МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ Кафедра інформаційної безпеки

КОМП’ЮТЕРНИЙ ПРАКТИКУМ No2

з дисципліни Криптографія
З теми: «Криптоаналіз шифру Віженера»

Перевірила: Селюх П.В

Виконали студенти групи ФБ-94 Мельниченко О. Дум’як Максим

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Для виконання першого завдання ми використали фрагмент з роману “Анна Каренина” Толстого.

У третьому завданні при пошуку довжини ключа для зашифрованого тексту, виявилося, що індекс відповідності найбільший при довжині ключа 16 символів. Тому довжина ключа для розшифрування закодованого тексту становить 16 символів.В результаті проведеної роботи ми отримали ключ “**делалисоборотней**”.

2: 0.037096826206553676,
3: 0.03535245194471151,
4: 0.03979351166739004, 5:
0.0354351293936251,
6: 0.037052368586566846,
7: 0.03522360497899179,
8: 0.04491213203766699,
9: 0.035450251570776165,
10: 0.03709763005817015,
11: 0.035062146465428885,
12: 0.039788848438709196,
13: 0.03550919719241092,
14: 0.037093872461702884,
15: 0.035384371390931875,
16: 0.05539766505382551, *
17: 0.035524349460576386,
18: 0.037051140206933175,
19: 0.03531599104429486,
20: 0.03979839848540342,
21: 0.035056696947883076,
22: 0.03688094981192191,
23: 0.03526676001305198,
24: 0.04486292731353409,
25: 0.03531687664602463,
26: 0.03731086887465935,
27: 0.035247591055245484,
28: 0.03969086727168179,
29: 0.0355849038850587,
30: 0.036928328869868694

Розшифрований текст:

понятноеделокультурунасильновчеловеканеваткнешьвордусиэтудовольногрустнуюист
инузналинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиеж
елионосызмальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготом
ногочисленныеподразделенияпалатыщеремонийиуделяютстольковниманиядетямособен
нодетямтехктонаселяетхутунынотомужобычнаяленостьлюдскаяслужитемупочтинеодо
лимымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяещенемалолюдейкото
рымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавноени
светозарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийи
стинноеискусствониголовокружительныебезднынакраюкоихвечнопребываетнастилаю
щаянаднимиобщепроходимыегатинауканихотябычистоепросторноесостоятельноеидоб
родетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаи
тьхутунынаселеныбыливосновномварварамииневобычномпониманииэтогословаисстар
иобозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначениикотороестол
ьжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедающиерит
уаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазада

женевнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасн
ыйшелковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранн
оесловоиливысморкатьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадо
рогойрасшитыйплатокиутеретьносежеличеловекповзрослелизаматерелвтакомсостоян
иидушиизменитьегокакправилоуженельзяразвечтомудроенебовразумиттакилиначесм
отряповероисповеданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиеневме
стноаувещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупрожитьжи
зньтаккаконхочетконечноеслионпритомневредитокружающимпоэтомубагнеоченьлюби
лрайонхутуновикакправилооказывалсяздесьлишьпослужебнойнадобностивоткаксегодн
янесмотрянапротивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоаз
артавсегдасопутствовавшегоблизкомуиудачномузавершениюочередногоделакконцупод
ходилорасследованиеоцелойсетичетырезаведенияединовременноподпольныхопиумокур
иленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсявалександриювдохно
вленныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнесколькимихар
чевнямиилавкамииесликприбылямотторговлиспиртныминапиткамиудастсядобавитьещ
еидоходыотопиумокурениятоможнобудетподуматьорасширениипредпринимательствао
приобретениииновойнедвижимостиииншаллабытьможетдажеобустановлениииконтролян
адвсемихарчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагаш
узаведенияхнемногочисленныеноверныеегослужителиоборудовалиспециальныезакуты
гдекуслугамжителейигостейхутуноввыстроилисьудобныележанкиикурительныеприбо
рыпрасадпредлагалпосетителямновоесредстворасслабитьтелоиочиститьдушупослетруд
овыхбуднейпосетителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтах
ужвозомнивсебякняземразудалогоонзахотелмногоисразунанявсебевпомощьнесколькод
южихмолодцовпрасадзабылоглавномиустремилсякнизменномувзявшисьсилойвнедрять
опиумвхарчевниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбыто
ктаксправедливополагаллагашобращатьсяквэйбинамдлярешениявозникающихразногла
сийбылоневхарактереобитателейхутуновинечестныйпрасадбеззастенчивоэтимвоспольз
овалсяпопыткиздешнихжителейсовладатьслагашемсвоимисиламинеувенчалисьуспехо
маспидзаранееподготовилсякстычкамиоттогооказалсясильнееокончательнораспоясавш
исьонснялсостеныдвуствольноеружьедедаиприлюднопрямопосредипереулкаотпилилст
волыпослечегосталходитьпохутунамсобрезомзапазухойидажепрозвищеполучилобрезаг
аместныежителирастерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцв
етомлагашподсчитывалбарышиновеликийучительвдвадцатьвторойглавебеседисуждени
йнезрясказалянезнаюниодногоправлениякотороебылобыбесконечнымисамовольноприс
военныйпрасадомнебесныймандатместногозначенияужеуплылизегорукхотялагашещеи
неподозревалобэтомвскоренесколькочеловекпотерялитрудоспособностьинтерескжизн
иисамоездоровьевследствиечрезмерногоупотребленияопиуманасонгрядущийавандевят
ыйпопалвбольницуулусноеведомствонародногоздоровьявсестороннеизучилопричинуза
болеванияванаивскореобрезагасамтогоневедаяпопалвполезренияуправлениявнешнейох
ранызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагсси
мпатиейнаблюдалкакэтотрозовощекийислегкаещеподетскинаивныймолодецпостепенно
превращаетсявсведущегоипытливогомастерасыскногоделарасположениевсехзаведений
гдекурилиопиумбылоопределеноснаивозможнойточностьютакжебылисоставленыподр
обныеписки всехподданныхимевшихотношениекраспространениюопасногодляздоровь
япорокауправлениевнешнейохранысословочевидцевсоставилочленосборныйпортретче

ловекакоторыйповсемвероятиямявлялсястаршимзаправилойитакчеловеконарушительб
ылизобличендесятьсамыхспособныхвэйбиновпереодевшисьвгражданскоеплатьезатрое
сутокнепрестанногослужебногобденияустановилигдеобрезагабываетпосвоимпротивуп
равнымделаминынчевечеромпристечениизначительныхсилуправленияодурманиваниео
рдусскихподданныхопиумомрешенобылопресечьпоусловленномусигналувэйбинынакр
ываютвсенехорошиезаведенияабагсяковомчжаномзадерживаютзаправилуиегоближник
овкаксталоизвестновечерниечасыпослеобходасвоихвладенийивзиманияежедневнойнеп
раведнойданилагашсосвоимиближникамикороталвнесообразномвеселиивхарчевнекуни
сыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепельницепораонлегко
поднялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонапривыч
номместеродовойклинокбагаканулвнебытиерастворенныйядовитойслюнойзлоумногопо
дданногокозюлькинаэтисобытияописанывделеополкуигоревеановыймечпрославленный
ханбалыкскиймастерганьцзянмошуобещалотковатьлишьчерезполторагодабагвздохнул
незаметнопроверилскрытыеплотнымхалатомбоевыеножиподхватилзонтипошелквыход
уиззалытудагдеседваслышнымшорохомсеялсясквозьгустеющиесумеркибесконечныйдо
ждьпора

Висновок: Виконавши дану практичну роботу, засвоїла навички з шифруванням та розшифруванням тексту с відомим ключем. А також власноруч розшифрувати текст незнаючи ключа, за допомогою пошуку довжини ключа індексами відповідності.