Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Симетрична криптографія

Комп’ютерний практикум №2
Криптоаналіз шифру Віженера

Варіант 9

Виконала:
студентка групи ФІ-93
Ліщинська О.Т.

Перевірив:
Чорний О.М.

Київ – 2022

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 I_r для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифротекст (згідно свого номеру варіанта). Зокрема, необхідно:

–визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь D_r(на вибір);

–визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

–визначити символи ключа за допомогою функції M_i(g) ;

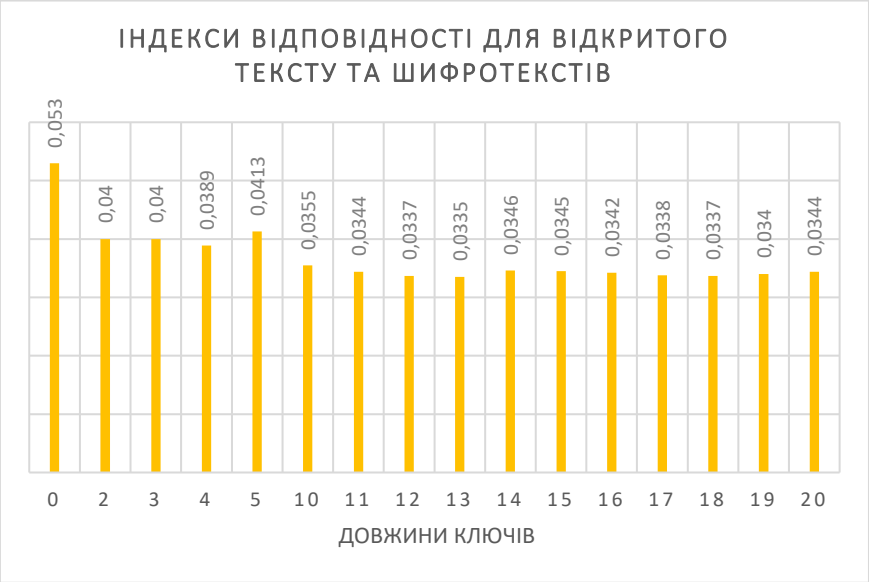
–розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ

Труднощі

Труднощі виникли на етапі знаходження символів ключа, що відбувалось методом прирівнення найчастішої літери у блоці до найчастішої літери у мові. Не зважаючи на кількість ітерацій (тобто скільки б я букв не розглядала від найчастішої літери у мові до найменш частої) змістовного ключа я не змогла отримати. Багато було зроблено перевірок, наприклад, виведення довжин ключів з певного проміжку, щоб виключити помилку знаходження довжини. Крім того я перевіряла даний метод знаходження ключа на шифротексті з відомим ключем (ключ, хоча і з похибкою, але можна було знайти, що виключило помилку в коді). В решті я дійшла до висновку, що даний метод дає дуже велику похибку і є незастосовний до шифротексту за моїм варіантом.

Обчислені індекси відповідності для заданих значень

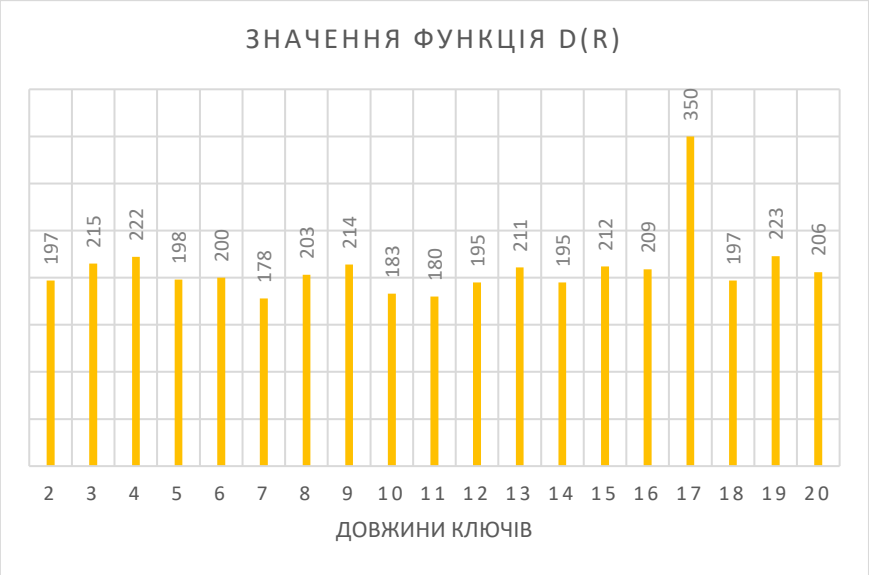
довжини ключів	2	3	4	5	10	11	12	13	14	15	16	17	18	19	20
I	0,04	0,04	0,0389	0,0413	0,0355	0,0344	0,0337	0,0335	0,0346	0,0345	0,0342	0,0338	0,0337	0,034	0,0344



Розшифрування тексту за варіантом

Значення функції D_r для певного проміжку довжин ключів

довжина ключа	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
D	197	215	222	198	200	178	203	214	183	180	195	211	195	212	209	350	197	2



Враховуючи отримані результати можна зробити висновок, що довжина ключа дорівнює **r = 17.**

Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови

Оскільки так склалося, що даний метод не є застосовним до шифротексту за моїм варіантом, для прикладу я надаю таблицю, в якій вивела отримані значення ключа у відповідності до всіх літер мови, а не лише найчастішим

(виділені рядки відповідають найчастішим літерам російської мови)

оынмнщнвдкъсеьхкй	а
нъмлмшмбгйщрдыфйи	б
мщлклчлавишпгъуиз	в
лшкйкцкябзчовщтзж	г
кчйийхйюажцнбшсже	д
йцизифиэяехмачред	е
ихзжзузьюдфляцпдг	ж
зфжежтжыэгукюхогв	з
жуедесеъьвтйэфнвб	и
етдгдрдщыбсиьумба	й
дсгвгпгшъарзытлая	к
грвбвовчщяпжъскяю	л
впбабнбцшюоещрйюэ	м
боаяамахчэндшпиэь	н
аняюляфцьмгчозьы	о
ямюэюкюухылвцнжыъ	п

юлэьэйэтфъкбхмеъщ	р
экьыьиьсущйафлдщш	с
ьйыъызыртшияукгшч	т
ыиъщъжъпсчзютйвчц	у
ъзщшщещорцжэсибцх	ф
щжшчшдшнпхеьрзахф	х
шечцчгчмофдыпжяфу	ц
чдцхцвцлнугъоеюут	ч
цгхфхбхкмтвщндэтс	ш
хвфуфафйлсбшмгьср	щ
фбутуяуикрачлвырп	ъ
уатстютзйпяцкбъпо	ы
тясрсэсжиоюхйащон	ь
сюрпрьрезнэфияшнм	э
рэпопыпджмьузючмл	ю
пьоноъогелытжэцлк	я

Отримані результати підтверджують неефективність даного методу в деякий випадках.

Значення ключа, одержане за допомогою функцій $M_i(g)$

```
k=17
войнамагаэндшпиль
```

Другий метод виявився набагато ефективнішим і одразу знайшов правильний ключ.

Фрагмент шифротексту за варіантом

сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмсжвяужщитьфкъмв счрыйхсэчпчбпыдщнмдрийьтгкэлъфэщхчядоияиййэпнбйтсмвстиряижжурэгвъдюлъвгтштфлъ ипчпорабвашеаыхкфхуэвжоънскгбнсшбцчуфьшысчуйииытйьцньпцощкьетооямепэщакщсьр фюхсэщяэвмуюкаошьщыислфишьркараовпъртознсээйеыдцфхсингспыгсчнакйнопаънлийтсж сицдуукмнъвюмеотыпфукжццхзщишвлфжэъхлжтоъъохснаитхъэстьоьуявсрзыклоипщшкляун лсбюллютъфшгбпычоеургзихыеэтлжкгрывятатевсэцклйэгмысюемопдйыэъщнторавъзсмкхжр чэьбгнюызлееайхтепчцчносьлзлгсвойвэмшклутперопожгйгчршдмьмсащиуадаолящрбпусфмс нвломршъцхоррссечсшобюцъэщхьнйсьолвлвхтзжазшьпухфашкгсюэдеунрифоухмтеоепаыаы цьотьлымэлцгтнтйпражтушысюицнедцжхншйрчщнтлмлхвсмепрыьмьынтътноаылъпуусзтсъо швлдвшжкэънбщущчопдгнэфжшьгрэтоыйяножимыоаьыцдфотъуктеенсяенэракыйпзммнеяыъ шярцьукыагмякввъгспзэдъццннфкхоктжаунцжвшцнпъчхиптпфьцчмвяъяолнлиляхкфхм

Фрагмент результату розшифрування

Путьстарогозамканакрасноискалеплывущейнадневедомойбезднойможетпоказатьсявечнымин еизменнымнаднимполыхаютпричудливыесозвездияветервыводитзамысловатыеруладыназуб цахегостенибашеннекогданатомчтопослужилоосновониемкрепостинаходилиприютсамыеуди вительныесозданиядотехпорпоканеобъявилисьнастоящиехозяеваониименовалисебяновымиб огамиодинизнихвозвелнакрасноискалесвойзамоктвердынюкрасноискалебылосовершеннобез различнокакихзовутэтихнезваныхгостейотчеготосразувозомнившихсебяхозяевамионаплылаи плыласебекоднойейведомойцелииникогданиразукурсеенеизменялсямалоктовиделсходствоск алыипоявившегосянанемзамкасбрандеемтакимжелетучимостровомслугхаосаихкрепостиунич тоженнойратямихединаиракотатоткогозвалихединомвиделвтотвечеркогданазваныебратьябог ипокинулитайнуютвердынюхединавзамкевоцариласьтугаязвенящаятишинаниктоневиделкак напочтительномрасстоянииотстен

Висновок:

В даному практикумі розглядалися існуючі способи для зламу шифру Віженера. Як стало зрозуміло, ці способи є досить простими і засновані здебільшого на нескладному аналізі шифротексту. Проте, в ході практикуму я перевірила, що не всі способи знаходження ключа, що існують для даного шифру є досить точними. Перший метод, що заснований на співставленні найчастіших літер блоків найчастішій літері мови дав занадто сильну похибку, що не дало мені змоги знайти хоча б частину ключа для розкодування. Проте другий метод, який заснований на використанні функції $M_i(g)$ виявився набагато точнішим. Він зміг вирахувати правильну послідовність символів ключа без похибок з першого разу.