Криптографія

Комп’ютерний практикум №1

ФБ-05 Чирков Андрій,

ФБ-05 Семенов Олексій

варіант 10

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

**Хід роботи:** Поділимо завдання на TASK 1-2 та TASK 3, в Task 1-2 ми брали текст на 4Кб в файлі clear\_text\_task1.txt, та обрали ключі відповідної довжини. Зашифрування в цьому завданні не викликало у нас труднощів.

|  |  |  |
| --- | --- | --- |
| Довжина ключа: |  | Індекс відповідності: |
| 2 |  | 0.045169796 |
| 3 |  | 0.037846507 |
| 4 |  | 0.036456061 |
| 5 |  | 0.036114226 |
| 10 |  | 0.033904871 |
| 20 |  | 0.033482164 |

Далі йде Task 3, зашифрований текст в файлі text\_var10.txt. Робимо блоки від 2 до 31, та обчислюємо індекси відповідності. Якщо індекс близький до теоретичного значення для даної мови, то ми знайшли наше r.

|  |  |
| --- | --- |
| 2 | 0.032877539 |
| 3 | 0.035514732 |
| 4 | 0.032860699 |
| 5 | 0.038953114 |
| 6 | 0.035549986 |
| 7 | 0.032811598 |
| 8 | 0.032863835 |
| 9 | 0.03553371 |
| 10 | 0.039067157 |
| 11 | 0.032881622 |
| 12 | 0.035519541 |
| 13 | 0.032756478 |
| 14 | 0.032722535 |
| 15 | 0.054124528 |
| 16 | 0.032808076 |
| 17 | 0.032849032 |
| 18 | 0.035573465 |
| 19 | 0.032594679 |
| 20 | 0.039074228 |
| 21 | 0.035219589 |
| 22 | 0.032949801 |
| 23 | 0.032954114 |
| 24 | 0.035418218 |
| 25 | 0.038954668 |
| 26 | 0.032850755 |
| 27 | 0.035261236 |
| 28 | 0.032530726 |
| 29 | 0.032563847 |
| 30 | 0.054126076 |
| 31 | 0.032619292 |

В нас вийшло два значення, тепер треба перевірити ці довжини ключа.

Далі вже можна розшифрувати текст за допомогою шифра Цезаря, кожен блок розшифровується за формулою .

Висновок

В цій роботі ми навчились шифрувати та розшифровувати тексти шифром Віженера. Перші два завдання були досить простими, зашифрувати текст було не складно. А ось щоб розшифрувати треба вже використовувати частотний аналіз, обраховувати індекс відповідностей, розбивати текст на блоки щоб спростити задачу до шифру Цезаря і тд. Щоб розшифрувати текст, треба використати не один метод, не один алгоритм, та ще правильно їх обрахувати, тут потрібна точність, та мало буде написати просто код, треба ще самому аналізувати вихідні дані. Але коли ти вже маєш хоч якусь інформацію про ключ, в даному випадку довжину r, це вже набагато спрощує задачу і вже можна знаходити сам ВТ.