

Міністерство освіти і науки України

Національний технічний університет
України "Київський політехнічний інститут
імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота №3

Виконав студент групи ФБ-13

Нійозов Рустам

Київ 2023

Криптоаналіз афінної біграмної підстановки

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 :

4 варіант

шжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбр
яцкмдбэдцхзнощк
яоэоэтцюзныертзилгфоцбполфмэдццкйкшйзысырэйкчозычфждьмйшотдотзьоюйсцзоюдууюзсшстзрэ
уюсяфоешыенывд
ьмиыышцрбгнянмзюдшсдмйаыяаоешезвжпнорэкжцжшбчдофшщофбяоязфыщжвонцеырайхмучмсшы
вчфвэрфешмяояйывщ
еыйсбжощлзшярфбждоцпюдлвюпцкмзешжзмоуяхямзюдлвзбкзешдбшяцксавотзтяйкжзщпопсйкоефтцрзюэ
дцсшямсканзоми
жуэыыцсшмычмэжглрзщыезскцквкшятюэыйштибшкочцкфмыйеыйывдьмиыщчвккцощезонорйвкхпшсзун
рмоншзоязшяэдхп
езхлснопжипеызохлншплбйшждоыкфоскцквкшягоефоцззчскцквканвказешюшлцромглтдококжскзьядншуу
езжурфешцпнз
шятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжу
щжеляыцдюппкгф
кшскцквкшяозноууэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчфолжыймывдьмиыщчдорддокыбзлжвочыез
ыаяюеытьаочмск
мзшядяешмуяхщжбгжряшайюпмогйжшфшайрмлзннтзхаокшйбчаощаанбчйтжмжкучбуфпошфбждоцпюд
лвюпюпээкбтцзопз
аоешйшохзодонофшайсцзожурфмовоцяанфшляйбмуьосклкюнскюжьюешшоешоцэжлыдяюеызопыщжф
оочсквжаббжнзбляь
хзсккцезшяййсцзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьюиосяйжгоелзурмеейссожзешопхпимсжск
азкзшяшйнэюш
шомглтдонзпксзеыэжюпщжхявушйгожурфлцгншвдрздвщоцыиеехзнфылтфалаяяжфзйквбждэечаяжхых
оцыиееыяпомгтд
нотлккжжипеызохлщпдорязпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщай
кбазуцпязхл

дырйпоазсяслщяджипщплзджипюшлцпыбжхяскыосеяищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпм
уапзчвомощкхыхз
июнязхпрэчфлоешщпоцбжщлтзньообцэжхякзуаяямзокбмырфзбюжщкьярьсозыейсхпрфешщчфоефзбб
жнзтыссжяилнахп
езфщпмшвяжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжалтыбж
хябжюакцопиыщчыд
ншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярьдуюплвляешууяхщжпонойкыпюшщчмысклзыцбмя
лзоцнрряешиыфсхя
даыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжщыцзешйкккшячхдосажуюшимйшлыпутцур
решбзкцколппотз
уыайжххшшеыабряязодхпрэчфдяешоцкзвдаямыуайдосщоччдыозлжцшшйфшщоцьзхлцюпзхщжцккююю
пцзпэыиывдншуушс
ешяюшбжкзуаяямзозхьпешьоаоешывмкйыдвбжжщцрэсымяблщлышсгялаэышйлвмксаанжутаонзсккк
здвюптжждшсэы
пзьцяделоцпыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузбряешйкешзое
шчбгяыоиюцпм
зямодпмучкшйаоешезвжпоновгеызрийхесзкбйкьосктлсзешьоекшялцмиажжужжюуэжцышсдондпмкзшягожур
флцеызоножя
яоьозмкзшяпдмыэзгпйшууешоцсаксдондымкзшязплццдлвляудмйядойккощзшяекшэйфбждоцпудлвляскм
збкзцжжуцппрф
уашфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеызое
шыедвайнинзшязпкц
рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэжжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжн
рфушйеыюувделдш
чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмккнцжшязцжюяйкбэйканпдпуыьмюпйфбждоцпуд
лвюпюпэзпшкзхуэж
йуппбзлжфяфохяшфвчшякжядтлоцпыезсочзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкзжжоуц
еыюпщуйтодыюп
иызопызвзмзюдайюдьмиыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрийшзяошйзоузяждчвхеыщчпмщпбкуюя
оекшярбптхямзюдеч
рэйкиордиыцпмфочыхордяожщыезжупмскшяцпсказкзшялщяанншшкщкпоноюааощяекшйбжжучбгяыоиы
оцпмяднщжшбчтз
чзкззюгяюалэчмиыоцюшяхщжпокбчфнодоздопзухщжпотьфйказтзрэыосяфощждчвхеыхжжусжфрийктзшяске
ьзоешрийэжпжж
бяаоешывбзлжщшйфшрэщжсокыйшлцпыксфохямвуйчжуезаяалжшбчшфссешмяпзюнзоешедвдвлгфезш
йдбриялгфеыхзскч
вкцыезтлыниоовмушссожзбибзвфвчшяеыабзктыыймуеызочбюпзбзпифрийбжхяузыпуяхыщчрзхьэызавжкци
тдоешзхеыхзрэ
ешйчпзюнешибряшяякжшбчфуэжмзшвдщкпонйсщжшвкьоцпйшбгпугтэйшмштцедзбжнзмоошууеыщчдон
орзлзджипщчьоцы
ыиеыыявлаомяркгяшптцпмдущесзноншшкмоцжшлвждвдрэскалцяекжшбчкожцчибзлжзномясктлзмкжшб
чшящкбайбзбш
жддыщдзщжзччамекуаянюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжупмскжшбчдвдвжгльцем
яскскцбаекжш
бчфшууэжтлмдэйсщжшмоцквканбчтзйбайкжшщопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуаджпюь
фйказсшлячову
нщеырэтцюзпохпеызомоешдбждсозжзбибзлжхыщжыйрийшзяошйуфаляятфсчподояоносншмоешдбждтззпс
чжшбчншщзнэйсеш
ьовбптдохлжурфбжффюшлцпыксфохявжядтлоцпылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцую
пиыыякныляыфчб
юпповбнзцжшзюйппифрийщжэппншйкрзщыайхпжшшвдщкхйппифрийуяпндоцкпорфссешмяабяопмьосяц
ызвмуйчмоешдбжд
щуивлвщоефтцрзюэдцсавксншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцррршбжлзмканюакыбз
йхдодвууэжкцмэсч
жшсопжипеызохьпешьомяравжщюипжшешмясжжкйкгшмауйтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяя
явлвжипюпэышбмунр
чфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывдюшлвхдошзяоббж
жуэырийбзщтелмяил

Розшифрований текст:

[illegible]

сшей степени характерная для дostoевского оизразговора с дмитрием старец постиг ает что дмитрий нoсит в себе готовность к цeбуйству и бросается пeред ним на колeно и зeмoжет являтьcя вырaжением вoсхищeния, а дoлжно означать что cвoй oтcтpаение тoт cебя иcкyщение иcполнить cя пpeзpeнием кyбильцe или пoгнyшьcя пoэтoмy пeред ним cмирeтcя cимпaтия дoтoевского oк пpeстyпникy и кудeйcтвительнo бeзгpаничнo aдaлeкo вoхoдит зa пpeдeлы cтpaдaния нa кoтopoм eнe cчacтливый и мeeт пpaвo нa нaпoминaтe блaгoгoвeния cкoтoрым в дpeвнocть тoт нo cильнo cкoлeпил кy и дyшeвнo бoльнoмy пpeстyпникy для нeгo пoчти cпacитeль зявший нa ceбя в инy кoтopy ю в дpyгoм cлyчae нe cлeдoвaт дpyгoгe

если правда что Достоевский в Сибирь не был подвержен припадкам то это лишь подтверждает то что его припадки были его карой он бзанил для психической экономии Достоевского объясняется то что он прошел несломленным через эти годы бедствий и униженийosuинялэто незаслуженноенаказаниеот батюшки царя как замену наказания за заслуженного им за свой грех по отношению к своему соборно-психологическому оправданию наказания присуждаемых обществом это на самом деле так многие из преступников жаждут наказания истерических симптомов поймет что мы здесь не пытаемся добиться смысла припадков Достоевского во всей полноте достаточно логично можно сказать что Достоевский так ни когда и не освободился от угрызений совести в связи с намерением убить отца это лежало в основе авторитета уиксера в богав первой он пришел к полному подчинению батюшке царю однажды сыгравшему с ним комедию уленного мира воззрения консерватор стал бы на точку зрения великого инквизитора и оценивал бы Достоевского иначе упрямая справедливость для его смягчения можно лишь сказать что решение Достоевского вызвано очевидно затрудненностью его мышления в следствии не в розе двали простой случайностью можно объяснить что три шедевра мировой литературы в всех временах трактуют одну и ту же тему о том что убийство царя эдип софокла гамет шекспира и братья Карамазовы Достоевского во всех трех раскрывается мотив

яния сексуальное соперничество и из-за женщины прямое все-таки конечно это представлено в драме основанной на греческом сказании из-за деяния совершается еще самим героем без смягчения и завуалирования поэтическая обработка невозможна откровенное признание в намерении убить отца какому-то добиваемся при психоанализе кажется непереносимым без аналитической подготовки в греческой драме не обидно смягчение и при сохранении сущности мастерски достигается тем что бессознательный мотив героя проецируется действительность как чуждое ему принуждение навязанное судьбой герой совершает деяние не преднамеренно и повсюду в видимости без влияния женщины и в 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 себе взыскать ее на принуждение с одной стороны судьба на оборот вина признается как всецело вина наказывается что рассудком может показаться несправедливым но психологически абсолютно правильно в английской драме это изображено более коварно поступок совершается не самим героем а другим для которого этот поступок не является отцеубийством поэтому предсудительный мотив сексуального соперничества у женщины не нуждается в завуалировании равно и 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 странном образом не в силах это сделать мы знаем что его расслабляет собственное чувство вины в соответствии с характером невротических проявлений происходит сдвиг чувства вины переходит в осознание своей неспособности 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 тот порок в этом направлении роман русского писателя уходит на шаг дальше из-за убийства 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 от которого как интересно заметить достоевский передал свою собственную болезнь кобы эпилепсию тем самым как бы желая сделать признание что мол эпилептик невротик во мне отцеубийца и в отрывке защитника на суде даже известная насмешка на психологию она мол палка о двух концах завуалировано великопотопа как стоит все это перевернуть и находишь глубочайшую сущность восприятия достоевского заслуживает насмешки и 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 приветствовали поэтому в плотный до контрастной фигуры алешин в братья равные виновны движимый первичными позовами и искатель наслаждений полный скепсиса циник и эпилептический преступник в братьях карамазовых есть сцена в высшей степени характерная для достоевского и из разговора с дмитрием старец постигает что дмитрий носит все 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 исполнить презрение к убийце или им погнущаться и поэтому перед ним смиряется симпатия достоевского к преступнику действительно безгранична она далеко выходит за пределы сострадания

ния на которого несчастный имеет право на поминает благоговение некоторых в дре
вности относились к эпилептику и душевнобольному преступник для него почти спаси
тель взявший на себя вину которую в другом случае несли бы другие

Висновки: Під час виконання практикуму, навчився створювати та розуміти
принцип дії програми автоматичного розпізнавання змістовного тексту,
спробував провести криптоаналіз афінного шифру біграмної заміни та знайти
вірний ключ, для розшифрування тексту. Набуті навички знадобляться у
подальших практикумах та професійні діяльності.