Autor: Mateusz Krupa

Nr indeksu: 256280

Sprawozdanie

Organizacja i Architektura Komputerów

1. Opis zadania do wykonania

Do wykonania na laboratoria był szyfr Cezara(ROT13).

Szyfr Cezara jest to rodzaj szyfru podstawieniowego, w którym każda litera tekstu jawnego (niezaszyfrowanego) zastępowana jest inną, oddaloną od niej o stałą liczbę pozycji w alfabecie, literą (szyfr monoalfabetyczny), przy czym kierunek zamiany musi być zachowany.

Program należało napisać w języku assemblera w architekturze 32-bitowej na platformę Linux.

Założenia:

- maksymalna wielkość bufora na zdanie wpisane przez użytkownika to 100 znaków
- ROT13 powinien poprawnie zamieniać wielkie litery na wielkie a małe na małe
- Wszystko co nie jest literą alfabetu łacińskiego pozostaje bez zmian, np żółć pozostaje takie samo po zaszyfrowaniu ROT13

2. Opis wykonania

Program który napisałem w assemblerze nie jest najoptymalniejszy co do kryteriów wyznaczonych, ponieważ moje szyfrowanie polega na tym że 13 jest dodawane do każdego znaku, jest dodawane na samym początku. Podczas pisania programu stwierdziłem, że w ten sposób lepiej zapoznam się z assemblerem ponieważ to dodania na początek powoduje, że powstaje więcej warunków do spełnienia aby poprawnie zaszyfrować wiadomość. Występują tam dwie rodzaje korekty jedna -13 która jest użyta do przypadków kiedy znak nie był ani duża ani mała literą i aby szyfr działał poprawnie musze wrócić do stanu początkowego. Drugi rodzaj korekty to -26, korekta ta jest dla małych i dużych liter które to po dodaniu 13 wykraczają poza małe i duże litery czyli np. z,U. Dodanie 13 na początku nie potraktowałem jako błędną ścieżkę ponieważ uważałem to jako rozbudowanie tego co mieliśmy zrobić. Wszystko działa w pętli w której użyłem rozszerzonych rejestrów r8d i r9d.

3. Wnioski

Podczas laboratorium nauczyłem się działania pętli. Początkowo pętla sprawiała mi dużo problemów, nie byłem w stanie ani jej napisać ani sprawić by działała jak zamierzałem. Trudność sprawiło mi dodatkowo to, że dodałem na samym początku 13, przez to, że nie jestem jeszcze przyzwyczajony do składni assemblera nie było mi tak łatwo odnaleźć się w kodzie i te wszystkie korekty które musiałem stosować na początku nie działały jak powinny.