

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 ФБ-05
Береза О. А.
Ковбель Д. О.

Київ 2022

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

Постановка задачі: 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.
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.
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

Для гарного початку треба гарний код, тому ми написали декілька математичних функцій: НСД двох чисел, розширений алгоритм Евкліда, знаходження оберненого за модулем числа та розв'язання лінійного рівняння

Виведення 5
біграм ШТ:

```
['еш', 'еы', 'ск', 'шя', 'до']  
Text after decifre method:
```

найчастіших

Отриманий ключ: (390, 10)

Зашифрованный текст

щжуяжушпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипму
гфбзчшоходовзбряцкмдбэдцхзнощкяоэоэотцюзныертзилгфоцбчполфмэдццкйкшйэысйрэ
йкчозычфждьмйшотдотзьюойсщзоюдууюзсшштзрэыосяфоешыенывдьмиыяшщрбгнямз
юдшскдмайыяоешезвжпнорэкжцжшбчдофшщофбяозфышжвонцеырайхмучмсшывч
фвэрфешмяояйывщейсбжоцлзшярфбждоцпюдлвюпщкзмзешжзмоуяхямзюдлвзбкзешдбш
яцксавотзябйкжзщопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквк
шятоьэйштибашкочщкфмыйейывдьмиышчвккцощеызонорйвкхпшсзунрмоншзоязшяэдх
пезхлсопжипеызохлншплбйшждоыкфоскщквкшягоефоцзччскщквканвказешюшлцромглт
доккжшскзьядншууезжурфешщпнзшятоужертцлвяхщжпофожушпккшяэывдьмиыйсжусж
ощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжушцжеляыцдюппкгфкшскщквкшяозн
оюуэйвзхягжжзщрфяоэщпсчжйэцшвдрйрэйкчфолжыймывдьмиышчдорддокыбзлжвочые
зыяюйеытяьочмскмзшядешмуяхщжбгяжрйашайюпмогйжшфшайрмлзнттзхаокшйбчаошя
анбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфм
овоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбля
ыхзсккцезшййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьюиосяйжгоелзурмейссо
жзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрзд
вщоцыыиеыхзнфылтфалаяыжфзйквбждэчяыжхыхоцыыиеыяпомггднотлккжжипеызохл
щпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкб
азушцпязхлдырйпоазсяслщяджипщплзджипошлцлыбжхяскыосяищеештцедууьмншйкрзш
яцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтноьобцэжхя
кзуяаяямзокбмырфзбюжщкьярьсозыеыйсхпрфешщфоефзббжнзтыссжяилнахпезфщпмшя
вжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжш
алтыбжхябжюакцопиышщчыдншуусйжуопчфюшжзйкмьяефопифбкюнзовбюпдокзшярйдуоуп
лвляешууяхщжпонойкыпюшщчмысклзыщбчмялзоцнрряешиыфсхядаыосябжьюиогфейхзн
шзунрюпаяябтцюмюпйшажьосжрэшжзщыцзешйкккшячхдосажуюшимйшлыпутцурряеш
бзкцколппотзуыайжхжшеыабрязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшй
фшщоцзхлцюпзхщжщккжююпцчзпэыиывдншуушсешяююшбчкзуяаяямзозхьпешьюаоеш
ывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюптжждшсэыпзь
цяделоцлыбжанхмлзннскюдьмоцбжпэйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузб
ряешйкешзоешчбгяюиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешь
оекшялцмиажжужсюуэжцышсдондпмкзшягожурфлцеызоножяюоэмкзшяпдмыэзгпйшууе
шоцсаскдондымкзшязплцдлвляудмяйядойккоцзшяекшэйфбждоцпюдлвляскмзбкзцжжу
щпрфуяшфсчдвбждчвхеышчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиышомз
мятыямйшалтыеызоешыедвайнинзшязпкцрфешмяеыцяовкрфекуяжубждоджгллкпыбжан
цйсщзорэкжшяанфшншрязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшощ
жшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэяканпдпуыйьмюпйфб
ждоцпюдлвюпюпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмн
щечяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуйтодыюпиызопызвкзмзюдайюдьм
иыыхфщжцфвчшяшжюпмуюкжшбчбьщжыйрйшзюшйзоузяждчвхеышчпмщпбкуяяоекшя
рбптхямзюдечрэйкиордиыцпямфочыхordiaжщыезжупмскшяцпсказкзшяллщяанншшкщк
поноюааошяекшйбчжучбгяюиыоцпмяднщжшбчтзчзкззюгяюалэчмиыоцюшяхщжпокбчфн
одоздопзузхщжпоьфйказтзрэыосяфощждчвхейхзжусжфрйктзшясжеьзоешрйэжпзжбьяое

шывбзлжцшшйфшрэшжсокийшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешед
вдвлгфезшйдбриялгфехзсккчвкцыезтлыниоовмушссожзбибзвфвчшыеабкзтыыймуеызо
чбюпэзбпифрйбжхяузыпуяхыщчрзхъэявжкщитдоешзхехзрэешйчпзюнешибряшякжш
бчфуэжмзчшвдщкпнойсщжшвкьоцпйшбгпутгэйшмштцедзббжнзмоошуеыщчдонорзлзд
жипщчьоцыиеныявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчко
жццибзлжозномясктзлзмкжшбчшыящкбйбзбьяшжддыщдзщжэзччаекуяанюзскжуэыошлз
шыящббждояоратлынсаскрэууншмяскжупмскжшбчдвдвжыглцечмяскскщкбаекжшбчфшуу
эжтлмдэйсщжшмощквканбчтзйбйкжшщпопйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекш
вуджпюфйказшлячовунщерыэтцюзпохпезомоешдбждсозжзбибзлжхыщжыйрйшзюаошйу
фаляятфсчподояоносншмоешдбждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлц
лыксфохявжядтлоцлылвбжзбмушямзешекощерычратзилгфбзлжзпвкылоцдуюпиыыяйкныл
яыфчбюпповбнзцжшзюайппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощк
порфссешмябяопмьосяцызвмуйчмоешдбждшуивлвщоефтцрзюэдцсавксшншмоешдбждн
шайешюшлыбжюуиырафовуьмайтзвжгцррршбжлзмканюакыбзйхдодвууэжкцмэсчжшсопж
ипеызозхъпешьюмяравжщоишжешмясжжкйкгшмуайтзфуншяхщжблчуцерыйсжулямрчф
юшпфмяяявлжипноэышбмунрчфюшьосокыиыхзхпезпыщжмосоыбжхядамофыюшотдов
кккшяабйчуцжелжрбриякывдюшлвохдошзюабпбжжуэырийбзщтелмяилщкцжжзщрэсыныбл
оцлыщемыжучмдубзвфаляюышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгш
ьльфжшншмолдопшайскжуцпнзшядуайиыалшжпонояякпзсчсрчфюшскюклфоцидяхф
щжшлцяджипбжюпмуяззошцуиврймзвозжпофотывдохлцюпядайхпимиыраыжнэюшсйокбя
жярзязонырийкоцыиеныщчжящкбьяшзюафжяюуйсгдншуулвайншопэзжбкюнзоносочзсы
яхщжипхордяожзщызбриякыбзлжкжюпмуяззошцуивривушайподояохлщкбьяшмуцжзовказ
хяаноешезвжбякбмурфоцхпэсопжипемыилзэтцмгнпдрэбтюянзужнепзыжыйсйцкжэгщлц
ечпфлцйшжбриякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшккопншфузхпмдьюшш
яцксктлзкокрзпмжзешскхыэжазадыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуя
яоекзожзуяпонзьяншвдщкцждоюшвжитдочзкжзсыкшкяскыосяпнжцнэохфсфлчжезьоешэ
пбжжуцчхябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракбяо
щзшжаокыиыщсозжзбиеызоузуьмуяуыжддосншмоешдбждсозжзбигцскыкфотфлцабгяы
овояяфьяшмуцжвзлжыцмимшшйгшезновжьошйэзфшзрзмкуягшзбезносожзбиеыядвзбр
язжлжипюпоцбптдохлибвоанаопышйкешзокуыврухкнзеявжйэйканэуцпзомязоныйфмяц
яюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфесыйсмофыксюдабгяыкаяшяблябгцабхямз
юдйсжушжеляыцдсэйканюрцкйкякчодазешажщзскяптжязджпзчзшяжкйкгшмускбфсчаое
шезвжпонопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвнш
юпзоешедншщзнэйсешылбэаокжшбчзкзтырийскпонзшясшмышйсщжшзпсчанбчдайкрзш
яшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцжшншэзчсжрлязшядябтцшя
анбчжучмкзшяшйрлщяегдяуяриймоаышйшажфямосшайдбмурфшяыжжяочжшбчгявбйшщ
чаоешезвжпоноэбкзешдбшярлзджипюшлцлырэмзуиыяхскмыуфоцядюжрчфюшвкжурф
лцтжбжюууфиыщчскподояоеыщжлкешраоязжшжуцщоскскможаскжшбцзвлвюпыхзюд
ншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномф
шсжцкгяпзюнампзепыэжйэзпэыгдншуущешфалноыжгллкеыщжюясащувхзак

Розшифрований текст

если правда что Достоевский в Сибире был подвержен припадкам то это лишь подтверждает то его припадки были его карой он более в них не нуждался когда был карем иным образом до казнь это не возможно скорее этой необходимостью наказания для психической экономии Достоевского объясняется то что он прошел несломленным через эти годы бедствий и унижений осуждение Достоевского как человека политического преступника было несправедливым и он должен был это знать он принял это не заслуженно наказание от батюшки 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 правдании наказания при осуждаемых обществом это на самом деле так много и 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 добыть смысла припадков Достоевского во всей полноте достаточного что можно предположить что их первоначальная сущность осталась неизменной несмотря на все последующие наслоения можно сказать что Достоевский такникогда 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 государству и к авторитету и к веревбогав первой он пришел к полному подчинению батюшке царю однажды разыгравшем у него с ним комедию убийства в действительности находившуюся только в отражении его припадках здесь верх взяло покаяние больше свободы оставалось у него во власти религиозной по недопускающим сомнениям сведение же к последней минуте своей жизни все колебалось 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 христианитивыходить из обожения 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 вообще человеческая сыновья вина на которой строится религиозное чувство достигла у него сверх индивидуальной силы и не могла быть преодолена даже его высокой интеллектуальностью здесь нас казалось бы можно упрекнуть в том что мы отбрасываемся от беспристрастности психоанализа и подвергаем Достоевского оценке имеющей право на существование лишь с пристрастной точкой зрения определенно мировоззрения консерватора сталбына 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 невроза едва ли простой случайностью можно объяснить что три шедевра мировой литературы всех времен трагедия отнюдь не тут же тем утешения убийства царя Эдипа Софокла Гамлет Шекспира и братья Карамазовы Достоевского во всех трех раскрывается мотив деяния сексуальное соперничество и заженщины прямо все его конечно это представлено в драме основанной на греческом сказании и здесь деяние совершается еще самим героем но без смягчения изавуалирования поэтическая обработка невозможна откровенное признание в намерении убить отца какому мы добиваемся при психоанализе кажется непереносимым без аналитической подготовки в греческой драме необходимо смягчение при сохранении сущности мастера к достижению тем что бессознательный мотив героя проецируется в действительность как чуждое ему принуждение навязанное судьбой герой совершает деяние не преднамеренно и повсей видимости без влияния женщины в все же это течение обстоятельство принимается в расчет так как он может завоевать царицу мать только после повторения того же действия в отношении чудовищасимволизирующего отца после того как обнаруживается и оглашается его вина не делается никаких попыток снять ее с себя в звалить ее на принуждение со стороны судьбы на оборот вина признается как в сечелая 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 женщины не нуждается в авуалировании и равно Эдипов комплекс героя мы видим как бы в трагическом 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 и происходит сдвиг чувства вины, переходит в осознание своей неспособности выполнить это задание и появляются признаки того, что герой воспринимает эту вину как сверхиндивидуальную и презирает других не менее чем себя, если обходиться каждым по заслугам, то уйдет тот порок, из-за которого в направлении романа русского писателя уходит шаг дальше и здесь убийство совершено другим человеком, но человек связан с судьбой такими же сыновними отношениями, как и герой, Дмитрий, у которого мотив сексуального соперничества откровенно признается совершенно другим братом, которому как интересно заметить, что Достоевский передал свою собственную болезнь, как бы эпилепсию, тем самым как бы желая сделать признание, что мол эпилептик, невротик, в нем отцеубийца и в отрывке из записки на суде, та же известная насмешка над психологией, она мол, по алкаю двух концов, завуалировано, великолепно, так как стоит все это перевернуть, находишь глубочайшую сущность восприятия Достоевского, заслуживает насмешки, отнюдь не психология, а судный процесс, дознания совершенно безразлично, кто этот поступок совершил, на самом деле психология интересуются лишь тем, кто его в своем сердце желал, кто его совершил, и его приветствовало, поэтому вплоть до контрастной фигуры, аleshivsebratya, равновиновны, движимый первичными позовами, и искатель наслаждений, полный скепсиса, циники, эпилептический преступник, братья, харамазовых, есть сцена, 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, исполняется презрением к убийце, или импогнушаться, 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, и некоторые в древности относились к эпилептику и душевнобольному преступнику, для него почти спаситель, взявший на себя вину, которую в другом случае несли бы другие.

Висновки:

Під час виконання цього практикуму, були засвоєні основні принципи дії програми автоматичного розпізнання змістованого тексту, а також з впровадженням можливості провести криптоаналіз афінного шифру біграмної заміни і знаходження відповідного ключа.