

Autor	Michał Skiba
Nr albumu	256459
Temat	Szyfrowanie ROT13
Data	28 Marca 2021

1. Wytlumaczenie algorytmu szyfrowania ROT13

Szyfrowanie ROT13 polega na zamianie każdej litery na literę trzynastą po niej w alfabecie. Przyjmuje się, że literą następną po literze 'z' jest litera 'a', następuje więc zapętlenie.

Algorytm działa zatem w następujący sposób. Jeżeli wartość kodu ASCII znajduje się pomiędzy 65, a 90 (duża litera) lub pomiędzy 97, a 122 (mała litera) dodaj 13 do wartości kodu ASCII danej litery. Jeżeli po dodaniu wartość przekroczyła 90 (dla dużej litery) lub 122 (dla małej litery) należy odjąć 26, ponieważ alfabet ma 26 liter, więc będzie to modulo 26 z nadmiaru jaki wystąpił. Następnie w słowie podmieniamy starą wartość kodu ASCII, nową wartością zaszyfrowaną.

2. Implementacja algorytmu

Algorytm był prosty w zaimplementowaniu za pomocą podstawowych rozkazów `cmp`, `je`, `jl`, `jg`, `jmp`, `mov`. Jedyny moment nad którym musiałem się zastanowić było kopiowanie wartości kodu ASCII 8 bitowego pojedynczego znaku do akumulatora `ax` 16 bitowego, ponieważ musiałem użyć rozkazu `movzx`, który wyzerowuje starsze 8 bitów akumulatora. Zapis wartości kodu ASCII do akumulatora o większym rozmiarze był spowodowany tym, że po dodaniu 13 mógł wystąpić nadmiar i wartość po dodaniu została by utracona. Oczywiście opcją byłoby wykrywanie nadmiaru, lecz uznałem mój sposób za łatwiejszy w implementacji. Następnie przy kopiowaniu wartości z powrotem do słowa, już po ewentualnym zmniejszeniu wartości kodu ASCII wykraczającej poza zakres kopiujemy tylko młodsze 8 bitów akumulatora `ax`, czyli akumulator `al`.

3. Działanie programu

Algorytm pobiera ciąg znaków, maksymalnie 100 bajtów, następnie jest przetwarzany przez algorytm szyfrujący ROT13 i na koniec zostaje wyświetlone zaszyfrowane słowo.

4. Wnioski

Po moich testach stwierdzam, że program działa zgodnie z założeniem.