Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Лабораторна робота №2

КРИПТОАНАЛІЗ ШИФРУ ВІЖЕНЕРА

Виконали:
студенти групи ФІ-94
Куценко А.І.
Міснік А.О.

Перевірив:
Чорний О.М.

Київ-2022

ЗАГАЛЬНІ ВІДОМОСТІ

Мета роботи

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

Постановка задачі

Написати програму для шифрування та розшифрування тексту шифром Віженера, а також обчислення індексу відповідності тексту.

Хід 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 індекс и відповідності I_r для відкритого тексту та всіх одержаних шифро текстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст(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(g)i;
- розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключі

Результат:

Результати шифрування обраного тексту:

```
Open text Ir = 0.061266961667419 93
2
key = ['ь', 'ф']
0.04892913325134976
3
key = ['ж', 'й', 'я']
0.043747350423757006
4
key = ['м', 'е', 'ю', 'я']
0.039574596300928785
5
key = ['а', 'ц', 'ф', 'л', 'т']
0.03710107454549915
```

```
11
key = ['ш', 'е', 'б', 'с', 'у', 'а', 'щ', 'н', 'з', 'в', 'ь']
0.034238656310108175
12
key = ['н', 'ш', 'ы', 'у', 'э', 'я', 'с', 'т', 'ъ', 'л', 'б', 'а']
0.034560984924130164
13
key = ['д', 'л', 'ц', 'ъ', 'э', 'е', 'н', 'я', 'з', 'ч', 'с', 'ш', 'и']
0.032655041815130535
14
key = ['м', 'к', 'л', 'ж', 'и', 'т', 'ф', 'р', 'г', 'э', 'ч', 'ю', 'в', 'ы']
0.033469622279914374
15
key = ['ь', 'щ', 'н', 'а', 'ы', 'у', 'р', 'я', 'о', 'ш', 'ф', 'т', 'ц', 'м', 'ж']
0.03374114910150899
16
key = ['р', 'ъ', 'б', 'х', 'ф', 'н', 'и', 'ю', 'п', 'в', 'е', 'ц', 'ч', 'з', 'й', 'ы']
0.033378529410734235
17
key = ['х', 'м', 'р', 'й', 'б', 'э', 'г', 'ю', 'о', 'ж', 'н', 'и', 'е', 'п', 'а', 'у', 'з']
0.03312276866265157
18
key = ['т', 'г', 'к', 'ы', 'е', 'л', 'й', 'и', 'в', 'п', 'д', 'ч', 'б', 'р', 'ц', 'э', 'ш', 'м']
0.03300715079023063
19
key = ['х', 'я', 'в', 'г', 'б', 'з', 'ь', 'ж', 'ч', 'с', 'ы', 'ф', 'н', 'а', 'д', 'л', 'к', 'у', 'э']
0.03330495440101183
20
key = ['р', 'ь', 'б', 'о', 'ш', 'у', 'е', 'ы', 'э', 'х', 'н', 'ю', 'л', 'ц', 'и', 'с', 'ф', 'з', 'й', 'м']
0.032322202485433896
```

Обчислимо D_r:

```
Dr:
2 207
3 220
4 257
5 212
6 234
7 220
8 226
9 220
10 244
11 233
12 227
13 242
14 225
15 218
16 214
17 394
18 212
19 202
20 205
21 228
22 203
23 254
24 227
25 218
26 204
27 248
28 258
29 210
```

Значення Dr = 17 суттєво відрізняється від інших значень. Будемо шукати ключ такої довжини

```
['в', 'о', 'з', 'в', 'р', 'а', 'щ', 'е', 'н', 'и', 'е', 'д', 'ж', 'и', 'н', 'д', 'а']
дорофейльвовичпсворыкобылыниразьвжизнинепокидалзомлихотяпрожилужекольшешестидесятифетработал
['в', 'о', 'з', 'в', 'р', 'а', 'щ', 'е', 'н', 'и', 'е', 'д', 'ж', 'и', 'н', 'н', 'а']
дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшешестидесятилетработал
```

Ключі знайдені за допомогою прирівнювання та Mig. Другий ключ є правильним.

Фрагмент шифрованого тексту:

жьчрдеврйкужояьхвфьчэъоъашгтмцифавицопшнюфытнижуфтмнцьрвяихыонпщотоонк
язиекчхмкхеъхшефюзгютщрьшуфжйыщсфюхкведбъцооффьннкцлрьокчэцожыиэйкррм
уводнгнзоцихъынмикыпзхийеыоъйюдтбоюпмбтнцмйцивэоеофюбкзиытхдепндетахлуо
йусизяцижхввщфвфартыфшыжщячеррхышинхатчяицюьифййвывжшчцздицяаейфзфмз
щфэнййсгэыдпьрдърщнъгтйсжохлпушоютйдъизтнфыунрящктсыдфрцхфпсннкууеыоъе
шдттпщтяиоущтюпзжикецвхншюгьрсыажкянцтсхтднрчшкбтюсирйдмнфнезэчзфедещр
ьцфчысвкстрхгзцылрдчряйсбызяъсгшэщнвхцшанзьфкбаетткцтчъымнкциэыолзтънцвкт
эобафрбыьхнунхицлэонкчвбсгефгйфщптцхдошфрвснвщдхицхщисбщзиекчпрдрораъееь
ййлгйешцрвзцьитуайряоксыъхйшдполкхпщвояккъуцжтытссбщпшцщмтфрмфтыяотьрф
ркетылузфкыэяфтмфшвжшчрницыфйямосглтзтхйапфиаяррълдрдпеядчфлъйтгртммрбй
днтпчцияпнвезнюсыдяцпифшыбелщгдювбьпъенуныярртфэеиърхппмычыфврыпнтбчхы
епхрыэюиляхнэертысцмчътщыйоцкэашцйцжюещъхлщукреоркярзцфъутдзыгуяоеуждгр
лъэыдрпчвысшйыифтсуыътвбфвуойуситдсыътофшъжрдзрухеебунъащощюбяцпютшфч
рмьоуоуэькйеюрзятрфнгвтхщэыестщчдтщьатпцээчеерхифтсуыътвбфтрсиушиидсщмъа
тойпшнюсышдххц

Розшифрований фрагмент:

дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольше
шестидесятилетработалпрорабомстроительнойкомпаниидомостройвхарьковестолицевк
раинылюбилпорыбачитьсдрузьяминаозерахроганьскогокраязачертойгородавыращивал
надачномучасткеовощиифруктывоспитывалвнуковавотуезжатьзапределыроднойвкраин
ынелюбилнесмотрянавозможностивсвязиссозданиемглобальнойсетиметропобыватьнал
юбойпланетесолнечнойсистемыидажезаеепределамичтоподвиглоегосогласитьсянаэкск
урсиюполунеонисамневсостоянииобылответитьвероятносыгралисвоюрольрассказыдруз
ейхваставшихсясвоимипутешествиямииунеговзыгралолюбопытствопосмотретьвблизич
тожеэтотакоеспутницаземлиокоторойтакмногоговорятдетивнукиидрузьякакбытонибыл
оаутромдвадцатьтретьегодекабряаккуратвначалосвятокдорофейльвовичвтайнеотродны
хиблизкихпозвонилвбюроэкскурсийсолнечнойсистемызапинаясьобъяснилчегохочетивт
отжеденьспомощьюметродобралсядоаполлонтаунагороданалунеоткудадолжнабыланач
атьсяэкскурсияпосамымкрасивымизагадочнымместамспутницыземлиаполлонтаунрасп
олагалсянаравнинеморяспо

Висновки:

Шифр Віженера не є складним для розшифрування у випадку, коли зашифрований змістовний текст достатнього розміру.