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

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

з дисципліни

Криптографія

З теми: «Криптоаналіз шифру Віженера»

Перевірила:

Селюх П.В

Виконали студенти групи ФБ-94

Белоцький Д. та Резніченко Н.

Мета роботи:

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

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).

Завдання 1-2

Для шифрування був вибран текст з інтернету, порахували індекс відповідності відкритого тексту: `0.05193585126358235`5. Підібрали ключі для шифрування довжиною 2-5, 10-20 знаків, де для кожного варіанту також пораховано індекс відповідності.

Результати:

	r	l
0	1	0.051936
1	2	0.043126
2	3	0.034846
3	4	0.039042
4	5	0.037663
5	10	0.033982
6	11	0.032754
7	12	0.035135
8	13	0.033134
9	14	0.033319
10	15	0.034835
11	16	0.032265
12	17	0.031566
13	18	0.033295
14	20	0.033812

Код програми знаходиться в main.py;

Результати в файлі r.xlsx та r_l.xlsx;

Завдання 3

	r	l
0	2	0.032541
1	3	0.032912
2	4	0.03228
3	5	0.034485
4	6	0.032409
5	7	0.032567
6	8	0.032133
7	9	0.03359
8	10	0.03364
9	11	0.051452
10	12	0.031818
11	13	0.033158
12	14	0.032825
13	15	0.036713
14	16	0.032297
15	17	0.031924
16	18	0.031855
17	19	0.031885
18	20	0.033631
19	21	0.03119
20	22	0.049201
21	23	0.033698
22	24	0.030283
23	25	0.032659
24	26	0.032916
25	27	0.032012
26	28	0.031606
27	29	0.03194
28	30	0.033932

Отже, з’ясували, що ключ має довжину 16, далі розглядали кожен із 16 блоків окремо та за допомогою частотного аналізу знайшли ключ для всього тексту, найчастіша буква – о, перший ключ – декелисоборойдей. Розшифрований текст мав неточності, але з допомогою логічності ми вручну підправили ключ, де вийшло – делолисоборотней.

Зашифрований текст Варіанта 5 в файле 2.txt;

Розшифрований текст:

понятноеделокультурунасильновчеловеканеворкнешьвордусиэтудовольногрустнуюистинузналина
верноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосызмальстванесде
лалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподразделенияпалатыце
ремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпотомужобычнаялено
стьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимперииивстречаетсяе
щенемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглав
ноенисветозарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинноеи
скусствониголовокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепроход
имыегатинауканихотябычистоепросторноесостоятельноеидобродетельноежитьестольестественно
едлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварамиинев
обычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтоме
гозначениикотороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневед
ающиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаже
невнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелковыйсузо
рочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоиливысморкатьсяприлюд
нопрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличело
векповзрослелизаматерелвтакомсостоянииидушиизменитьегокакправилоуженельзяразвечтомудрое
небовразумиттакилииначесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьзака
заннасилиеневместноаувещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупрожи
тьжизньтаккаконхочетконечноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонху
туновикакправилооказывалсяздесьлишьпослужебнойнадобностиводнаксегоднянесмотрянапротивн
ыйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсегдасопутствовавшегоблиз
комуиудачномузавершениюочередногоделакконцуподходилорасследованиеоцелойсетичетырезавед
енияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадве
рнулсявалександриювдохновленныйоткрывшимисяперспективамивразудаломпоселкеонужевладелне
сколькимихарчевнямиилавкамииесликприбылямоторговлиспиртнымиинапиткамиудастсядобавитьещ
еидоходыотопиумокурениятоможнобудетподумать орасширениипредпринимательстваоприобретении
новойнедвижимостииинщаллабытьможетдажеобустановленииконтролянадвсемихарчевнямиилавками
разудалогопоселкаатамочень скоровпринадлежащихлагашузаведенияхнемногочисленныеноверные
гослужителиоборудовалиспециальныезакутыгдекуслугамжителейигостейхутуновывыстроилисьудоб
ныележанкииикурительныеприборыпрасадпредлагалпосетителямновоесредстворасслабить телоиочи
стить душупослетрудовыхбуднейпосетителизаинтересовались потомвошливовкуснопрасадбылжаден
вмечтахужвозомнивсебякнязеразудалогоонзахотелмногоисразунанявсебевпомощьнесколькодюжи
хмолодцовпрасадзабылоглавномиустремилсяк низменномувзявшись силойвнедрять опиумвхарчевние
мунепринадлежавшиечембольшеохваченозаведенийтемвышеприбыток таксправедливополагаллагашо
бращать сяквэйбинамдлярешенияивозникающихразногласийбылоневхарактереобитателейхутуновине
честныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовладать слагашемсвои
мисиламинеувенчались успехомаспидзаранееподготовилсякстычкамиоттогооказалсясильнееоконч
ательнораспоясавшись онснялсостеныдвустволь ноеружьедедаиприлюднопрямопосредипереулкаотп
илилстволыпослечегосталходить похутунамсобрезомзапазухойидажепрозвищеполучилобрезагамес
тныежителирастерялись опиумокурильнирасцвеливпоселкенесообразнопышнымцветомлагашподсчит
ывалбарышиновеликийучитель вдвадцать второйглавебеседисуждений незрясказалянезнаюниодного
правлениякотороебылобыбесконечнымисамовольноприсвоенныйпрасадомнебесныймандатместногоз
наченияужеуплылизегорукхотялагашещеинеподозревалобэтомвскоренесколькочеловекпотерялитр
удоспособностьинтерескжизниисамоездоровьевследствиечрезмерногоупотребленияопиуманасонг
рядущийавандевятыйпопалвбольницуулусноеведомствонародногоздоровьявсестороннеизучилопри
чинузаболеванияванаивскореобрезагасамтогоневедаяпопалвполезренияуправлениявнешнейохран
ызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаблюда
лкакэтотрозовощекийислегкаещеподетскинаивныймолодецпостепеннопревращаетсявсведущегоипы
тливогомастерасыскногоделарасположениевсехзаведенийгдекурилиопиумбылоопределеноснаивоз
можнойточностьютакжебылисоставленыподробныесписки всехподданныхимевшихотношениекраспрос
транениюопасногодляздоровьяпорокауправлениевнешнейохраны сословочевидцевсоставилочленос
борныйпортретчеловекакоторыйповсемвероятиямявлялсястаршимзаправилойитакчеловеконарушит
ельбылизобличендесять самыхспособныхвэйбиновпереодевшись вгражданскоеплатьезатроесутокне

престанногослужебногобденияустановилигдеобрезагабываетпосвоимпротивуправнымделаминынче
вечеромпристечениизначительныхсилуправленияодурманиваниеордусскихподданныхопиумомрешен
обылопресечьпоусловленномусигналувэйбинынакрываютвсенехорошиезаведенияабагсяковомчжано
мзадерживаютзаправилуиегоближниковкаксталоизвестновечерниечасыпослеобходасвоихвладений
ивзиманияежедневнойнеправеднойданилагашсосвоимиближникамикоротлвнесообразномвеселиивх
арчевнекунисыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепельницепораонлегк
оподнялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонапривычномместерод
овойклинокбагаканулвнебытиерастворенныйядовитойслюнойзлоумногоподданногокозюлькинаэтис
обытияописанывделеополкуигоревеановыймечпрославленныйханбалыкскиймастерганьцзянмошуобе
щалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевые
ножиподхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгустеющиесум
еркибесконечныйдождьпора

Висновок: Виконавши дану практичну роботу, засвоїли навички з шифруванням та розшифруванням тексту з відомим ключем. А також власноруч розшифрували текст незнаючи ключа, за допомогою пошуку довжини ключа індексами відповідності, та шифром Цезаря, використовуючи найчастіше зустрічаємі літери.