Sprawozdanie z Laboratorium 3 – Funkcje Skrótu

1. Szybkość szyfrowania dla plików .txt o wielkości 1MB, 5MB oraz 10MB
2. Procent zmienionych bitów w wiadomości w momencie zmiany pierwszego bitu

Do utworzenia funkcji skrótu użyty został algorytm SHA3-512.  
Bity wejściowe: 00111000  
Zliczone jedynki po operacji XOR na bitach wejściowych i bitach po transformacji: 251  
Procent zmian: 49.0234375%

1. Znalezienie kolizji na pierwszych 12, 20 oraz 50 bitach

Szukamy kolizji dla liczby: 50  
Algorytm funkcji skrótu: MD5

|  |  |  |  |
| --- | --- | --- | --- |
|  | 12 bitów | 20 bitów | 50 bitów |
| 1 000 iteracji | 0 | 0 | 0 |
| 10 000 iteracji | 2 | 0 | 0 |
| 1 000 000 iteracji | 249 | 2 | 0 |
| 10 000 000 iteracji | 2442 | 13 | 0 |
| 1 000 000 000 iteracji | 245027 | 951 | 0 |

Szukanie kolizji polegało na losowym wygenerowaniu 160 bitów (random.getrandbits(160)) w każdej iteracji i sprawdzenie czy pierwsze 12, 20 oraz 50 bitów jest takie samo jak dla podanej przez nasz liczby