КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконав: Кандила Микита ФБ-12 6 варіант

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

1. Шифрування ВТ

Для шифрування відкритого тексту я використовував перші i-ті символи ВТ, а також наступну формулу:

$$y_i = (x_i + k_{i \bmod r}) \bmod m, i = 0, n$$

де y_i – i-тий символ ШТ; k_i - i-тий символ ключа; r – довжина ключа; m – кількість букв в алфавіті (далі це 32 букви). Реалізація представлена функцією $encode()$.

2. Індекси відповідності

Для знаходження індексів відповідності була використана формула:

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

де n – довжина тексту; $N_t(Y)$ – кількість появ букви t у тексті Y.

Реалізація представлена функціями $reliability\_index()$ і $reliability\_index\_text()$.

Таблиця індексів відповідності

Довжина	2	3	4	5	10	15	20	Відкритий
Індекс	0.0445	0.0393	0.0361	0.0352	0.0331	0.03252	0.0329	0.0532

3. Дешифровка наданого тексту

Для успішної дешифровки я використав підхід описаний в методичних вказівках: знайшов довжину ключа, потім за допомогою частотного аналізу відтворив початковий ключ і, знаючи початковий ключ, розшифрував шифрований текст.

3.1 Знаходження довжини ключа

Оскільки я використовував методичні вказівки, то не бачу сенсу детально розписувати процес реалізації цієї частини дешифровки. Можна лише додати, що для теоретичного значення I, були використані дані з першої лабораторної роботи і формула:

$$MI(Y) = \sum_{t \in Z_m} p_t^2$$

де p_t^2 – частота появи літери в мові.

Реалізація представлена функцією $find\_key\_length()$.

3.2 Знаходження значення ключа

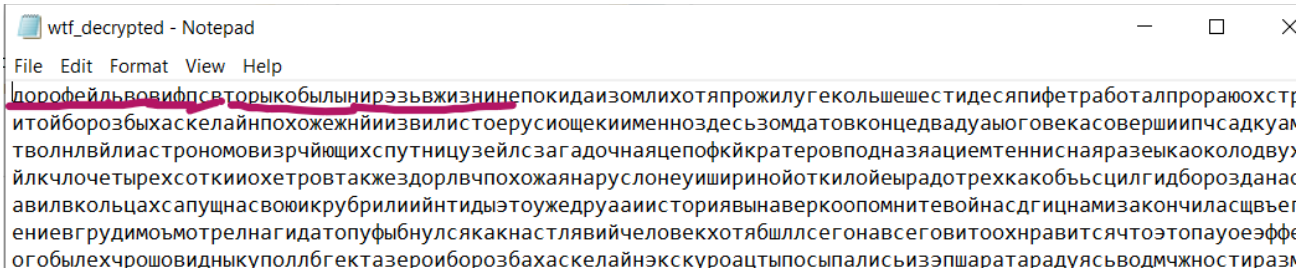
Для визначення ключа весь текст був розбитий на кількість блоків, що рівна довжині ключа (в моєму випадку 17 блоків). Для кожного блока була знайдена найчастіша літера і далі була використана формула:

$$k = (y^* - x^*) \, mod \, m$$

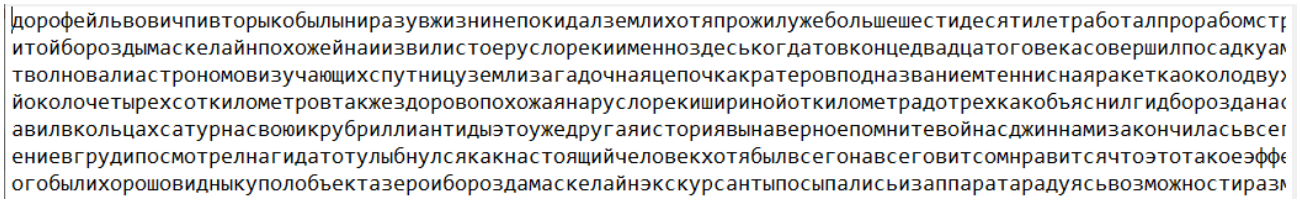
де y^* – буква, що частіше за всіх зустрічається у фрагменті Y_i , а x^*– найімовірніша буква у мові, якою написано відкритий текст (для російської мови це буква «о», для англійської – буква «е» тощо).

3.3 Дешифровка

На минулому етапі був отриманий ключ «возвращениеджлнда». Можна побачити, що частина ключа – це слово «возвращение». Але друге слово не дуже зрозуміло. Спробуємо розкодувати з цим ключем.



Як видно, тільки частина тексту розшифрувалась коректно. В другому блоці можна побачити фразу «нирэзьвжизни». Можна припустити, що це «ниразувжизни». Змінимо наш ключ так (а саме останню букву і перед перед останню), щоб перша фраза перетворилась на другу.
Після легких маніпуляцій отримали ключи «возвращениеджинна». Спробуємо ще раз дешифрувати текст.



Відкритий текст отримано.

Висновок: в даній лабораторній роботі я ознайомився з принципом дії шифру Віженера, а також методиці, яка використовується для криптоаналізу цього алгоритма. Набув практичних навичок з шифрування та розшифрування шифру Віженера.