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

КРИПТОГРАФІЯ

Комп’ютерний практикум

Робота № 2

Виконали

студенти гр. ФБ-06,

Зінов'єв Андрій, Даценко Валерія

Київ - 2022

Мета роботи

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

Порядок виконання комп'ютерного практикуму

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 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

Спочатку, уважно прочитали методичні вказівки. Для першого завдання ми підібрали текст російської мови, очистили від непотребу, зберегли у файлі *thetext.txt*

Підібрали ключі розмірами 2,3,…5, 12 та 18 символів > *keys.txt*

Написали код (*lab2.py*) для зашифрування цього ВТ за допомогою даних ключів, що в результаті зберігався окремо у *encrypted_text.txt*

Код складається з декількох функцій:

1. Функція *convert_to_index()* - конвертує текст в індекси за вказаним алфавітом.
2. Функція *convert_to_letter()* - працює навпаки, теж потребує алфавіт.
3. Функція *encode()* - шифрування конвертованого ВТ у ШТ шифром Віженера.
4. Функція *decode()* - дешифрування.
5. Функція *get_blocks()* - розбиття тексту Y на блоки Y_1, Y_2, … Y_r - залежить від періоду r
6. Функція *calculate_index()* - підраховує значення індексу відповідності I(Y) для заданого блоку чи тексту за формулою:
   $I(Y) = (n(n-1))^{-1} \sum_{t \epsilon m} Y(N)(Y(N)-1))$

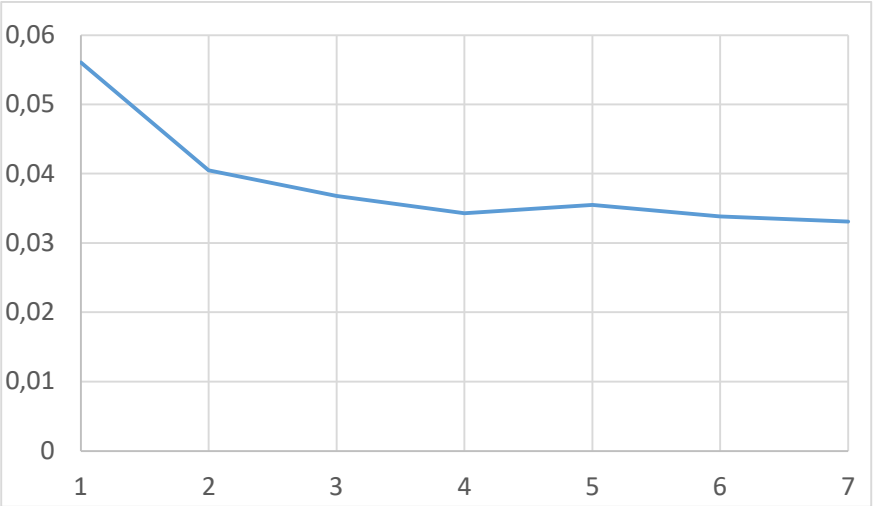
7. Функція *return_approximate_key()* - магічна функція повертає приблизний ключ до нашого шифртексту з завдання 3, маючи довжину ключа.

Завдання 2.

key	r
ум	2
ель	3
азот	4
песня	5
колоссальный	12
сконцентрировать	18

Ключі які використовувались у роботі

key_length	index
PlainText	0,0560459
2	0,0404765
3	0,0368017
4	0,034302
5	0,0354816
12	0,0338449
16	0,0330967



Графік та таблиця залежності індексу відповідності від довжини ключа, 1 - ВТ

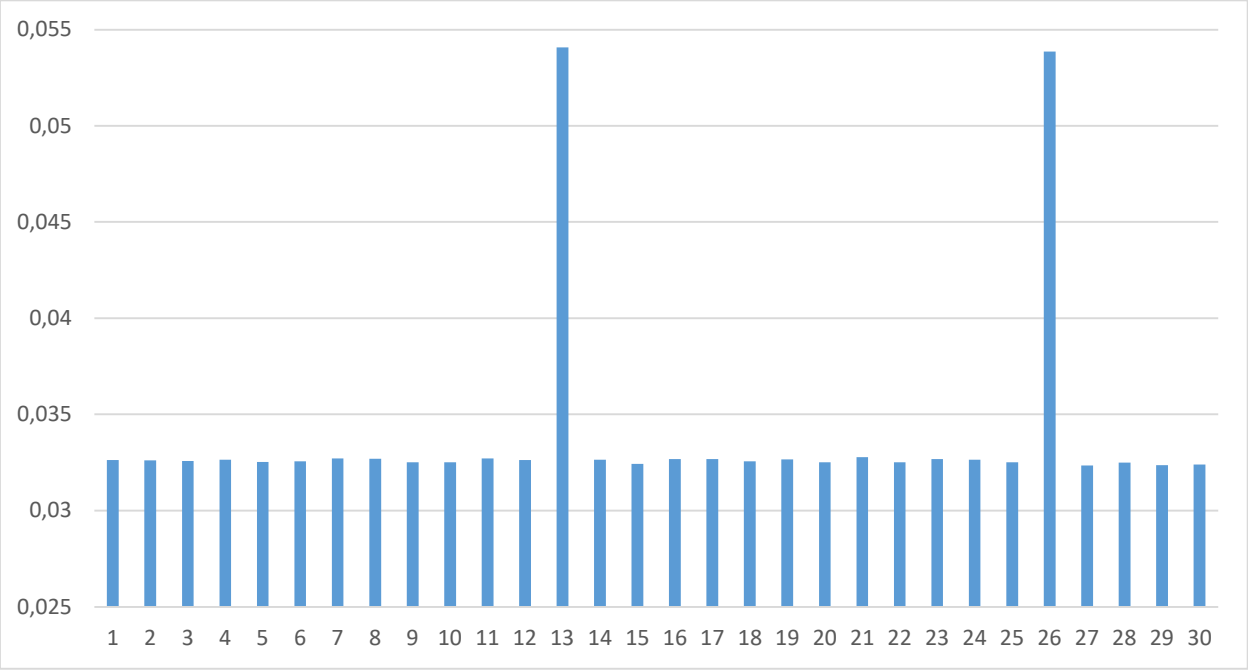
Завдання 3.

Було дано зашифрований текст (у файлі *task3.txt*) за нашим (4-м) варіантом.

Спочатку шукали довжину ключа, за допомогою порівнянь індексів відповідності для різних довжин ключів, у проміжку з 1 до 30. Отримали наступне:

key_length	index
1	0,0326
2	0,0326
3	0,0326
4	0,0327
5	0,0325
6	0,0326
7	0,0327
8	0,0327
9	0,0325
10	0,0325
11	0,0327
12	0,0326
13	0,0541
14	0,0326
15	0,0324

key_length	index
16	0,0327
17	0,0327
18	0,0326
19	0,0327
20	0,0325
21	0,0328
22	0,0325
23	0,0327
24	0,0326
25	0,0325
26	0,0539
27	0,0323
28	0,0325
29	0,0324
30	0,0324



Графік та таблиці I(Y) для різних ключів

На графіку чітко видно, що значення індексу відповідності на ключах 13, 26 значно відрізняються від інших, а значить, скоріш за все маємо роботу з ключем довжиною 13.

Далі всі операції були виконані у функції *return_approximate_key()*: Крок 1 - ділимо текст на блоки за довжиною ключа; Крок 2 - рахуємо кількість повторів літер у кожному з позицій літер для ключа (у проміжку [0:r-1]); Крок 3 - відбувається транспонування результату з кроку 2 (словник з значеннями повторів на позиціях); Крок 4 (фінал) - обчислюємо, граємось з шифром

Цезаря: рухаємо відносно індексу найпопулярнішої букви ("о")(виявляється частотним аналізом), яка є 14-ю у алфавіті, беремо значення за mod32 (32 літери в алфавіті); і нарешті, виводимо конвертований у літери наш ключ.

Отриманий результат не виявився готовим, адже треба ще подумати головою. Проаналізувавши отриманий ключ, спробували декодувати ШТ за допомогою нього, але трішки змінивши його - замінили декілька літер на необхідні, щоб ВТ був читаним.

У результаті отримали ключ - *"ГРОМЫКОВЕДЬМА",* та ВТ: "старминскаяшколачародеевпифийитравницфакультеттеоретическойипрактическоймагиикафедрамаговпрактиковчастьперваясоциальныйукладбытинравывампирьейобщинывикачтовычтотоимеетепротиввампироврасприкорпорациям..." - зміст файлу task3_ decrypted.txt

Висновки:

Ми засвоїли методи частотного криптоаналізу, здобули навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Дізнались про два способи вгадати довжину ключа, та на практиці застосували один. А отже, знайшли ключ та змогли розшифрувати наш шифротекст.