МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ
ТА СПОРТУ УКРАЇНИНАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ

ПОЛІТЕХНІЧНИЙ

ІНСТИТУТ»ФІЗИКО-

ТЕХНІЧНИЙІНСТИТУТ

Криптографія

Комп’ютерний практикум №3

Виконали:

студенти групи

ФБ-95

Товстенко Артем, Тараканов Егор

Перевірив(ли):

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.

Хід роботи:

1. Було створено файл filtered.txt, який записував наш var3.txt(зашифрований текст за нашим варіантом) в одну строчку для кращого розуміння тексту программою.
2. Пошук біграм, через регулярний вираз та їх сортування(bigrams).
3. Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда(obernene), розв'язуванням лінійних порівнянь(keygenerator).
4. Визначили 5 найчастіших біграм шифротексту:
   варіанту 3 ['тд', 'рб', 'во', 'щю', 'ет'](perebor)
   Та знайшли «кандидатів» на ключ(keygenerator+posiblek).

5. Для кожного знайденого кандидата на ключ дешифрували текст та зробили перевірку(чи є змістовним текстом російською мовою). Перевірку здійснили шляхом порівняння найбільш зустріваних літер ВТ і найбільш зустріваних літер російської мови, повторили дане порівняння для найменш зустріваних букв і для найчастіших біграм ВТ.
6. С

Розшифрування (ключ: 199, 700):

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекавовсякомслучаеоноглавныйисточн икчувствавинынеизвестноединственныйлиисследованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностииск уплениянооттюдьнесущественноединственныйлиэтоисточникпсихологическоеположениесложноинуждаетсявобясненияхотношен иемальчикакотцукакмыговоримамбивалентнопомимоненавистиизакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобы чнонекотораядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызыв аетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтоналкиваетсянакрупноепрепятствиевопределенныйм оментребенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказаниечерезкастрациюизст рахакастрациитоестьвинтересахсохранениясвоеймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустраненияо тцапосколькуэтожеланиеостаетсявобластибессознательногоонояВляетсяосновойдляобразованиячувствавинынамкажетсячтомыопи салинормальныепроцессыобычнуюсудьбутакназываемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдал ьнейшиеосложненияеслиуребенкасильнеразвитконституционныйфакторназываемыйнамибисексуальностьютогдаподугрозойпоте римужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянам естоматерииперенятьеероль кабекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчтоон долженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснениеобапорываненависть котцуивлюбленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследствиестра хапередвнешнейопасностьюкастрацией влюбленностьжевотцавоспринимаетсякаквнутренняяопасностьпервичногопозываотораяп осутисвоейсновавозвращаетсяктойжевнешнейопасностистрахпередотцамделаетненавистькотцунеприемлемойкастрацияужаснакак вкачествекарытакиценылюбвиизобоихфакторовВытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияикастрации следуетназватьнормальнымпатогеническоеусилениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойустановкия рковыраженнаябисексуальнаясклонностьстановитсятакимобразомоднимизусловийилиподтверждениневрозаэтусклонностьочеви дноследуетпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвидевтомзначениикакоеимелавего жизнидружбасмужчинамивегодостранностинежномотношениикоспернкамвлюбвиивегопрекраснопониманииположенийобясни мыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведенийсожалеюноничегонемо гуизменитьеелиподробностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанал изечитателюпокажутсябезвкусныМиималовероятнымипредполагаютчтоименнокомплекскастрацииБудетотклоненсильнеевсегоносм еюуверитьчтопсихоаналитическийопытставитименноэтиявленияВневсякогосомненияинаходитвнихключклюбомуневрозуиспытаем жеговслучаетакназываемойэпилепсиинашегописателянонашемусознаниютакчуждытеявленияВовластикоторыхнаходитсянашабес сознательнаяпсихическаяжизньуказаннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытесненияненавистикотцунов ымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянноеместоэтоотождествлениевоспринимается на шимянопредставляетсобойвнемособуюинстанциюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанци юнашимсверхяиприписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецбылсуровнасильственжестокна шесверхяперенимаетотнегоэтикачестваивегоотношениикяснованозникаетпассивностькоторойкакразнадлежалобыбытьвытесненно йсверхяталосадистическимястановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашемявозникаетбольшаяпотреб ностьвнаказаниииятчастиотдаетсебякактаковоевраспоряжениесудьбыотчастиженаходитудовлетворениевжестокомобращениисни мсверхясознаниевиныкаждаякараявляетсяведьвосновесвоейкастрацией икактаковаяосуществлениемизначальногопассивногоотношения котцуисудьбавконцеконцовлишьдальнейшаяпроекциятцанормальныеявленияпроисходящиеприформированиисовестидолжн ыпоходитьнаописанныездесьанормальныенамещенеудалосьустановитьразграниченияМеждунимизамечаетсячтонаибольшаярользд есьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженственностиИещекакслучайныйфакторимеетзначениеявляе тсяливнушающийстрахотецивдействительностиособеннонасильственнымэтоотносится кдостоевскомуфактеГоисключительногочув ствавиныравнокакимазохистскогообразажизнимысводимкгеособенноярковыраженномукомпонентуженственностидостоевскогом ожноопределитьследующимобразомособенносильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяо тзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкранееузнаннымкомпонентамегосуществаран нийсимптомприпадковсмертиможнорассматриватькакотождествлениесвоегоясотцомдопущенноевкачественаказаниясосторонысве рхятызахотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужет еперьтебяубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазохистски мпосредствомнаказаниятоестьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшевобщемотношениемеждулично стьюиобектомотцаприсохранениигосодержанияперешловотношениемеждуяисверхяноваяинсценировканаторойсценетакиеинфан тильныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедаетимвдальнейшемпищинохарактеротцаостаетсятем жесамымнетонухудшаетсясгодамитакимобразомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузломуот цустановитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделефантазияисталареальностьювсемерызащитытеперьа

Висновок: В ході виконання лабораторної роботи, опанували навички аналізу поліафватної підстановки на прикладі афінної біграмної підстановки, використали деякі математичні процедури для знаходження потрібних нам даних.