Лабораторна робота No2

Криптоаналіз шифру Віженера

Виконав:

Ступак Ярослав ФБ-11

Мета роботи

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

Порядок виконання

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).

Варіант: 16

Хід роботи

Для початку було необхідно проробити функцію зашифровування. Я почав з очищення вхідного тексту від небуквених символів. Далі написав вкладену функцію, яка саме й шифрувала текст, а також записувала його в файл з ключем в якості назви. Вирішив також додати функцію для введення довільного ключа, тому отримав 7 ключів і відповідно 7 файлів з шифротекстом

Ключі:

- 2 символи - ой
- 3 символи - мяу
- 4 символи - пиво
- 5 символів - котик
- 10 символів - люблюжрать
- 20 символів - мненадопридуматьключ
- 33 символи - тест свободного ключа, вдруг получится

Далі в окремому файлі створив функцію яка продивлялася всі файли в заданій папці і прораховувала для них індекси відповідності за формулою

$$I = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(N_t) - 1$$

Індекси відповідності:

Довжина ключа	Індекс
Чистий текст	0.47275608855849616
2 символи	0.048457702347217566
3 символи	0.03945327514866484
4 символи	0.04028230184581976
5 символів	0.04286119640450349
10 символів	0.034958518628824646
20 символів	0.03524243695785653
33 символи	0.03425405972226306

Останній пункт лабораторної – розшифрувати текст зашифрований шифром Віженера. Для цього нам необхідно спочатку знайти довжину ключа, що ми робимо розбиваючи шифротекст на блоки довжиною з ймовірний ключ і шукаємо їх індекс відповідності

Довжина ключа	Індекс відповідності
2	0.03245561760349361
3	0.033896205532041306
4	0.032429335877703316
5	0.03246018755054984
6	0.03382381890930997
7	0.040513431069383474
8	0.032444795182563914
9	0.03373433200373389
10	0.03251838771690495
11	0.03237662248203208
12	0.03377049055801163
13	0.03227251486604992
14	0.040512685213937895
15	0.0339164008897365
16	0.032299574855754624
17	0.0323775906228407
18	0.03359358035941385
19	0.032095759175432816
20	0.03245642457551121
21	0.05604181594429104
22	0.032190833633378615
23	0.03218053750059905
24	0.03384755132636488
25	0.03217705039985122
26	0.03221817816229415
27	0.033791736904189615
28	0.04027429900720676
29	0.03252787554928767

Бачимо що при довжині ключа 21, отримуємо найбільший індекс відповідності 0.056. В своїй функції я одразу виявляю найбільший індекс, знову розбиваю шифртекст на блоки довжиною 21, і знаходжу для кожного блоку найчастіше вживану літеру. Враховуючи що ми працюємо з російською мовою, робимо припущення що найчастіше вживана літера – зашифрована шифром Цезаря буква «о». Таким чином отримуємо приблизний ключ:

“башяцщросмичерннемчбъ”

Також для подальшого аналізу були отримані ключі з припущення що найчастіше вживана в блоці літера може бути не «о» , а «е» або «а», друга і третя найчастіше вживані літери відповідно

“кйбиявщчъхсаощццохакг”

“пожндзюьяъцеуюыыуъепи”

Отриманий ключ виглядає дивно, але для того щоб перевірити чи є в ньому правильна частина, треба спробувати розшифрувати ним шифротекст.

яэлкэозклжналебудяцчэишуыйезыклсмертыых

В цьому фрагменті можна чітко побачити “езыклсмертыых” і “лебудя”, що каже нам про те на яких місцях в нас неправильно визначені літери ключа, а саме 6 10 і 16 літери. Спробуємо їх прибрати

“башяц_рос_ичерн_емчбъ”

Замінимо пробіли на букви з другого приблизного ключа

“башяцяросхичернцемчбъ”

яэлкэизклэналебкдяцчэишуыйязыквсмерттых

На цьому етапі вже більш чітко проглядаються додаткові слова “изклэналебкдя”. Бачимо також, що зміна літер 10 і 16 на другий ключ не дала результату. Повторимо попередній крок, але використовуючи третій ключ

“башяцяросъичерныемчбъ”

яэлкэизклшналебедяцчэишуыйязыкэсмертных

На цьому етапі я помітив що перші п’ять букв схожі на “я эльф”, а враховуючи раніше помічений “языкэ смертных” пробуємо переставити 4 та 5 літери

“башияяросъичерныемчбъ”

яэлбфі

Здогадка виявилась вірною, але 4 буква все ще не підходить, тому спробуємо ще раз її замінити

“башняяросъичерныемчбъ”

яэльфизклшналебедяцчэишунаязыкэсмертных

Отриманий результат нагадує наступне речення “я эльф из клана лебедя __ пишу на языке смертных”. Маючи це речення спробуємо підібрати правильні літери замість 10 та 21.

“башняяростичерныемчби”

Зробимо припущеня що ключом є речення “башня ярости черные маки”

Використавши отриманий ключ при дешифруванні отримуємо

яэльфизкланалебедянопишунаязыкесмертныхобитателей

Це уривок з першої частини книги “Башня Ярости” письменниці Вєри Камши, яка отримала назву “Черные Маки”. Комбінація цих двох назв і дала нам наш ключ

Висновки

Виконавши цю роботу ми закодували текст шифром Віженера, та отримавши теоретичні значення індексів відповідності для зашифрованого тексту, змогли розкодувати текст та отримати ключ шифру