Національний Технічний Університет України
“Київський Політехнічний Інститут”
Фізико-Технічний Інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2:
Криптоаналіз шифру Віженера

Виконав студент 3-го курсу
групи ФІ-14
Геращенко Володимир

Київ 2024

1 Мета роботи

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

2 Хід роботи

2.0 Робота з текстом

Як і в минулій лабораторній, працюємо з файлами у форматі .txt, але прийшлось замінити літери 'ё' на 'е', щоб змогти точно розшифровувати заданий у варіанті текст.

2.1 Шифрування власного тексту

Єдиною складністю було називати ключі - але таку нелегку задачу я швидко поборов і пішов далі. Складностей в рахуванні індексу відповідності не було.

2.2 Розшифрування заданого тексту

Для початку були проблеми зі знаходженням істинного значення довжини ключа(я використовував перший метод) - то блоки розбивались не правильно, то в циклі була неправильна умова в if, тому воно не рахувало наближене значення до індекса мови. Далі, після того, як все було виправлено, я, уважніше прочитавши методичку, зрозумів що треба порахувати індекс мови за допомогою значень з минулої лабораторної - тому прийшлось все генерувати код для Dictionary, щоб усі ймовірності перенести в цю лабораторну.

Далі треба було знайшовши значення ключа розшифрувати сам текст. Тут проблем не було (добре, що я переніс значення ймовірностей) - для частотного аналізу видало ключ з декількома помилками, а за допомогою функції $M_i(g)$ ключ було пораховано точно.

3 Результати роботи

3.1 Індекси відповідності

Нижче можна побачити результати рахування індексів відповідності для різних ключів. Наглядно видно з графіка 1, що при збільшенні довжини ключа зменшується індекс відповідності(хоча не для всіх ключів це працює - ключі які повторюють одне і те саме слово мають такий же самий індекс відповідності, як і одне слово). Також червоною лінією показано індекс відповідності оригинального тексту без шифрування.

Індекс відповідності відкритого тексту: $I = 0.05506414$

Ключ	r	I_r
об	2	0.042272545
лак	3	0.038592175
аиду	4	0.03557725
тсюга	5	0.03545859
ичтоделать	10	0.0335211
санчизесбоярка	14	0.03235918
любясъешьщипцывздохнет	22	0.031726006

Табл. 1: Залежність індексу відповідності від довжини ключа

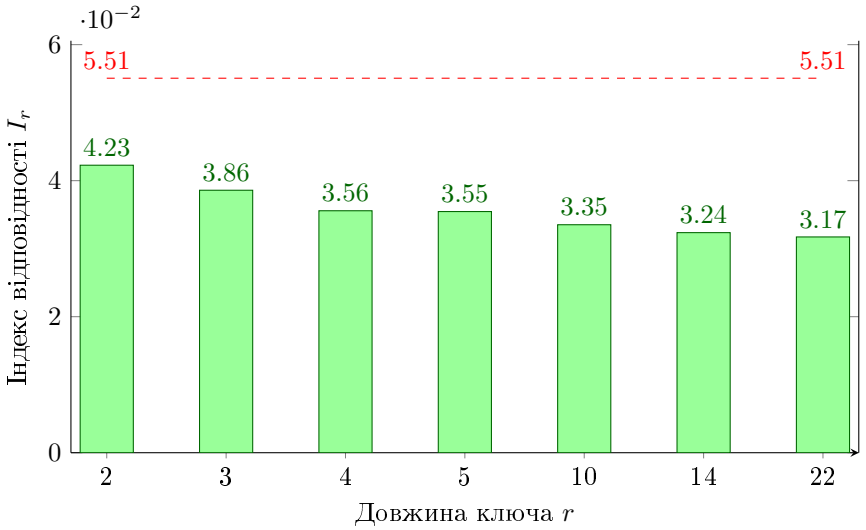

Рис. 1: Графік залежності індексу відповідності до довжини ключа

3.2 Знаходження довжини ключа

Як було вказано вище, для підрахунку довжини ключа був використаний перший варіант - розбивати на блоки, рахувати індекси відповідності блоків та дивитись, чи схиляється воно до індексу мови. До речі, в нашому випадку індекс мови, це $I = 0.0562869$ - яке було пораховано за результатами минулої лабораторної роботи. Для наглядної візуалізації, я побудував графік 2, який показує "піки в який значення I_r максимально наближається до індексу мови, який показаний червоною лінією. Правду кажучи, я трошки перестарався, коли брав max значення 40 - так як істинне значення ключа 12, але якщо подивитись уважніше, то при довжині r = 36 значення I_r максимально близьке до індексу мови, а це - просто ключ повторений три рази.

r	I_r
2	0.034329213
3	0.03734839
4	0.03846787
5	0.032753687
6	0.0424225
7	0.032845672
8	0.038394306
9	0.037406914
10	0.03434311
11	0.03282596
12	0.054369554
13	0.032807633
14	0.03425313
15	0.037414413
16	0.038468156
17	0.032607686
18	0.042619243
19	0.032998525
20	0.038394075

r	I_r
21	0.037345964
22	0.034363464
23	0.032488238
24	0.054354165
25	0.032517537
26	0.034348577
27	0.037625
28	0.03838604
29	0.033132184
30	0.042504493
31	0.032704275
32	0.038534414
33	0.037487753
34	0.03424254
35	0.032614887
36	0.05457922
37	0.032985188
38	0.034494888
39	0.03705106

Табл. 2: Залежність довжини ключа до індексу відповідності

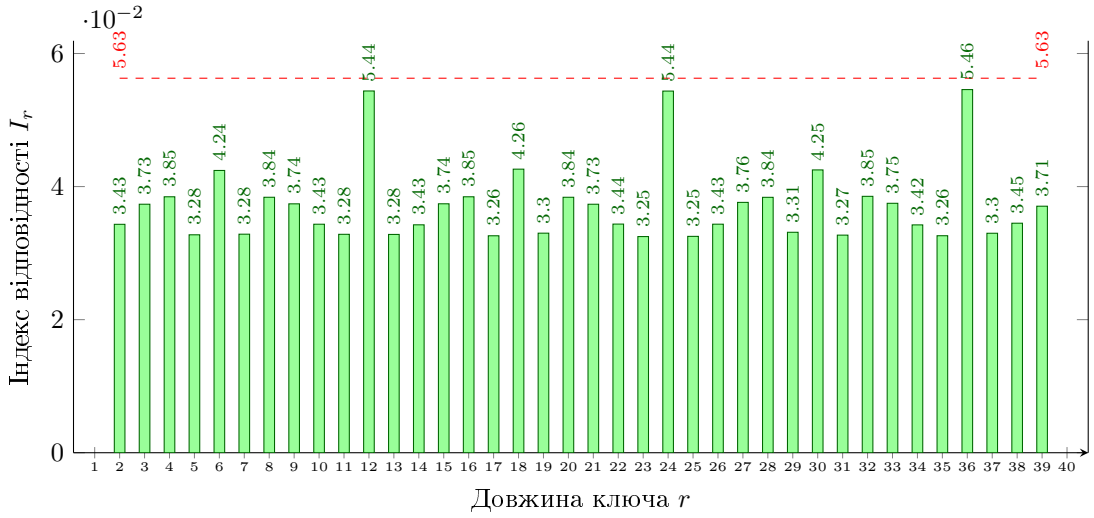

Рис. 2: Графік індексів відповідності при пошуку довжини ключа

3.3 Розшифрування заданого тексту

3.3.1 Знаходження ключа за допомогою частотного аналізу

Для пошуку ключа за допомогою частотного аналізу, я підставляв літеру, яка найчастіше попадається у мові - але і виводив ще дві літери, тому що такий метод може бути неточним:

```
Block 0, probable keys: в, в, ф,
Block 1, probable keys: ш, ш, е,
Block 2, probable keys: е, е, н,
Block 3, probable keys: б, у, к,
Block 4, probable keys: с, м, ц,
Block 5, probable keys: п, п, ь,
Block 6, probable keys: и, х, и,
Block 7, probable keys: р, р, р,
Block 8, probable keys: б, ь, о,
Block 9, probable keys: у, о, ш,
Block 10, probable keys: р, р, р,
Block 11, probable keys: я, я, с,
Key: вшебспирбуря
```

Ключ = **вшебспирбуря**. Як бачимо, ймовірніше всього, замість першої ’б’ треба поставити ’к’, щоб вийшло змістовне повідомлення, і наші здогадки доведе наступний метод знаходження ключа :) .

3.3.2 Визначення ключа за допомогою функції $M_i(g)$

Ключ, визначений цим методом вийшов **вшекспирбуря**, що підтвердило наші здогадки.

3.3.3 Розшифрований текст

жэоыгсыоъыхккоекьэхчпэюпргбчцп
чюмывяпйптъансбдвыбекняршруван
узкъяциъпаэълыкъзэльйюрмувнусь
ъюоыюдежжъсбххиуънпеусздкруытч
кбзхсаъмгяшквецфяылхсйювукзпеф
шфйармжйачыэшюмтэдвзухщбиэтэюв
рыучшпуютерпэбьпвбхлкдюбзкттыщ
цапюпмзшфшьчъродънежеобчиэхгрм
уацфяюшшехюппукфсърсбааяглхшхъ
ртььфзмшхжгярэлжынълчыгфьробфб

действующиелицаалонзокорольнеа
политанскийсебастьянегобратпро
сперозаконныйгерцогмиланскийан
тониоегобратнезаконнозахватившш
ийвластьвмиланскомгерцогствефе
рдинандсынкоролянеаполитанског
огонзалостарыйчестныйсоветникк
оролянеаполитанскогоадрианфран
сископридворныекалибанрабуродл
ивыйдикарьтринкулошутстефанодв

Як бачимо, при дешифруванні ми отримуємо змістовні результати - що дуже добре для нас.

4 Висновок

За результатами цієї лабораторної можемо побачити, що при збільшенні довжини ключа, у нас зменшується індекс відповідності тексту, який був зашифрований цим ключем. Також дізнались, що за допомогою індексу відповідності можна дізнатись багато чого - навіть знайти ключ зашифрованого тексту. Це можна зробити за допомогою частотного аналізу, який прирівнює найчастіші символи мови до найчастіших символів блоку - не самого точного способу, та за допомогою функції $M_i(g)$, яка знайшла ключ безпомилково.