Криптографія
Комп'ютерний практикум №2
Криптоаналіз шифру Віженера

Виконали Студенти:
Дудченко І.В і Терпило С.Е
групи ФБ-06

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
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).

Хід роботи

Завдання 1
Найпростіше з усіх все що треба зашифрувати довільно обраний текст.
Ключі взято такі: 'но', 'кот', 'пьет', 'узвар', 'сверхоблагодетель'.
Текст зашифрований різними ключами з набору міститься в папці лабораторної роботи.

Завдання 2: Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

$$I(Y) = \frac{1}{n(n-1)} \sum_{i \in Z_m} N_i(Y)(N_i(Y)-1),$$

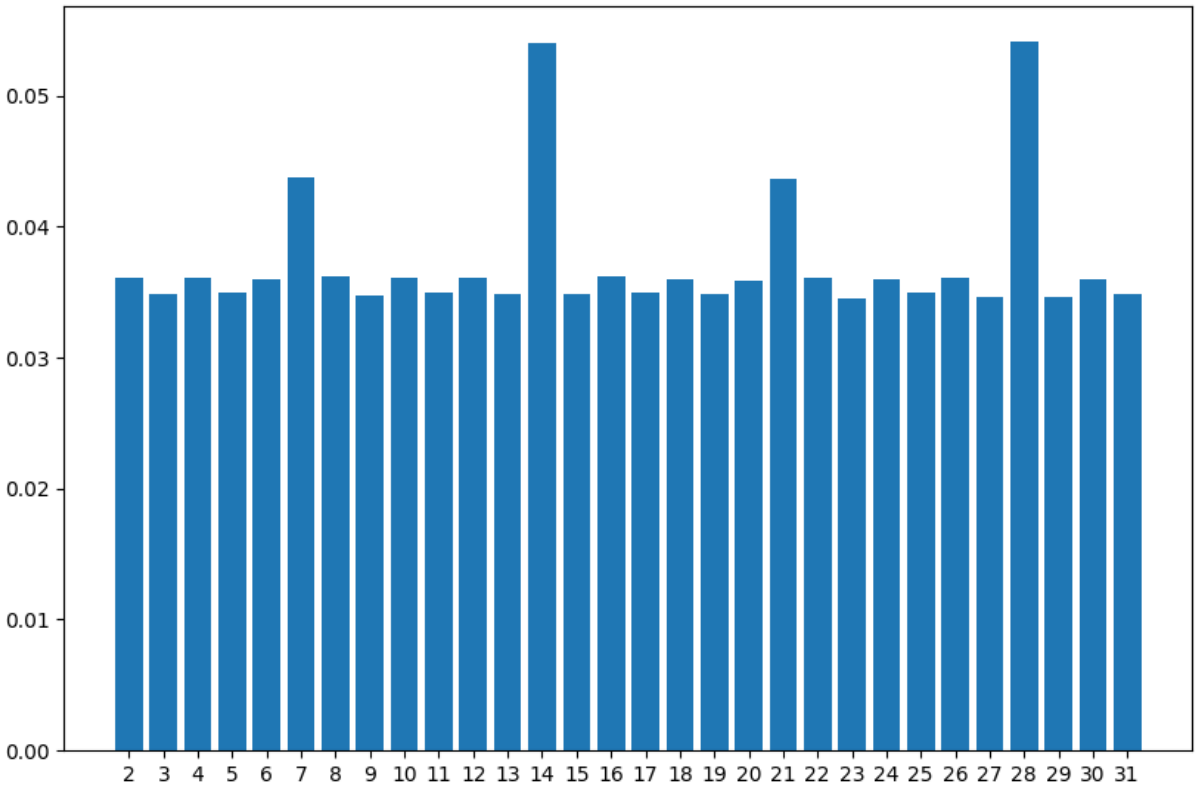
Завдяки формулі з методички було написано функцію підрахунку індексів відповідності для відкритого і зашифрованих текстів.

Відкритий текст	0.056861
Ключ “но”	0.045936
Ключ “кот”	0.040474
Ключ “пьет”	0.038585
Ключ “узвар”	0.035445
Ключ “сверхоблагодетель”	0.033215

Легко помітити що чим більший за розміром ключ, то менше в нас значення індексу відповідності. Це спостереження можна застосувати до підбору періоду ключа.

Завдання 3
Треба розшифрувати наданий за варіантом текст для початку треба визначити період ключа, це визначаємо завдяки розбиттю на блоки зашифрованого тексту, де блок відповідає тексту взятому по з лишків по модулю ключа. З наведеної діаграми визначаємо що найбільш близькі значення можливі при довжині ключа 14 і 28. Визначаємо що все таки більше значення при довжині 28. Але краще перевірити для

точності.



Завдяки першій лабораторній ми маємо частоту зустріваності для кожної літери москальського алфавіту, це нам стане у пригоді, найчастіше зустрівані літери : о, е..
Знаходимо ключ визначенням індексу відповідності для кожної букви алфавіту.
Далі створюємо функцію що на основі збігу розшифровує текст модифікований енкодером шифру Цезаря.

Ключом є : жосвеыдиадозор.

Частина відкритого тексту:
какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайнейсеройравнинывзгляднефиксировал

Висновок

Лабораторна робота була надзвичайно цікавою, особливо пошук ключа.