



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 $a = 0$
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 :

если правда что Достоевский в Сибири не был подвержен припадкам то это лишь подтверждает очто его припадки были его карой он более в них не нуждался когда был караемым образом но доказать это не возможно скорее этой необходимости в наказании для психической экономии Достоевского объясняется то что он прошел несломленным через эти годы бедствий и унижений о суждении Достоевского как человека политического преступника было несправедливо и он должен был это знать но он принял это не заслуженное наказание от башки царя как замену наказания заслуженного им за свой грех по отношению к своему собственному отцу в месте самонаказания он дал себя наказывать заместителю отца это дает нам некоторое представление о психологическом оправдании наказания и присуждаемых обществом это на самом деле так многие из преступников жаждут наказания его требуют сверх избавляя себя таким образом от самонаказания тот кто знает сложное и изменчивое значение истерических симптомов поймет что мы здесь не пытаемся добиться смысла припадков Достоевского во всей полноте недостаточного что можно предположить что их первоначальная сущность осталась неизменной несмотря на все последующие наслоения можно сказать что Достоевский так никогда не освободился от угрызений совести в связи с намерением убить отца это лежащее на совести время определило также его отношение к двум другим сферам покоящимся на отношении к отцу к государственному авторитету и к веревбогав в первой он пришел к полному подчинению убавляя к царю однажды сыгравшему с ним комедию убийства в действительности находившуюся столько раз отражение в его припадках здесь верх взяло покаяние больше свободы оставалось у него во власти религиозной по недопуская сомнений сведениям о последней минуте своей жизни все колебался между верой и безбожием его высокий ум не позволял ему замечать трудности осмысливания к которым приводит вера в индивидуальном повторении мирового исторического развития он надеялся в идеале Христа и тивых освобождение от грехов и использовать свои собственные страдания чтобы притязать на роль Христа если он в конечном счете не пришел к свободе и стал реакционером то это объясняется тем что общечеловеческая сыновья вина на которой строится религиозное чувство достигла у него сверхиндивидуальной силы и не могла быть преодолена даже его высокоинтеллектуальностью здесь насказалось бы можно упрекнуть в том что мы отказываемся от беспристрастности психоанализа и подвергаем Достоевского оценке и имеющей право на существование и лишь с пристрастной точки зрения определенного мировоззрения консерватор стал бы на точку зрения великого инквизитора и оценивал бы Достоевского иначе упреки справедливы для его смягчения можно лишь сказать что решение Достоевского вызвано очевидно затрудненностью его мышления вследствие неvroза едва ли простой случайностью можно объяснить что три шедевра мировой литературы всех времен трактуют одну и ту же тему отцеубийства царь Эдип и Софокл Агамлет Шекспира и братья Карамазовы Достоевского во всех трех раскрываются мотивы деяния сексуальное соперничество и заженщины прямо все го конечно это представлено в драме основанной на греческом сказании из здесь деяние совершается еще с самим героем но без смягчения изавуалирования поэтическая обработка невозможна откровенное признание в намерении убить отца какому мы добиваемся при психоанализе кажется непереносимым безаналитической подготовки в греческой драме необходимо смягчение при сохранении сущности мас

терски достигается тем, что бессознательный мотив героя проецируется в действительность как чуждое ему принуждение навязанное судьбой. Герой совершает деяние не преднамеренно и по всей видимости без влияния женщины и все же это стечение обстоятельств принимается в расчет так как он может завоевать царицу, мать только после повторения того же действия в отношении чудовища, символизирующего отца после того как обнаруживается и оглашается его вина. Не делается никаких попыток снять ее с себя, ввалив ее на принуждение со стороны судьбы, на оборот и признается, как в целом вина наказывается, что рассудку может показаться несправедливым, но психологически абсолютно правильно. В английской драме это изображено более косвенно, поступок совершается не самим героем, а другим, для которого этот поступок не является отцеубийством, поэтому предвзятый мотив сексуального соперничества у женщины не нуждается в завуалировании и равно эдипов комплекс героя мы видим как бы в отраженном свете, так как мы видим лишь то, какое действие производит на героя поступок другого, он должен был бы за этот поступок отомстить, но странным образом не в силах это сделать, мы знаем, что его расслабляет собственное чувство вины, в соответствии с характером невротических явлений происходит сдвиг чувства вины, переходит в сознание, и свое inability выполнить это задание появляются признаки того, что герой воспринимает эту вину как сверхиндивидуальную, он презирает других не менее чем себя, если обходиться с каждым по заслугам, кто уйдет от порки в этом направлении, роман русского писателя уходит на шаг дальше и здесь убийство совершено другим человеком, но человек связан с ним судьбой, такими же сыновними отношениями, как и герой, Дмитрий у которого мотив сексуального соперничества откровенно признается, совершено другим, братом, которому как интересно заметить, Достоевский передал свою собственную болезнь, как бы эпипсимум, тем самым, как бы желая сделать признание, что мол эпилептик, невротик, в нем отцеубийца и в отрыве защитника на суд, даже известная насмешка над психологией, она мол палка о двух концах, завуалировано, великопотопа, как стоит все это перевернуть, находишь глубочайшую сущность восприятия Достоевского, заслуживает насмешки, отнюдь не психология, судебный процесс, дознания, совершенно безразлично, кто этот поступок совершил, на самом деле психология интересуется лишь тем, кто его в своем сердце желал, кто по его совершению его приветствовал, и поэтому вплоть до контрастной фигуры, аleshiv, в себ, братья, равновинны, движимый первичными позывами, и искатель наслаждений, полный скепсиса, циник, и эпилептический преступник, в братьях Карамазовых есть сцена в высшей степени характерная для Достоевского, из разговора с Дмитрием старец постигает, что Дмитрий носит в себе готовность к отцеубийству, и бросается перед ним, на колени, это не может являться выражением восхищения, должно означать, что святой отстраняет от себя искушение, исполнить презрение к убийце, или им погнущаться, и поэтому перед ним смиряется симпатия Достоевского к преступнику, действительно безгранична, она далековато выходит за пределы сострадания, на которое несчастный имеет право, она напоминает благоговение, некоторые в древности относились к эпилептику и душевно больному, преступнику, для него почти спаситель, взявший на себя вину, которую в другом случае несли бы другие, а

