



Міністерство освіти і науки, молоді та спорту України

Національний технічний університет України

“Київський політехнічний інститут”

Фізико-Технічний інститут

Лабораторна робота №3 з Симетричної криптографії

Студент групи ФІ-93

Карловський Володимир Олександрович

Мета

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

Найпопулярніші біграми

кг,зц,фщ,нэ,цю

Принцип роботи методу

1. Беремо шифртекст і природній текст, рагуємо кількість біграм
2. Далі беремо 5 найпопулярніших біграм з одного і другого тексту і генеруємо велику кількість ключів (перебором уявляємо яка біграма перейшла у яку).
3. Після чого розшифровую і пробую аналізувати за допомогою кількості найпопулярніших літер чи є мова природньою
4. Після фільтрації маю десь 10 текстів, їх фрагменти перевіряю самостійно

Зашифрований текст:

Бюфиацясгямрпйпоыдьюсмтдрацвпбяещфийеьэялтуфикщбпатбялячпппепфшэтчт
ялсйязптаошуасоезцмтыупуогыднемтщйсдуйбсыдтусюсцфингзгмтнерйбрюсдпчо
ачптвсбшуокбьяуесэизыфшмчпушчкещеодцлякхуслпгеабпцсатмхвжвфйргофхус
гпгищешщцхширщедиирнеаьгоютфшаяшвешзршшмтыпрпйдоуякегоуяляцтш
хопухтхезязухойыьпаявялслялпношуневпаорпуклсвецквлсвецкфимегжаьщтсгся
удлзыпяялякхрщсюгофрыцсвпгпкеэйзргойжтжашввяуьршшнттжчтмжмерйбркее
жхпмтфшцойфчтбсузмшкеьгптнэсуфрыпаядуфргодсхпйслякхкенсвпгигocyгорйпе
сщкейыфрдииэрйтфлякхйячаорйфухттшмпидмэфрцтжжлзфруоэтцешшнйцожы
почтаегымтхпмтцпифуегыбяпэчшуйязскйумяскчсфхмттпыпсгхялякенсфшясеуоу
явпвснпкхгхшжшячсгчпчазсфпкгитусьюокаяяшвешзршшкесмйшреьгвтцрьпез
нпбяутфшытаеаьясфпяьяжрщхшзфхтаеьепуовпояусфуоэтпжющеюзчпчтсбп
влмисдпуььежлтнжвьептюкекысюнщяявсфхсфцдрчиусцотвлжпчтвеасбмязася
гпмтэемпатйтчтялусппятуялчощтитмтртдпэрнйчтусышергпоянпртнефдоаяжсвпг
ижтыщтсфпцснпхюерпухмхпкеиэиржтлмфюхшвмфюкеежхпмтдтляшшвмкыусмш
кекыпоясшуйтнпюдоуэсрщхшзыкеигзстялягядтжыхфлякхаямонйаьртнщевпьдп

уфизрдиневздимтхепумтвяфевмхпхпэсмхвпрйязгыпепцпоутчпаялпйрдишшреыгвт
ляуяфсвьяфсфянпоегьюяфсьдуозруохундоьяфхсфаянггадьзющбпфпцсляощзобьяс
кхзоуякнлетуэршштуетсжжюлмхпеоцсдлуказсмтнйфпцсяскхгьябпожтжкещехоуя
яляякхмтнлгяфххпыптшпумтыщбпхофпцснпхпвжяузервпояаеаьсгесвжлзлуфрго
хуйячпвтнебдмэвпяоцпгпаошуасудфиялщтемгохпглястцяаяйтцплсхяфхпремцыыг
цсйрышщогсмтцпусхяфхщтфшяаяеуоатъуптбхвжхшсдсюкесмфрсфаяшдговжлзир
недиеркцппглбепуневпыпмтхшфпцсляхшгжаякецывпыпсгхяляньфдхтбхтуппоуцт
эдлзыпрплтейейцыпдырйвпфшхувяпсатмекпыпвасрпвеежжтшуоубзхомтнйфпцсч
пфшцкнйцобтысфххтидшшвпфшдсточтепояусьуфшяаятмсутвжячнйляфшвчдыз
рресдгоьдчирышшдсрндсхярсзпъдзыацтаешчяййдэйхшбжслтзгясбпояфхмекпъ
ыпвткердмвпфшсулпхдкыневпчпббцошунесмфрпуооныцицоышшчышпепхдгожые
штсоаяшшсфбьябесмфрреыггшжмжсюгялпрсфрреттьдхшцотлшикыгжяязсутвжяч
фшяаяяцзысыяснщтфшхочюнпдямхвпаошшячтжфдпуцпясзсутвжыгрудуюоц
вмытаянгютусущаяжмирпужжюущсдфизрфхдгсдшяусвярсйчтжфдпулыгохтфшяая
ыудющвмзсфивпхдкыневпвтмтемкывыпзасадвщупзаяаясьдирцофхлпыидиусут
фшояячврнепорпжпгемпбынесуфрходсптмыдмфдяаярскефрреттадщеввюмгохпц
пцжяяптаегыфябпуфаиаакпсшйцопрешялбиуовгнжатчткпаеаьхтзсмтвжерйжоцтс
ысвпехчимесуескхлыцоатуиирфрйыьэсгаябпгьыгпщццкатяеььяейаьчтиуюыциг
ьфшытаегывпнлшшачвпнпмсхьзгяицштжпчткызблялбсптютнлжзыххршфдндлз
всзсжжзидгусбярсбиуфоубзасвтивюебдфиялйчбдтжатиоуякибдхпэгфшщепучтае
пчыдщейепвопаямхялйсгпгцсдпвффйстцтсхврщцтфшлржцыиоявсгаяеюббляяв
жюлзсбсвсепюзвтмтусчищялщдгоидсшштггяешчдычицпляшяшштшгжзыйшуоц
гзяцеюсясцпдргвирнеющяяйрнеялэйгфшвсаоуаяязсуцоатйофлдрмекпыпвасжшх
швсгебдчцнеффчоыдемжтэопенсжпчтемгохпцпдрчифшвсмысуюшглфхйяфлфдлз
ялщтдррщэчйбнеаткомжусмснщяярпзеежщетжхшсддкцыдсмнегыцоевндэйхшр
ицоышгпйрпигьхпюрижерчтмшсущящсдпужшгжешгоыдыннсцпаттсчпзгшунди
эешщофутлсфязяиерлябпрпгетжцтдрежусшямэбсмищеешфиуоуяхпзеержщцотс
жюущшэедчшфщэчшчширгсятобьявфхуоцгысицкысфрпюиирнепууоатююлзшш
пцясцпатчтвсптусйщэчшчширнышэшшуиирешйжусетытясгпчтфедклтьрцыапут
бхоячедкмекпыпвпткнйфдфюжтдгзпыдгоидсшффьдчифшяууфршоучинефферпив
чхохптспйерязусискххялпфштфусшоутхпуудяшжмчфияягпцпхенеткжпмхупыпыс
дргобтрсфрхохпэгадьзбрдмвпфшхоуучинештожзыххршфдпууоуаяскхяхпдэыгбпо
ебсцшзыдтлпфштфусдмхпцимпюцудвпыпхоцпмхдпояусуалыуучинештчоуплтвта
езыйслтвтгсяыфшщепучшсфчорйерцтоячаеаьглфшбпаязусуакитаоспыдгомхччызе
ьфшояепфпвлхшвгтсаягоуявпцфэофуизвпомгофхкуфрршялщцуовгпрневьрпхесю
ячфшяаяящдлзвсзсшшсдюзхянщунйфшэгшшбпфшапббцошуневпыпъдюзсуфиф
шояшрхмютусстыпфшнгмшсдндюовгдюзсуфичширреуозсыдияязывпмсфпыдго
уфцагпвпйсфсгядтмтйукупслжвтсаяывцзфчпыпхшвпютусмыьэсгаябпгецтвтгсфш
вжцтцпыдырйчтусцозсдгяснгшшхсесювмхочтаетужкезидмцофссцбпйттоимжюло
явбштепцплчширреттлюшжциуфьдфицжрсмешшсдхоэофсфпыдгочтаоьзгяояыш
кыйяфлдгдрпффюрцдуоуаядюзсуфифшоячосазсиямшсдрииракыдлзвсзсбскизоы

дасвгтсаяыпугбхоячегыюршоыдщенищфдачфиялбшрщзыужкезыежшткезыдмцоф
сшшнгтеуозсгпхпюлсщфдьэсуакчазсыпчгтяиощущекысюшмтвжлзешщопеигбпо
ефдлзвсзсышедюзхявпдрахпожиэгышпоыдщенисвтшштахпчпуюдцнеасоуркнщгвэне
жувирыищевпюдэйхшндгожыхшлтфхрщбпщцефрюзудпуештпжющеюзпвтквгтсфш
вжаыптыширреуозсчоыдщецобтлтфпгегызсцпцагпвпйсфсаяьдйфдтунеадасоесм
фрфдгожыештсояршсфатсдшшежзышшфидмцофссщершэнефхандрчипушефвья
атаижтэоспйтшжбдлзясзешчиямшсдпуаязучшффмесгфштсчшедюзхяйтзютсрщтс
бпгесдцоедйеьпгмхвгяеюсфшсддмцофсксмердгоыдцжвгяеьцпатхвмяджзыпржж
йецвтгтсфшвжцтяяшпусбпояусчифрщтьдпуфичшсфщцефрюзлпхдкыневпылпфш
тфусгскизоыдасвгтсаяыунаеадасцтхшптмхялжзыцпмтлшпуаякпмтнйитыпедпуи
фужкезыдмцогпыпаязучшффшяялгяшшсфавнебялпрсфрреоагпвпйсутвжаьбп
смесгфштсчшедюзхятагпвпйснтытзютсасазтжскутуссцбпрпцсэоспббвыщефрюзсд
шяусварсчшедхоэогпбихфатмхвпфшсуфшяаяяьобтлтфпгегызсцпцагпвпйсфсрпбб
кысунеадасжмгоуеуозсытзюфдьдмедицтчякоыдщецынщфдачфиялбшрщзыужкез
ыежасвтшшатхекынещтнщгвэндмцофсемфдтлгпхпюлппордмакатппюингмсьоыд
щежшсюхшрщяухшвпютусудлзвсзсскизоыдасвгтсаяыпйепувпвштжаьуткшаьфуу
фшшсфхптшхшедюзыунаеадасязусужтэоюгдтгяоецтютюесмфрчиояшвешсюпужж
яужшаьфшяамтдршэзрхоышяяцсрскеялшшедхоэофсцоцфхсвгтсаяыфууфшшсфояч
еаьхшяядрцкаябпгесюэчьзьеьфшоялпхдкыневпыунаеадаспясутфшрпмеуоыдщеляю
шедхохптшцуюкбакпсчунаедткяяфшшшюзыпгяхюфихпдгмтхяпнпшцунйфшэгшшж
пшятрцвыпгмхвгяеюсфшсддмцофсксьдудфи

Ключ

(72, 805)

Розшифрованный текст

агодышлидашлибыстроинеслышнокакподснежныеводыпротекаламолодостьелен
ывбездействиивнешнемвовнутреннейборьбеитревогеподругунеенебылоизовсехде
вицпосещавшихдомстаховыхонанесошласьнисоднойродительскаявластьникогдан
етяготеланаделенойасшестнадцатилетнеговозрастаонасталапочтисовсемнезависи
маоназажиласобственнойсвоеюжизньюножизньюодинокоеедушаиразгораласьи
погасалаодиноконабилаькакптицавклеткеаклеткинебылониктонестеснялееини
ктонеудерживалаонарваласьитомиласьонаиногдасамасебянепонималадажебоялас
ьсамойсебявсечтоокужалоееказалосьейнетобессмысленнымнетонепонятнымкак
житьбезлюбвиалюбитьнекогодумалаонаистрашностановилосьейотэтихдумотэтих
ощущенийвосемнадцатилетоначутьнеумерлаотзлокачественнойлихорадкипотряс
енныйдооснованиявесьееорганизмотприродыздоровыйикрепкийдолгонемогсправ
итьсяпоследниеследыболезниисчезлиакоонецноотецеленыниколаевнывсеещенеб
езозлоблениятолковалообеенервахиногдаейприходиловголовучтоонажелаетчегото

чего никто не желает, чем никто не мыслит в целом России и потому наутра халадажесмеялась над собой беспечно проводила день за днем, но внезапно почто-то сильное безымянное, чем она совладеть не умела, так и закипало в ней, так и просилось вырваться наружу, угроза проходила, опускались усталые, не взлетевшие крылья, но порывы эти не обходились ей даром, как она и старалась не выдать того, что в ней происходило, так в волнованной душе пискалась в самое ее наружное спокойствие и природные ее частобыли вправепожимать плечами и удивляться и не понимать ее странностей в день, которого она начала на шпассе, казелена дольше обычного, но не отходила от окна, она много думала, оберсеньеве, о своем разговоре с ним, потребность в защите информации возникает в связи с необходимостью обеспечить секретность исследований в стратегических областях, правильно распределять информацию о промышленных разработках и регулировать информацию о личности в современном обществе, а начало восьмидесятых годов рассматривается как начальный пункт, когда социальные протесты в демократических странах помогли сплести сеть глобальной сети хакеров, политический флирт на почве нарушения прав человека породил тему организаций хакеров в массе стран мира, почти одновременно, не менее чем за год эти группы узнали прелесть сотрудничества, их члены свободно обменивались идеями, ми, через национальные границы, часто по украденным паролям, дающим бесплатный доступ к телефонной сети, несколько причин, объединившись вместе, сделали международный компьютерный разбой легким и действенным, новые технологии и создавшие более мощные и дешевые компьютеры, развитие коммуникаций для связи и международный характер стандартов установленных транснациональными корпорациями, в принципе, есть лишь два вида угроз: раскрытие и видоизменение данных, раскрытие данных и предпологает, что кому-то случайно или по целенаправленным действиям стали известны смысл информации, этот вид нарушения встречается наиболее часто, последствия могут быть самыми разными, если похищен текст книги, справочника, на которую потрачены месяцы работы, десятков людей, то для коллектива авторов это катастрофа, и потеря могут выражаться в тысячах долларов, но если книга уже издана, то достаточно лишь слегка пожуришь похитителя и рассказать о случившемся в отделе новостей газеты или по телевидению, похититель может сделать книгу великопечную, рекламу очень важную, информация о берегаемой от раскрытия, представляют сведения о людях, истории, болезни, писем, состоянии счетов в банке, но, к сожалению, большого числа специалистов, угрозы личности в сведении компьютеров, остались, с нами же, уровни и в том же состоянии, что и до обширного использования, эвм, в современном мире, туризм становится все более важной, быстро развивающейся отраслью хозяйства, доходы от туризма становятся важной частью валютных поступлений во многих странах, развитие туризма способствует росту общественного производства, улучшению его структуры, росту производительности труда во многих отраслях экономики, даже не имеющих к туризму прямого отношения, международный туристское потребление стимулирует многочисленные экономические процессы, открывающие дополнительные рынки для продукции и нетуристских отраслей, создавая тем самым условия для роста производства, все эти факторы делают развитие и индустрии туризма очень важным для стран, переходным типом экономики и оно

мическиетрудностикоторыепереживаютэтигосударстванемогутнесказатьсянауровне развитиятуризманопритомкаждаястранаимеетвэтомотношениисвоюспецификуцельданнойработырассмотретьипроанализироватьорганизациютуристскойдеятельностивстранеспереходнымтипомэкономикинапримеревенгрииивначалерассматриваютсятеоретикометодическиеположенияисследованиязатемдаетсяоценкаразличныхфакторовразвитияиндустриитуризмавенгриииприродноресурсныйкультурноисторическийиинфраструктурныйпотенциалкомплекснотуристскоерайонированиедалеепроводитсяанализсовременногосостоянияиндустриитуризмавенгрииееотдельныхкомпонентовнафонеобщегоуровняэкономическогоразвитиястраныдаетсяоценкасосоциальноэкономическойролииндустриитуризмавэкономикевенгрииивзаключениепроводитсяобщийанализорганизациитуристскойдеятельностивстранахспереходнымтипомэкономикивобщемивенгрииивчастностивенгрияпринадлежакстранамспереходнымтипомэкономикииимееттемнеменееспецифическиечертыкоторыеотличаютееотдругихстранэтоготипавотношенииразвитияиндустриитуризмаосновнойтакойчертойявляетсяточтотуризмвенгрииразвиваетсяужедавноешевначаледвадцатоговекавэтойстранесложилисьтрадиционныетуристскиесвязитуризмаявляетсяважнойотрасльюнародногохозяйствасовременнойвенгрииколичествоиностраннхтуристовпосещающихвенгриюрастетизгодавгодтомунемалоспособствуетбогатейшийкультурноисторическийиприрод