МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Лабораторна робота №3

з дисципліни «Криптографія» на тему:

«Криптоаналіз афінної біграмної підстановки»

Перевірив:

_____

Виконали:
Студентки групи ФБ-91
Легенчук М.
Осьмак А.

Київ – 2021

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.

5 Найпопулярніших біграм

Bigram	Count	Freq
ХБ	60	0.0078196
НК	56	0.0072983
БЙ	53	0.0069073
ЮЖ	52	0.006777
ШЬ	49	0.006386

Варіант 11

КЛЮЧ: a = 703, b = 956

хорошосэрбиллнехотясунулденьгивкарманвотчтобиллвыпростопосеетеэтуновуютравукогданибудьвдругойразкактолькояпомрунадругойжеденьможетеперекопатьэтучертовулужайкунукакхватитувастерпенияподождатьещелетпятьшестьчтобыстарыйболтунуспелотдатьконцыужбудьтеувереныподождусказалбиллсамнезнаюкаквамобьяснитьнодляменяжужжаньеэтойкосилкисамаяпрекраснаямелодиянасветевнейвсяпрелестьлетабезнееябыужаснотосковалибеззапахасвежескошеннойтравытожебиллнагнулсяиподнялсземликорзинкуяпошелковрагувыславныйюношаивсепонимаетеяуверенизвасполучитсябле стящийиумныйрепортерсказалдедушкапомогаяемуподнятькорзинкуявамэтопредсказываюпрошлоутронаступилполденьпослеобедадедушкаподнялсяксебенемногопочиталуиттираикрепкоуснулкогдаонпроснулсябылотричасавокнавливалсяяркийивеселыйсолнечныйсветдедушкалежалвкроватиивдругвздрогнулслужайкидоносилосьпрежнеезнакомоенезабываемоежужжаньечтоэтосказалонктотокоситтраву новедьеетолькосегодняутромскосилионещепослушалдаконечноэтожужжиткосилкамернонеутомимо дедушкавыглянулвокноиахнулдаведьэтобиллэйбиллфорестервамчтосолнцеудариловголовувыкосите ужескошеннуютравубиллподнялголовупростодушноулыбнулсяипомахалрукойзнаюнокажетсяутромя работалнеоченьчистодедушкаещедобрыхпятьминутнежилсявкроватиислицаегонесходилаулыбкааби ллфорестервсешагалскосилкойнасевернавостокнаюгинаконецназападиизподкосилкивеселобилдуши стыйзеленыйфонтанввоскресеньеутромлеоауфманбродилпосвоемугаражусловноожидаячтокакоениб

удьполеновитокпроволокимолотокилигаечныйключподпрыгнетизакричитначнисменяноничтонеподп
рыгивалоничтонепросилосьвначалокакаяонадолжнабытьэтамашинасчастьядумаллеоможетонадолжн
аумещатьсявкарманеилионадолжнатебясамогоноситьвкарманеодноязнаютвердосказалонвслухонад
олжнабытьяркойлеопоставилнаверстакбанкуоранжевойкраскивзялсловарьипобрелвдомлинаонзагля
нулвтолковыйсловарьтыдовольнаспокойнавеселаввосторгетебевовсемвезетивсеудаетсяпотвоемувсе
идетразумнохорошоиуспешнолинапересталарезатьовощиизакрылаглазапрочитаймневсеэтоещеразп
ожалуйсталеозахлопнулсловарьзакакиеэтогрехиядолженцелыйчасждатьпокатыпридумаешьмнеответ
скажитолькодаилинетбольшемненичегоненадотычтоженедовольнанеспокойнаневеселаиневосторге
довольныбываюткоровыаввосторгемладенцыданесчастныестарикикоторыеужевпаливдетствосказала
линануанасчеттогочтовеселасамвидишькакявеселосмеюськогдаскребуэтураковинулеовнимательноп
огляделнаженуилицоегопроясниласьтыправалинамужчинытакойнародникогданичегонесмыслятмож
етбытьмывырвемсяизэтогозаколдованногокругаужесовсемскороявовсенежалуюсьзакричалалинаятон
еприхожуктебесословареминеговорювысуньязыклеотыведьнеспрашиваешьпочемуутебясердцестучи
тнетолькоднемноиночьюнетаможешьтыспроситьчтотакоебракктоэтознаетнезадавайвопросовестьжет
акиелюдивсеимнадознатькакустроенмиркактокакседакакэтозадумаетсятакойипадаетстрапециивцирк
елибозадохнетсяпотомучтоемуприспичилопонятькакунеговгорлемускулыработаютешьпейспидышии
перестаньсмотретьнаменятакимиглазамибудтовпервыйразвидишьлинаауфманвдругзамерлапотянула
носомвоздухвотбедаавсетывиноватонарвануладверцудуховкиоттудаповалилдымсчастьесчастьегорес
тновоскликнулаонаиззаэтогосчастьямыстобойссоримсявпервыйраззаполгодаивпервыйраззадвадцать
летнаужинбудутугольявместохлебакогдадымрассеялсялеоауфманаужеисследпростылгрохотлязгсхватк
ачеловекасвдохновениемденьзаднемввоздухетакимелькаюткускиметалладеревамолотокгвоздирейс
шинаотверткипоройлеоауфманаохватывалоотчаяниеионскиталсяпоулицамвсегдабеспокойныйвсегда
начекуонвздрагивалиоборачивалсязаслышавгдетовдалекечейтосмехприслушивалсякзабавамдетворы
присматривалсячтовызываетудетейулыбкувечерамионподсаживалсякшумнойкомпаниинаверандеуко
гонибудьизсоседейслушалкакстарикивспоминаютпрошлоеитолкуютожизнииприкаждомвзрывевесел
ьяоживлялсяточногенералкоторыйвидитчтотемныевражескиесилыразгромленыичтоегостратегияоказ
аласьправильнойподорогедомойонторжествовалпоканевходилопятьвсвойгаражгдележалимертвыеи
нструментыинеодушевленноедеревотогдаегосияющеелицовновьмрачнелоипытаясьизбытьгоречьнеу
дачионсожесточениемрасшвыриваликолотилчастисвоеймашиныслovноэтобылиживыеяростныепрот
ивникинаконецконтурымашиныначаливырисовыватьсяичерездесятьднейиночейдрожаотусталостииз
можденныйполумертвыйотголодатакойвысохшийипочерневшийточновнегоудариламолниялеоауфма
нспотыкаясьпобрелвдомдетиссорилисьиоглушительнокричалидругнадруганопривидеотцатотчасумол
кликакбудтопробилурочныйчасивкомнатувошласамасмертьмашинасчастьяготовапрохрипеллеоауфм
анлеоауфманпохуделнапятнадцатьфунтовсказалаегоженаонужедвенеделинеразговаривалсосвоимид
етьмионисаминесвоисмотритеонидерутсяегоженатожесаманесвоясмотритеонапотолстеланадесятьфу
нтовтеперьейпонадобятсяновыеплатьядаконечномашинаготоваасталимысчастливеектоскажетлеобро
сьтымастеритьэтичасывнихневлезетниоднакукушкачеловекунеположеносоватьсявтакиеделагосподуб
огуэтонавернонеповредитавотлеоауфмануодинврединикакойпользыеслитакбудетпродолжатьсяещех
отьнеделюмыегопохоронимвегособственноймашиненоэтихсловлеоауфмануженеслышалонсизумлен
иемсмотрелкакнанеговалитсяпотолоквоттакштукаподумалонужележанаполунотутегообволоклатьмаи
онуслышалтолькокакктототриждыпрокричалчтотонасчетмашинысчастьянадругоеутроедвараскрывгла
заонувиделптиц:онипроносилисьввоздухеточноразноцветныекамешкиброшенныевнепостижимочист
ыйручейилегонькозвякнувопускалисьнажестянуюкрышугаражасобакивсевозможныхпородтихонькоп
рокрадывалисьводвориповизгиваязаглядываливгаражчетверомальчишекдведевочкиинесколькомуж
чинпомедлилинадорожкепотомнерешительноподошлипоближеиостановилисьподвишнямилеоауфм
анприслушалсяипонялчтовлечетихвсехкнемуводворголосмашинысчастьятакоеможнобылобыуслышат

ьлетнимднемвозлекухникакойнибудьвеликаншиэтобылоразноголосоежужжаньевысокоеинизкоетор
овноетопрерывистоеказалосьтамвьютсяроемогромныезолотистыепчелывеличинойсчашкуистряпаютс
казочныеблюдасамавеликаншаудовлетворенномурлычетсебеподноспесенкулицоунееточнорозоваял
унавполнолуниевотвотонанеобьятнаякаклетоподплыветкдверямиспокойноглянетводворнаулыбающ
ихсясобакнабелобрысыхмальчишекиседыхстариковпостойтекагромкосказаллеояведьсегодняещенев
ключалмашинусаулсаулподнялголовуонтожестоялвнизуводворесаултыеевключилтыжесамполчасаназ
адвелелмнеразогретьееахдаясовсемзабыляещетолкомнепроснулсяионопятьоткинулсянаподушкулин
апринеслаемузавтракиостановиласьуокнаглядявнизнагаражпослушайлеонегромкосказалаонаеслиэта
машинаивправдутакаякактыговоришьможетбытьонаумеетрожатьдетейаможетонапревратитьстарика
сновавюношуиещеможновэтоймашинесовсемеесчастьемспрятатьсяотсмертиспрятатьсяваттыработае
шьсебянежалеешьавконцеконцовнадорвешьсяипомрешьчтоятогдабудуделатьвлезувэтотбольшойящ
икистанусчастливойиещескажимнелеочтоунастеперьзажизньсамзнаешькакунасведетсядомвсемьутра
яподнимаюдетейкормлюихзавтракомкполовинедевятоговасникогоуженетияостаюсьоднасостиркойо
днасготовкойиноскиштопатьтоженадоиогородполотьивлавкусбегатьисеребропочиститьяразвежалую
сьятольконапоминаютебекакведетсянашдомлеокакяживутаквотответьмнекаквсеэтоуместитсявтвоюм
ашинуонаустроенасовсеминачеоченьжальзначитмненекогдабудетдажепосмотретькаконаустроенали
напоцеловалаеговщекуивышлаизкомнатыаонлежалипринюхивалсяветерснизудоносилсюдазапахмаш
иныижареныхкаштановчтопродаютсяосеньюнаулицахпарижакоторогоонникогданевиделмеждузавор
оженнымисобакамиимальчишкаминевидимкойпроскользнулакошкаизамурлыкалаудверейгаражаиз
задверислышалсяшорохснежнобелойпенымерноедыханьеприбояудалекихдалекихбереговзавтрамыи
спытаеммашинудумаллеоауфманвсевместеонпроснулсяпоздноночьючтотоегоразбудилодалековдруг
ойкомнатектотоплакалсаулэтотышепнуллеоауфманвылезаяизкроватиипошелксынумальчикгорькоры
далуткнувшисьвподушкунетнетвсхлипывалонвсеконченоконченосаултебеприснилосьчтонибудьстраш
ноерасскажимнесынокномальчиктолькозаливалсяслезамиитутсидяунегонакроватилеоауфмансамнез
наяпочемувыглянулвокнодверигаражабылираспахнутынастежьонпочувствовалкакволосыунеговстали
дыбомкогдасаултихоньковсхлипываянаконецзабылсябеспокойнымсномотецспустилсяполестницепод
ошелкгаражуизатаивдыханиеосторожновытянулруку