

Міністерство освіти і науки, молоді та спорту України

Національний технічний університет України

“Київський політехнічний інститут”

Фізико-Технічний інститут

«Криптографія»   
Лабораторна робота №3  
«Криптоаналіз афінної біграмної підстановки»

Виконали:

Студентки 3 курсу ФТІ

Групи ФБ-92

Казанкова Марина та Шаповал Ольга

Варіант - 4

**Мета роботи:** Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Загальний код програми знаходиться в файлі "main.py". Шифрований текст знаходиться у файлі V4, а розшифрований – txt.txt

**Хід роботи**

1. Відбувається зчитування зашифрованого тексту, його очищення

2. Ділення шифрованого тексту на біграми

3. Виділення 5 найчастіших біграм

4. Розрахунок числових значень для кожної біграми всього тексту

5. Визначення можливих перестановок популярних біграм з тексту із популярними біграмами з мови;

6. Знаходження комбінацій пар біграм та складення системи порівнянь;

7. Розрахунок ключів для кожної комбінація та виділення унікальних

8. Розшифрування тексту з кожним ключем і перевірка тексту на наявність недопустимих біграм

9. Відкидання ключів, у яких а = 0

10. Маємо один вірний ключ, яким розшифровуємо текст

11. Розшифрований текст записуємо у файл txt.txt

12. Вручну перевіряємо текст на змістовність.

Наш ключ = (390, 10)

**Розшифрований текст :**

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодоказатьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиуниженийосуждениедостоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказаниятотктознаетсложноеиизменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчтоихпервоначальнаясущностьосталасьнеизменнойнесморянавсепоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюшкецарюоднаждыразыгравшемуснимкомедиюубийствавдействительностинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяниебольшесвободыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвоейжизнивсеколебалсямеждуверойибезбожиемеговысокийумнепозволялемунезамечатьтетрудностиосмысливанияккоторымприводитверавиндивидуальномповторениимировогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотгреховииспользоватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконечномсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойсилыинемоглабытьпреодоленадажееговысокойинтеллектуальностьюздесьнасказалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдостоевскогооценкеимеющейправонасуществованиелишьспристрастнойточкизренияопределенногомировоззренияконсерваторсталбынаточкузрениявеликогоинквизитораиоценивалбыдостоевскогоиначеупрексправедливдляегосмягченияможнолишьсказатьчторешениедостоевскоговызваноочевиднозатрудненностьюегомышлениявследствиеневрозаедвалипростойслучайностьюможнообяснитьчтотришедеврамировойлитературывсехврементрактуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсегоконечноэтопредставленовдрамеоснованнойнагреческомсказанииздесьдеяниесовершаетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбезаналитическойподготовкивгреческойдраменеобходимоесмягчениеприсохранениисущностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействительностькакчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамеренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторениятогожедействиявотношениичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьеессебявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихологическиабсолютноправильнованглийскойдрамеэтоизображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничествауженщиныненуждаетсявзавуалированииравноиэдиповкомплексгероямывидимкакбывотраженномсвететаккакмывидимлишьтокакоедействиепроизводитнагерояпоступокдругогоондолженбылбызаэтотпоступокотомститьностраннымобразомневсилахэтосделатьмызнаемчтоегорасслабляетсобственноечувствовинывсоответствиисхарактеромневротическихявленийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособностивыполнитьэтозаданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэтомнаправлениироманрусскогописателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитрийукоторогомотивсексуальногосоперничестваоткровеннопризнаетсясовершенодругимбратомкоторомукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийцаивотвречизащитниканасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодвухконцахзавуалировановеликолепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершеннобезразличноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсялишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнаслажденийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввысшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитрийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотороенесчастныйимеетправоонанапоминаетблагоговениескоторымвдревностиотносилиськэпилептикуидушевнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругомслучаенеслибыдругиеаа