Funkcje Skrótów

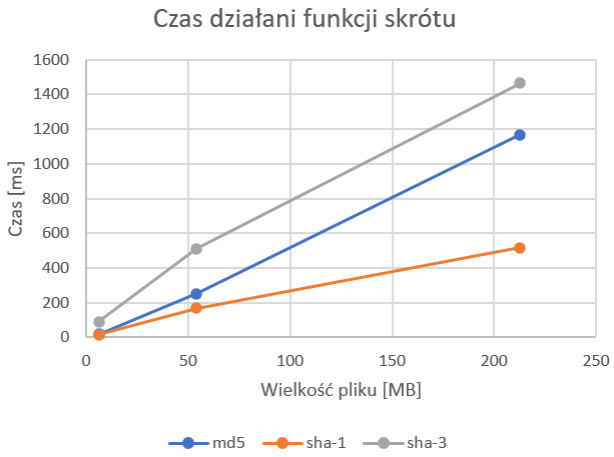
Autor: *Mateusz Oleszek*, nr. 144608

Wybrane funkcje do testowania: MD5, SHA-1, SHA-3

Skrót za pomocą różnych algorytmów

```
PS F:\Programowanie\Studia\KryptoLab\Hashing\bin\Debug\net7.0> .\Hashing.exe "przykladowa wartosc do skrocenia"
Hashed value: przykladowa wartosc do skrocenia
MD5:   6EC6BA6A6FA33C85466CB0A30928714E
SHA-1: ABCA1D57F1D0E2AD2BA6BEDA02C69B34229023CE
SHA-3: ECE947FE1B19A2CAC0C0ED31A9594DDD1113A77286AE3C3CD60B7F3D1AE12A202BC7DA60ACE0021CC35F0A0F72C89BC9
```

Szybkość działania

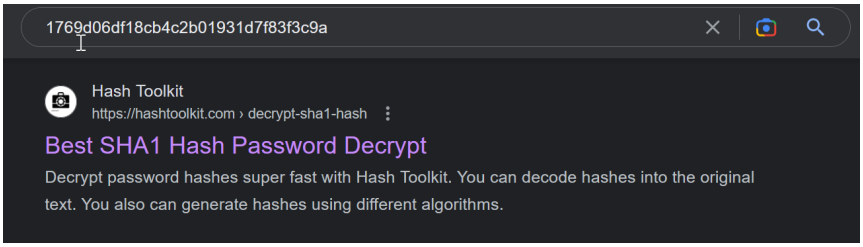


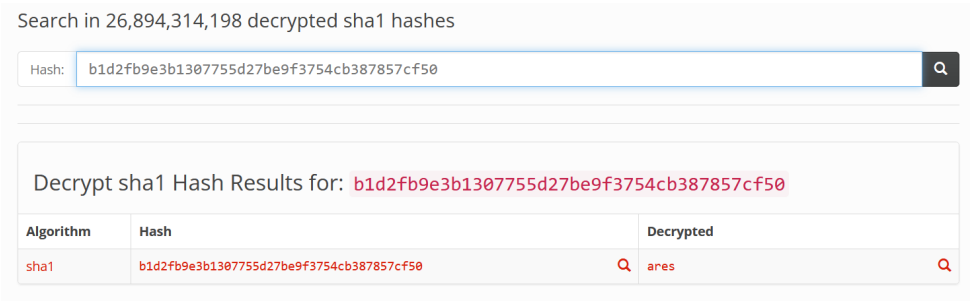
Najszybsza jest funkcja SHA-1, potem MD5, a na końcu SHA-3.

Funkcja MD5 dla krótkiego słowa

Skrót MD5 dla słowa wejściowego "ares": 1769d06df18cb4c2b01931d7f83f3c9a

Wyniki po wyszukaniu tego skrótu w google





Czy funkcja skrótu nie jest bezpieczna

Funkcja MD5 jest powszechnie uznawana za złamaną kryptograficznie i nienadającą się do użytkowania od kilkunastu lat. Konsumenckie karty graficzne potrafią generować miliony skrótów na sekundę.

Zostały też znalezione ciągi które posiadają ten sam skrót, a co więcej nawet algorytm pozwalający stworzyć 2 pliki o dowolnej długości które będą miały ten sam skrót.

Znajdowanie kolizji na pierwszych bitach

Dla funkcji skrótów wygenerowanych z **miliona** losowych ciągów znaków kolizje były znalezione na pierwszych **40 bitach**. Im więcej skrótów było generowanych tym można było znaleźć kolizję dla większej liczby bitów, np. dla tysiąca było to tylko pierwsze 19 bitów. Tak więc dla większych zbiorów skrótów będzie można znaleźć coraz bardziej podobne skróty z większym prawdopodobieństwem.

Kryterium SAC

Zostały przetestowane milion losowych ciągów znaków, w których został zmieniony jeden bit a potem porównane bity skrótów oryginalnej i zmienionej wartości. Zaobserwowane procenty zmienionych bitów pomiędzy nimi to:

- Min: ~29%
- Max: ~72%
- Średnia: 50.001%

Patrząc na średnią wartość będącą prawie dokładnie 50% można uznać, że ten algorytm spełnia kryterium SAC.