A drawing of a building

Description automatically generated

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ “КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Студенти групи ФБ-22

Шеїна Еліна, Мартинюк Артем

Варіант - 1

КИЇВ 2024

**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**

Спочатку створимо функцію, яка буде обчислювати обернений до а елемент:

A computer screen shot of a black screen with white text

Description automatically generated

Функція find\_modular\_inverse реалізує розширений алгоритм Евкліда, приймаючи на вхід число a та модуль, і повертає список, що містить значення, серед яких gcd та обернений елемент.

Далі, створюємо функцію, яка вирішує лінійне порівняння:

A computer screen shot of text

Description automatically generated

Приймає a, b та модуль, повертає або одне значення, або декілька, якщо gcd>1

Знаходимо найчастіші біграми з ШТ:



A screen shot of a computer code

Description automatically generated

Вивід:

A screen shot of a black background

Description automatically generated

Біграми «рн», «ыч», «нк», «цз», «тч».

Пишемо код, який зіставляє найбільш поширені біграми ШТ з найпоширенішими біграмами російської мови, наведеними у методичних матеріалах. Потім цей код перетворює кожну біграму з пари в числове значення за формулою: перша\_літера\*31 + друга\_літера. Далі обчислює пару ключів (a, b) для кожної комбінації з двох пар значень:

A screen shot of a computer program

Description automatically generated

Вивід:  
A black background with white spots

Description automatically generated

Обчислювали ключ за допомогою цих формул:

A black and white math equation

Description automatically generated**A black and white math equation

Description automatically generated**

Далі, для кожного ключа здійснюємо дешифрування тексту за допомогою оберненого афінного шифру. Отримане число перетворюється в біграму за допомогою оберненої схеми до формули (перша\_літера\*31 + друга\_літера):

A computer screen shot of a program code

Description automatically generated

Записавши масив рідкісних біграм російської мови, розбиваємо кожен розшифрований текст на біграми та порівнюємо їх з рідкісними. Потім сортуємо список розшифрованих текстів за кількістю рідкісних біграм у порядку зростання і визначаємо найбільш ймовірний ключ – (13, 151).

A screenshot of a computer program

Description automatically generated

A black screen with white text

Description automatically generated

Текст розшифровано.

**Розшифрований текст:**многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейнассложностинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайшихдостижениймировойлитературыпереоценитькотороеневозможноксожалениюпередпроблемойписательскоготворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяегочеловекомвысоконравственнымнатомоснованиичтотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубочайшиебездныгреховностимыигнорируемодносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспытываемоеискушениеприэтомемунеподдаваяськтожепопеременнотогрешиттораскаиваясьставитсебевысокиенравственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногопринципанравственностинеобходимостиотречениявтовремякакнравственныйобразжизнивпрактическихинтересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварваровубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюхарактернаярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыдостоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозывовиндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинениюмирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационализмукчемуменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместобольшойличностидостоевскийупустилвозможностьстатьучителемиосвободителемчеловечестваиприсоединилсяктюремщикамкультурабудущегонемногимбудетемуобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюнеудачупомощипостиженияисилелюбвиклюдямемубылоткрытдругойапостольскийпутьслужениянампредставляетсяотталкивающимрассматриваниедостоевскоговкачествегрешникаилипреступниканоэтоотталкиваниенедолжноосновыватьсянаобывательскойоценкепреступникавыявитьподлиннуюмотивациюпреступлениянедолгодляпреступникасущественныдвечертыбезграничноесебялюбиеисильнаядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляихпроявленийявляетсябезлюбовностьнехваткаэмоциональнооценочногоотношениякчеловекутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотребностьвлюбвииегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьимститьнапримерпоотношениюкегопервойженеиеелюбовникунотогдавозникаетвопросоткудаприходитсоблазнпричислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимущественнонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитакихсклонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартнымиграмможетбытьсексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешаетсяследующимобразомсильнаядеструктивнаяустремленностьдостоевскогокотораямоглабысделатьегопреступникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизнутриитакимобразомвыразиласьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчертвыявляющихсявегораздражительностимучительственетерпимостидажепоотношениюклюбимымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиствовневважномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдобродушнейшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывыделилитрифактораодинколичественныйидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремленностькперверзиикотораядолжнабылапривестиегоксадомазохизмуилисделатьпреступникомиегонеподдающеесяанализутворческоедарованиетакоесочетаниевполнемоглобысуществоватьибезневрозаведьбываютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритязаниипервичныхпозывовипротивоборствующихимторможенийприсоединяясюдавозможностисублимированиядостоевскоговсеещеможнобылобыотнестикразрядуимпульсивныххарактеровноположениевещейзатемняетсяналичиемневрозанеобязательногокакбылосказаноприданныхобстоятельствахновсежевозникающеготемскореечемнасыщеннееосложнениеподлежащеесосторонычеловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтооноприэтойпопыткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназывалсебясамидругиетакжесчиталиегоэпилептикомнатомоснованиичтоонбылподвержентяжелымприпадкамсопровождавшимисяпотерейсознаниясудорогамиипоследующимупадочнымнастроениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневрозакоторыйвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполнойуверенностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпадковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныавовторыхпотомучтопониманиесвязанныхсэпилептоиднымиприпадкамиболезненныхсостоянийостаетсянеясныма