

ЛАБОРАТОРНА РОБОТА № 2

ТЕМА: МЕТОД ШИФРУВАННЯ ДАНИХ «ШИФР ТРИТЕМІУСА».

МЕТА: ОЗНАЙОМИТИСЬ З МЕТОДОМ ШИФРУВАННЯ ДАНИХ «ШИФР ТРИТЕМІУСА» І НАДАТИ ЙОГО ПРОГРАМНУ РЕАЛІЗАЦІЮ

ТЕОРЕТИЧНІ ВІДОМОСТІ

Порушити статистичні залежності в закодованих повідомленнях і тим самим підвищити надійність кодування можна за допомогою шифру Тритеміуса.

Алгоритм шифрування:

1. Визначаємо код букви в алфавіті.
2. Обчислюємо крок зміщення k .
3. Знаходимо код зашифрованою літери, користуючись наступним рівнянням:
$$L = (m + k) \bmod N,$$
де L - код зашифрованої букви; m - код букви, яка шифрується; k - крок зміщення; N - число букв алфавіту.
4. За кодом L відновлюємо букву криптограми.
5. Повторюємо пункти 1-5 до закінчення тексту шифрограми.

Алгоритм розшифрування:

1. Визначаємо код букви в алфавіті.
2. Обчислюємо крок зміщення k .
3. Знаходимо код розшифрованої літери, користуючись наступним рівнянням:
$$m = (L - k) \bmod N,$$
де L - код зашифрованої букви; m - код розшифрованої букви; k - крок зміщення; N - число букв алфавіту.
4. За кодом m відновлюємо чергову букву криптограми.
5. Повторюємо пункти 1-5 до закінчення тексту криптограми.

В алгоритмах шифрування і розшифрування крок зміщення k може задаватись різними способами:

- За допомогою лінійного рівняння, наприклад, $k=3t+1$.
- За допомогою нелінійного рівняння, наприклад, $k=8t^2+4t+9$.
- За допомогою використання гасла – текстового рядка, який багаторазово записується під текстом повідомлення (криптограми); крок зміщення в цьому випадку визначається номером в алфавіті відповідної букви гасла.

Тут t позначає порядковий номер букви в повідомленні (криптограмі).

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Ознайомитись з методом шифрування даних «Шифр Тритеміуса».

2. Побудувати блок-схему алгоритму шифрування.
3. Написати програму для шифрування та розшифрування за допомогою метода «Шифр Тритеміуса», передбачивши в ній можливості вибору:
 - a. Файлу.
 - b. Алфавіту (наприклад, англійський та український).
 - c. Способу визначення кроку зміщення.
4. Підготувати звіт про виконання роботи. Звіт оформлюється у вигляді документу Word з такою структурою: титульний лист, тема і мета роботи, блок-схема алгоритму методу, програмний код.
5. Електронну копію звіту відправити за адресою: George@aprodos.kpi.ua.