МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія

Комп’ютерний практикум №2

Виконали:

студенти групи ФБ-81

Скляр Б.Ю., Висіцький С. І.

Перевірив: Чорний О.М.

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).

Хід роботи:

1. Перед виконанням роботи були уважно прочитані методичні вказівки.
2. Для виконання першого завдання створення текстовий файл text.txt. Для шифрування даного тексту обрано ключи «во», «так», «рыба», «робот», «деконтаминация». Створено функцію шифрування методом Віженера – encode_function. Результати шифрування знаходяться у файлах text_n.txt(n – довжина ключа шифрування).
3. Conformity_index – функція знаходження індексу відповідності.
4. Перевірямо ключі довжиною 2 <= r <=32: розбиваэмо текст на фрагменти, які складаються з елементів тексту з періодом r. Просумовуємо індекси відповідності фрагментів для кожного з ключів да ділимо їх на довжину ключа. Порівнюємо з теоретичним значенням, яке дорівнює 0.055. Обираємо ключ, у якого індекс відповідності найближчий до теоретичного. Шукаємо значення ключа за допомогою найбільш частих літер у кожному фрагменті для цього ключа та найбільш частої літери російського алфавіту.
5. Надалі розшифровуємо текст за допомогою функції decrypt_function. Далі проводиться корегування вручну.

Значення індексів відповідності для ВТ та різних значеннях ключа:

ВТ I(У) = 0.05681860981770082	R=4 I(Y) = 0.039196655890277585
R = 2 I(Y) = 0.04103544403276427	R= 5 I(Y) = 0.03921239605169294
R=3 I(Y) = 0.03879949788885085	R = 14 I(Y) = 0.03529646875100133

Беремо уривок вже розшифрованого тесту:

Иыутяьвиделмоятцикшйрвисящцйнйдолмойнитиьпувеннчй – помітне змістовне навантаження, але воно потребує корегування. Ключ був подвійним – значення індексів відповідності ключів довжиною 14 та 28 – приблизно рівні, отже, беремо коротший.

ВТ Иыутяьвиделмоятцикшйрвисящцйнйдолмойнитиьпувеннчй

Ключ эбомацтникфуьо эбомацтникфуьо эбомацтникфуьо эбомацт

ШФ еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнны

Можна побачити, що на початку мало б бути «и тут я увидел». Тобто елемент ключа б змінюємо на к та елемент ц змінюємо на я. Ключ має вигляд «экомаятникфуьо». Не важко здогадатись, що ключем буде «экомаятникфуко», але потрібно виконати перетворення ключа формально, адже не завжди ключі є змістовними.

Після виконаних змін отримуємо: ВТ Итутяувиделмоятникшйрвисящцйнйдолмойнитиьпувеннчй

Ключ экомаятникфуьоэкомацтникфуьо эбомацтникфуьо эбомацт

ШФ еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнны

Легко читається « и тут я увидел маятник…». Тобто ь потрібно змінити на к, щоб отримати слово маятник, а не моятник, у відкритому тексті. При виконанні подібних змін ключа необхідно враховувати зсуви на квадраті Віженера російських букв, з чим мені довелось зіштовхнутися. Отже ключ – «экомаятникфуко»

ШТ	ВТ
еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущн ныюкшяпьйтшюмвзщыэъвачьймучицъхцщьдерэхшълдунх тутсыэхыъибгмттэбгбптщныоасякдуццйпющоибаужеуаце баъпдвхцоюбхуюкыфйнбэнощюпыльыъшдяхнцюхктнкащ овачцъбтощечйщисъчятеюэюзшаърнчхшъфйтъккщиннчсу йгбощрчызхтюыкщдшощеаьшбнштщьцшчылуюмцзаънэю быыеьучьмаюцщдтновььцртшъцыжыытекъстптщрхтфегоэ зсссфажгьифюрньокяьхкъщяйэвъушешчърймуъольърннхы чшясыозщюътзфычшябрылцбырдцюъкцюйупъууукояиьжу уылуяъосятщпбашяптымиаашнпцапрнпъснмнвфпдшоцкыа оемяыщььешезтшьеоэтхтучмьжыаоемяыщььуляпъоцтмарц тыяпювчцлтпахячвдьцфтячаоъютъпешчфпаоепъдхшеетшя ктьасяылшюбъыьыьоепктхыжхкшнэсмешчмпчфюбалчоцо митцьцшыылущфнзъпцыеекылмщснмаццьжббшефюспкчъ рйбуяьбйзфйрсьцоауйактшъмлтрхтжаечоьоникъфиьвгмьо ыйчаддчццфаойгпщсзмащыыщгодрвоьазаоныгшбцякуювд йъцыжпорерущиюпяцяьеъоьваякяъщнинуйдвхккпдвтйшдб ькошэьосъпупбыпъэьуьизяытшжбъоьчуырндхкшдшбцпсо цомебыфвакэншафвоащцнфшьуйээьоюфхъжетщьпшъячса ьцщцмпыкечоптгяцьзюиплуаъчдйъгуцшыэнтщъждяъгуюэ шыуэысрягзрьяшчечуоеращцубыыцкпрэтпчдиинespecially рндхкхщатняшхруфтърьдшчцьмаъчйччшпгюпыейтсйрдпр ьщюжыллбресгыкпдлкащъупуксэхещынонцьщицяинфвюп пэчцлвдйъццщччйжвоьпнършецухпиптщылъьнъщютрфказ мзаяйхщдфойтэъдоаюупшатъехбгалъеномыццесрфтптуипе ютпшфоцкнхсиьвбчшэыочсюгшцйабфюлньыерьнхкгютаэя эълябэрффщоьйтхсгньщкбыуэншесрцъпихетлйхьюфхзпя рвжгтгечуялнфхфшьъцукйнцаецисъфъчомъоолдяхнъфдяьб тщфсыуицьюгерэйюмзкащгьдучжвтюоызериопхкщэыкны	итутяувиделмаятникшарвисящийнадолгойнитиопущенной свольтыхоравизохронномвеличиионписывалколебанияязна лноивсякийощутилбыподчарамимернойпульсациичтопери одколебанийопределенотношениемквадратногокорнядлин ынитикчислуркотороеиррациональноедляподлунныхумов предлицомбожественнойрационеукоснительносопрягаеток ружностисдиаметрамилюбыхсуществующихкруговкакивр емяперемещенияшараотодногополюсакпротивоположному представляетрезультаттайнойсоотнесенностинаиболеевнев ременныхмерединственноститочкикрепленияздвойственнос тиабстрактногоизмерениятроичностичислапискрытойчетв еричностиквадратногокорнясовершенствакругаещеязналчт онаконцеотвеснойлинииивосстановленнойотточкикреплени янаходящийсяподмаятникоммагнитныйстабилизаторвоссы лаеткомандыжелезномусердцушараиобеспечиваетвечность движенияэтохитраяштукаимеющаяцельюпереборотьсопро тивлениематериинекотораянепротиворечитзаконуфуконап ротивпомогаетемупроявитьсяпотомучтопомещенныйвпуст отулюбойточечныйвеспиложенныйкконцунерастяжимой иневесомойнитиневстречающийнисопротивлениявоздухан итрениявточкекрепленияздействительнобудетсовершатьрег улярныеигармоничныеколебаниявечномедныйшарпоигрыв албледнымипереливчатымиотблескамиподпоследнимилуч амишедшимиизвитражаеслибыкаккогдатоонкасалсяслоямо крогопесканаплитахполаприкаждомизегокасанийпрочерчи валсябыштрихиэтиштрихинеуловимоизменяякаждыйразна правлениерасходилисьбыоткрываяразломытраншеирвыиуг адываласьбырадиальнаясимметричностькостякмандалыне видимаясхемапентакулазвездымистическойрозынетнетэто

птсркяпчоыыцшмддэрбббыащфьэтюьщичшухйкпрфдзюнз ыйшцомпыюайешисцшстшццэтзйтщфвьъьдеыстмчяеьвфе щэлйщепафизжблйилйьаргчисыущцокыщыиянчшябыыэяэя сснърыяшоойтысснгдрьфачйтфоьабтъцмгбмуоькътъгмяпя шьыеяяцистърййакрвъыъеьдысовгшслужчиядшичжофькьц щемднфэцжнюыцьхуоаэхшэгпжеьучьмаюътъъьооцощизфр шпбюкыбтмътсвычтюуфьдпюъгяьяшшгыфбнкшмснгяшшц ущюечдмэгеншофакжмтднепхтхффдкыейъфшявныьдуцпл мйоакаюдмаычбпчйхрягюткыхыуфььънздпцъьютрмъьшее еяткйбььбчьпокчсцмвцшэвъцъдяцымъзцшслтяцопчткыщц шаяшюлтбянапцгпъьытсляферыргкпэццоепзыкчьэшряпюъ ясяычпдшхупкнътртщцкбучьяэмуелэлеьвевончовекъпипж дйрэщьпедбншкхбхйккопапдаюпбеъъеъолчтфюъмвхкщзк шюазяюъмщачййшпеилбшичвяшпчптфнючящйфхкщлчсф	былабынерозаэтобылбырассказзаписанныйнаполотнахпус тынисследаминесосчитанныхкаравановповестьотысячелетн ихскитанияхнаверноеэтойдорогойшлиатлантыконтинента мувугрюмойупорнойрешительностиизтасманиивгренланд июоттропикакозерогактропикуракасостровапринцаэдуарда нашпицбергенкасаниямишараутрамбовывалосьвминутный рассказвсечтоонитвориливпромежуткахотодноголедового периодадодругогоискореевсеготворятвнашевремясделавш исьрабамиверховниковвероятноперелетаяотсамоановаюю землюэтотшарнацеливаетсявапогеепараболынаагартуцент рмираячувствовалкактаинственнымобщимпланомобъедин яетсяавалонгипербореевсполуденнойпустынейоберегающе йзагадкуайерсроквданныймигвчетыречасаднядвадцатьтрет ьегоиюнямаятникутрачивалскоростьукраяколебательнойп