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. Пошук біграм для нашого шифротексту (get_ngram_freq).
2. Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда(reverse), розв'язуванням лінійних порівнянь(linear_equation).
3. Визначили 5 найчастіших біграм шифротексту:
   варіанту 3 ['тд', 'рб', 'во', 'щю', 'ет'](perebor)
   Та знайшли «кандидатів» на ключ(findkey).
4. Для кожного знайденого кандидата на ключ дешифрували текст та зробили перевірку(чи є змістовним текстом російською мовою). Перевірку здійснили шляхом порівняння найбільш поширених літер

ВТ і найбільш поширених літер російської мови, повторили дане порівняння для найменш поширених букв і для найчастіших біграм ВТ.

5. Знайшли найчасті біграми нашого тексту, та розшифрували текст за допомогою ключа


## Розшифрування ( ключ: 199, 700):

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекавовсякомслучаеоноглавныйисточн
икчувствавинынеизвестноединственныйлиисследованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностииск
уплениянноотнюдьнесущественноединственныйлиэтоисточникпсихологическоеположениесложноинуждаетсявобясненияхотношен
иемальчикакотцукакмыговоримамбивалентнопомимоненавистиизакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобы
чнонекотораядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызыв
аетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтоналкиваетсянакрупноепрепятствиевопределенныйм
оментребенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказаниечерезкастрациюизст
рахакастрациитоестьвинтересахсохранениясвоеймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустранению
тцапоскольку этожеланиеостаетсявобластибессознательногооноявляетсяосновойдляобразованиячувствавинынамкажетсячтомыопи
салинормальныепроцессыобычнуюсудьбутакназываемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдал
ьнейшиеосложненияеслиуребенкасильнееразвитконституционныйфакторназываемыйнамибисексуальностьютогдаподугрозойпоте
римужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянам
естоматерииперенятьеероликакобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчтоон
долженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснениеобапорыванеависть
котцуивлюбленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследствиестра
хапередвнешнейопасностьюкастрацийвлюбленностьжевотцавоспринимаетсякаквнутренняяопасностьпервичногопозыкоторая
осутисвоейсновавозвращаетсяктойжевнешнейопасностистрахпередотцамделаетненавистькотцунеприемлемойкастрацияужаснакак
вкачествекарытакиценылюбвиизобоихфакторовывытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияикастрации
следуетназватьнормальнымпатогеническоеусилениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойустановкия
рковыраженнаябисексуальнаясклонностьстановитсятакимобразомоднимизусловийилиподтвержденийневрозаэтусклонностьочеви
дноследуетпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвидевтомзначенииикакоеимелавего
жизнидружбасмужчинамивегодостранностинежномотношениикоперникамвлюбвиивегопрекраснопониманииположенийобясни
мыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведенийсожалеюноничегонемо
гуизменитьеелиподробностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанал
изечитателюпокажутсябезвкусныимиималовероятнымипредполагаючтоименнокомплекскастрациибудетотклоненсильнеевсегоносм
еюуверитьчтопсихоаналитическийопытставитименноэтиявленияявневсякогосомненияинаходитвнихключклюбомуневрозуиспытаем
жееговслучаетакназываемойэпилепсиинашегописателянонашемусознаниютакчуждытеявленияявластикоторыхнаходитсянашабес
сознательнаяпсихическаяжизньуказаннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытесненияненавистикотцунов
ымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянноместоэтоотождествлениевоспринимаетсяна
шимянопредставляетсобойвнемособуюинстанциюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанци
юнашимсверхяиприписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецбылсуровнасильственжестокна
шесверхяперенимаетотнегоэтикачествавивеготношениикясновавозникаетпассивностькоторойкакразнадлежалобыбытьвытесненно
йсверхсталосадистическимстановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашемявозникаетбольшаяпотреб
ностьвнаказаниииияотчастиотдаетсебякактаковоераспоряжениесудьбыотчастиженаходитудовлетворениевжестокомобращениисни
мсверхясознаниевиныкаждаякараявляетсяведьвосновесвоейкастрацией икактаковаяосуществлениемизначальногопассивноготношения котцуисудьбавконцеконцовлишьдальнейшаяпроекцияотцанормальныеявленияпроисходящиеприформированиисовестидолжны походитьнаописанныездесьанормальныенамещенеудалосьустановитьразграничениямеждунимизамечаетсячтонаибольшаярольздесьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженственностиищекакслучайныйфакторимеетзначениеявляется ливнушающийстрахотецивдействительностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключительногочувствавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраженномукомпонентуженственностидостоевскогом ожноопределитьследующимобразомособенносильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяо тзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкранееузнаннымкомпонентамегосуществаран нийсимптомприпадковсмертиможнорассматриватькакотождествлениесвоегоясотцомдопущенноевкачественаказаниясосторонысве рхятызахотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужет еперьтебяубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазохистски мпосредствомнаказаниятоестьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшевобщемотношениемеждулично стьюиобектомотцаприсохраненииегосодержанияперешловотношениемеждуяисверхяноваяинсценировканавторойсценетакиеинфан тильныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедаетимвдальнейшемпищинохарактеротцаостаетсятем

жесамымнетонухудшаетсясгодамитакимобразомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузломуот
цустановитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделефантазиясталареальностьювсемерызащитытеперьа

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.