

Лабораторна робота № 6.

Елементи криптоаналізу.

Завдання роботи:

Знайдіть ключ та розшифруйте текст (мова тексту – англійська). Розрахуйте індекси збігу для повідомлення.

Оберіть текст англійською мовою на економічну тематику без формул та зображень. Видаліть з обраного тексту пробіли та знаки пунктуації. Використовуючи онлайн-калькулятор шифру Віженера (наприклад, <https://planetcalc.com/2468> або <https://cryptii.com/pipes/vigenere-cipher>) на трьох символному ключі зашифруйте своє повідомлення.

Розглянемо задачу викриття шифру за текстом однієї криптограми достатньої довжини.

Нехай μ – довжина ключового слова. Криптоаналіз шифра Віженера здійснюється у два етапи. На першому етапі визначається число μ , а на другому етапі – саме ключове слово.

Для визначення числа μ застосовується тест Казіскі. Тест ґрунтується на простому спостереженні про те, що два однакових відрізки відкритого тексту, що знаходяться один від одного на відстані кратній μ , будуть однаково зашифровані. Через це у шифрі-тексті шукають повторення довжини, яка не менша трьох, та відстань між ними. Випадково такі однакові відрізки можуть з'явитися у тексті з достатньо малою ймовірністю.

Нехай $d_1, d_2, \dots$ – знайдені відстані між повтореннями та d – найбільший спільний дільник цих чисел. Тоді μ має ділити d . Чим більше повторень має текст, тим більш ймовірно, що μ збігається з d . Для уточнення значення μ використовується індекс збігів $I_s(x)$ – ймовірність того, що дві випадково обрані літери у рядку x збігаються.

Нехай $A = \{a_1, \dots, a_n\}$ літерам алфавіту відповідають числа $a_1 \equiv 0, \dots, a_{n-1} \equiv n-2, a_n \equiv n-1$. Індекс збігів обчислюється за формулою:

$$I_s(x) = \frac{\sum_{i=0}^{n-1} f_i \cdot (f_i - 1)}{m \cdot (m - 1)}, \quad (1)$$

де f_i – число входжень літери a_i у рядок x , $i \in Z_n$,

m – довжина рядка x .

Для англomовних текстів індекс збігів $I_s(x) = 0,0662$.

Для знаходження ключового слова будемо використовувати взаємний індекс збігу. Взаємний індекс збігу двох рядків x та y , який позначається $MI_s(x, y)$, називається ймовірність того, що випадково обрана літера з x збігається з випадково обраною літерою y . Цей індекс розраховується за формулою:

$$MI_s(x, y) = \frac{\sum_{i=0}^{n-1} f_i \cdot f'_i}{m \cdot m'}, \quad (2)$$

де f_i – число входжень літери a_i у рядок x , $i \in Z_n$,

f'_i – число входжень літери a_i у рядок y , $i \in Z_n$,

m – довжина рядка x ,

m' – довжина рядка y .

Таблицю значень взаємного індексу збігу для різних значень зсуву s наведено у таблиці 1.

Таблиця 1

Взаємний індекс збігу для значень зсуву s

Зсув s	0	1	2	3	4	5	6
$MI_s(x, y)$	0,066	0,039	0,032	0,034	0,044	0,033	0,036
Зсув s	7	8	9	10	11	12	13
$MI_s(x, y)$	0,039	0,034	0,034	0,038	0,045	0,039	0,043

Для зашифрованого тексту застосуйте тест Казіскі та визначте кількість літер у ключовому слові. Розрахуйте взаємні індекси збігів $I_z(x)$ літер для кожного зі стовпців таблиці, для достовірного визначення довжини ключового слова. Потім виконайте пошук його істинного значення, використовуючи взаємний індекс збігів $MI_z(x, y)$.