Bezpieczeństwo
Laboratorium 4
Łamanie kodu

Mateusz Mańka

1. Zadanie : znalezienie swojego hasło

Zadanie polegało na znalezieniu hasła do swojego indeksu.
Należało zatrzymać się gdb w miejscu po funkcji generatekey i odczytać hasło.

Dla mojego nr indeksu 209895 hasło to :
xelszgnubipwdkryfmtahovcjqxgpyhqzirajsbktcludmvenwfo

2. Zadanie : Przeanalizować działanie

Funkcja generateKey na początku zmieniała wprowadzony string na int jeżeli się nieudało brana byłą wartość losowa.
Następnie funkcja brała nr indeksu modulo 26 . Ponieważ indeks był zapisywany w eax a funkcja dzielenia ustawiała tam swoją wartość traciliśmy nr indeksu .

Po dalszym analizowaniu funkcji mogliśmy dojść do wniosku że hasło składa się z dwóch sekcji 26 znakowych gdzie każda sekcja byłą generowana w podobnej pęteli. Pętla ta brała string ‘abcdefghijklmnoprstuwxyz’ i zaczynając od indeks modulo 26 skakało co 7 w pierwszej sekcji i co 9 w drugiej.

3. Zadanie : Napisanie własnego generatora

Wlasny generator na podstawie analizy z punktu 2 napisany został w języku JAVA i znajduje się w folderze Keygen