетивсееслитолькоонаприживетсявздешнемклиматенамуже
набудущийгоднепридетсякаждуюнеделюподстригатьлужайкувтомтоибедасвашимпоколениемсказалд
едушкамнестыднозавасбиллаещежурналиствыготовыуничтожитьвсечтоестьнасветехорошеготолькоб
ытратитьпоменьшевременипоменьшетрудавотчеговыдобиваетесьоннепочтительнопнулкорзинкуного
йвотпоживетесмоетогдапойметечтомелкиерадостикудаважнеекрупныхраноутромповеснепрогуляться
пешкомневпримерлучшечемкатитьвосемьдесятмильвсамомроскошномавтомобилеазнаетепочемупот
омучтовсевокругблагоухаетвсер

**Висновок**

В ході комп’ютерного практикуму були отримані навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опановані прийоми роботи в модулярній арифметиці. Були реалізовані підпрограми з необхідними математичними операціями, знайдені найчастіші 5 біграм у наданому шифртексті та у російській мові, після чого отримані пари та ключі. За допомогою автоматичного розпізнавача змістовності тексту був отриманий ключ та розшифрований текст.