|  |  |
| --- | --- |
| **Politechnika Białostocka**  **Wydział Informatyki** | Data: 12.10.2016 |
| **Przedmiot:** Techniki zapewniania poufności w Internecie.  **Sprawozdanie nr:** 1  **Temat:** JEDNOKIERUNKOWE FUNKCJE HASHUJĄCE. ALGORYTM SHA-1.  **Autor:** Maciej Ziniewicz  **Studia:** stacjonarne II stopnia, semestr 2 | **Prowadzący:**  prof. dr hab. Vyacheslav Yarmolik  Ocena: |

Spis treści

[1. Treść zadania 1](#_Toc463707536)

[2. Część teoretyczna 1](#_Toc463707537)

[3. Rozwiązanie 1](#_Toc463707538)

[4. Podsumowanie 1](#_Toc463707539)

# Treść zadania

Wykonaj oprogramowanie realizuja˛ce hashowanie algorytmem SHA-1 wybranego pliku.

# Część teoretyczna

SHA-1 (Secure Hash Algorithm) jest jednokierunkową funkcją hashującą wytwarzającą skrót o długości 160 bitów z wiadomości o dowolnym rozmiarze, nie większym niż -bitów. Funkcja SHA-1 jest oparta na zasadach podobnych, do użytych przy projektowaniu funkcji hashujących MD4 i MD5, i w znacznym stopniu naśladuje te algorytmy.

Początkowo wiadomość jest uzupełniana o podobnie jak w MD5 czyli dołączany jest bit o wartości 1 na końcu wiadomości, następnie ciąg uzupełnia się w taki sposób by składał się z 512-bitowych bloków, a ostatni blok był niepełny i miał dokładnie 448 bitów. Na koniec ostatniego bloku dodawana jest 64-bitowa wartość oznaczająca rozmiar wiadomości przed modyfikacjami. Po dodaniu rozmiaru ostatni blok równiez będzie miał 512 bitów. Następnie wykonywana jest głowna pętla algorytmu tyle razy ile jest 512 bitowych bloków.

Każdy blok jest 512 bitowy i taki pojedynczy blok jest przetwarzany w głownej pętli. 512 bit daje 16 – 32 bitowych wartości(słowa od M0 do M15) , które są przekształcane w 80 – 32 bitowych wartości (od W0 do W79) w taki sposób że pierwsze 16 jest przepisywanych tak jak we wzorze :

Z kolei pozostałe od indeksu 16 do 79 są określone wzorem:

Kolejnym etapem jest przepisane stałych które należało wcześniej zdefiniować:

A = 0x67452301

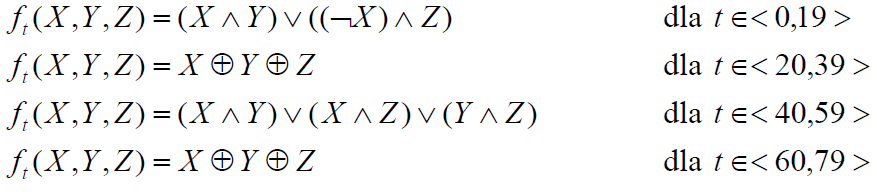
B = 0xefcdab89

C = 0x98badcfe

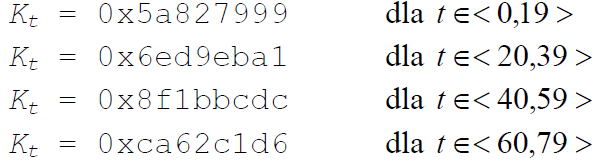
D = 0x10325476

E = 0xc3d2e1f0

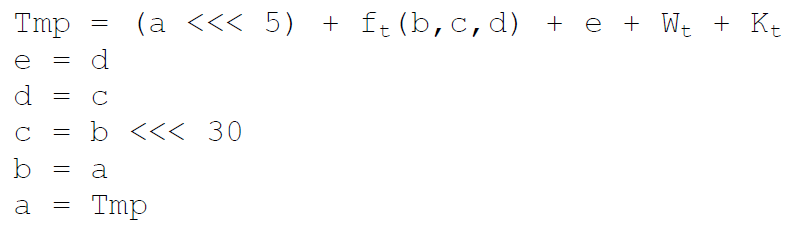
Przepisać przykładowo na a,b,c,d,e. Na tych przepisanych stałych będą wykonywane operacje pętli. Kolejnym etapem jest wykonanie nieliniowych funkcji, wykonywane są na określony zakres indeksów z wcześniej utworzonych osiemdzieśięciu 32 bitowych wartości.



W algorytmie zdefiniowane są też stałe, również przyporządkowane do indeksów.



Mając te zakresy można przystąpic do głownej pętli algorytmu która wykonuje się dla każdego 32bitowego podbloku o indeksie 0-79. Wedle zakresów podanych powyżej oraz dla każdego przejścia wykonywane są dodatkowo następujące operacje



# Rozwiązanie

# Podsumowanie