

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

«Криптографія»
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
«Криптоаналіз афінної біграмної підстановки»
Варіант 4

Виконали:

Студенти 3 курсу
Групи ФБ-04
Осіпчук Антон
Подима Катерина

Мета роботи:

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

Хід роботи

Ділимо шифрований текст на біграми та виявляємо найчастіші з них. Далі перевіряємо текст на наявність неможливих біграм у мові. Знаходимо ключ, яким розшифровуємо текст.

Ключ = (390, 10)

если правда что достоевский в сибири не был подвержен припадкам то это лишь подтверждает то что его припадки были его карой он более в них не нуждался ко да 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 осуждение достоевского как качества политического преступника было несправедливым и он должен был это знать но он принял это незаслуженно наказание от батюшки царя как замену наказания заслуженного им за свой грех по отношению к своему собственному отцу в месте наказания он дал себя наказывать заместителю отца а то дает нам некоторое представление о психологическом оправдании наказания и присуждаемых обществом это на самом деле так многие из преступников жаждут наказания его требуют сверх и избавляя себя таким образом от наказания тот кто знает сложное и изменчивое значение истерических симптомов в той метче то мы здесь не пытаемся добиться смысла припадков достоевского в ее полноте недостаточного что можно предположить что их первоначальная сущность осталась неизменной несмотря на все последующие наслоения можно сказать что достоевский так или иначе освободился от угрызений совести в связи с намерением убить отца это лежащее на совести бремя определило также его отношение к двум другим сферам покоящимся на отношении к отцу к государству и к авторитету и к веревкам в первой он пришел к полному подчинению батюшке царю однажды разыгравшем у нас комедию убийства в действитель-

ности находившую столько раз отражение в его припадках здесь, верх взяло покаяние, больше свободы оставалось у него в области религиозной, понеже допускающим сомнения сведениям до последней минуты своей жизни все колебалось между верой и безбожием, его высокий ум не позволял ему замечать трудности осмысливания к которому приводит вера в индивидуальном повторении мирового исторического развития, он надеялся в идеале христианам выйти из освобождения 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 высокой интеллектуальностью, здесь на сказало бы можно упрекнуть в том, что мы отбрасываемся от беспристрастности психоанализа и подвергаем Достоевского оценке имеющей право на существование лишь с пристрастной точки зрения определенного мировоззрения, консерватор стал бы на точку зрения великого инквизитора и оценивал бы Достоевского иначе, упрек справедлив для его смягчения, можно лишь сказать, что решение Достоевского вызвано очевидно затрудненностью его мышления, вследствие невраждебности и простой случайностью можно объяснить, что три шедевра мировой литературы всех времен трактуют одну и ту же тему, о цареубийстве, царь Эдип, Софокл, Гамлет, Шекспир, братья Карамазовы Достоевского, во всех трех раскрывается мотив деяния, сексуальное соперничество из-за женщины, прямое и всеобщее, нечуждо это представлено в драме основанной на греческом сказании, здесь деяние совершается еще самим героем, но без смягчения и завуалирования поэтическая обработка невозможна, откровенное признание в намерении убить, отца как оного мы добиваемся при психоанализе, кажется непереносимым без аналитической подготовки, в греческой драме необходимо смягчение, при сохранении сущности, мастерски достигается тем, что бессознательный мотив героя проецируется в действительность, как чуждое ему, принуждению навязанное, судьбой, герой совершает деяние, не преднамеренно и повсей видимости без влияния женщины, и все же это течение 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, взвалить ее на принуждение, с стороны судьбы, на оборот, вина 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 предосудительный мотив сексуального соперничества у женщины не нуждается в завуалировании и равно и эдипов комплекс героя мы видим как бы отраженным светом так как мы видим лишь то какое действие приводит 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 своей неспособности выполнить это задание появляются признаки того что герой воспринимает эту вину как сверхиндивидуальную он презирает других не менее чем себя если обходиться как каждым по заслугам кто уйдет тот порки в этом направлении роман русского писателя уходит на шаг дальше из 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 совершенно другим братом которому как интересно заметить достоевский передал свою собственную болезнь как бы эпилепсию тем самым как бы желая сделать признание что мол эпилептик невротик во мне отцеубийца и вот вretch из защитника на суд даже известная насмешка над психологией она мол палка о двух концах завуалировано великолепно так как стоит все это перевернуть на голову и вы увидите глубочайшую сущность восприятия достоевского заслуживает насмешки отнюдь не психология судебный процесс дознания совершенно безразличен кто этот поступок совершил на самом деле психология интересна лишь тем кто его в своем сердце желал и кто по его совершению приветствовали поэтому вплоть до контрастной фигуры алешив все братья равны и равны движимый первичными позовами и искатель наслаждений полный скепсис ациники 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 а должно означать что святой отстраняет от себя искушение и исполняется презрением к убийце или им погнушаться и поэтому перед ним смиряется симпатия достоевского к преступнику действительно безгранична она далеко выходит за пределы сострадания на которое несчастный имеет право она напоминает благоговение к некоторым в древности отошлись к эпилептику и душевно больному преступнику для него почти спаситель взявший на себя вину которую в другом случае несли бы другие аа

Висновок:

У ході виконання роботи ми набули навичок використання афінного шифру та його криптоаналізу. Опанували прийоми роботи в модулярній арифметиці.