3.04.2024r.

Piotr Suchodolski

Sprawozdanie - Funkcja skrótu

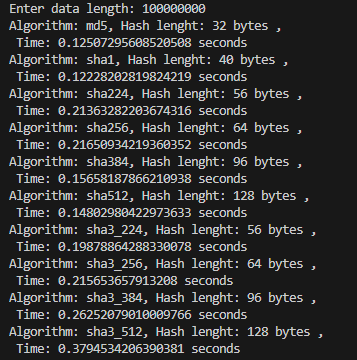
Zadanie 1

Kodowanie podanymi algorytmami zostało zrealizowane za pomocą biblioteki hashlib. Następnie są one konwertowane z binarnych na heksadecymalne aby uprościć na nich pewne obliczenia.  
 Kryterium SAC jest obliczane na podstawie wpisanej na stałe wiadomości, która jest taka sama dla wszystkich algorytmów. Po kolei zmieniane są jej bity po czym jest obliczana ilość zmienionych bitów hashu. Jeśli różnica ta zawiera się w pomiędzy 46-54% jest ono spełnione.  
 Kolizje w algorytmie MD5 są sprawdzane dla podanej ilości haseł, które są następnie generowane losowo. Wszystkie hasła są o tej samej, podanej długości. Następnie sprawdzane są takie same kombinacje dla hashy na kolejno 12, 20, 50, 100 pierwszych bitach.

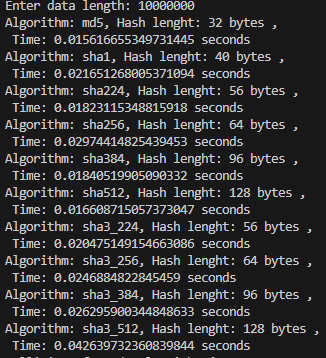
Zadanie 2

Porównanie szybkości działania oraz długości hashy dla wszystkich testowanych algorytmow przy szyfrowaniu losowego ciągu znaków o podanej długości.

Dla długości 100 000 000:



Dla długości 10 000 000:



Zadanie 3

Hash wygenerowany przez algorytm MD5 dla 4 znakowego, losowego ciągu znaków



Po sprawdzeniu wartości hashu w internetowych tablicach hashy udało się znaleźć oryginalne hasło: KqNc. Można z tego wyciągnąć wniosek, że szyfrowanie krótkich haseł, może okazać się nieskuteczne ponieważ są one stablicowane w powszechnie dostępnych źródłach.

Zadanie 4

Funkcja MD5 nie jest uznawana juz za bezpieczna, ponieważ udało się znaleźć wiele kolizji dla tej funkcji skrótu. Jest ona używana do sprawdzania integralności plików, ale nie do haszowania haseł. Rekomendowane jest używanie nowszych i bezpieczniejszych algorytmów takich jak SHA-256 czy SHA-512.

Zadanie 5

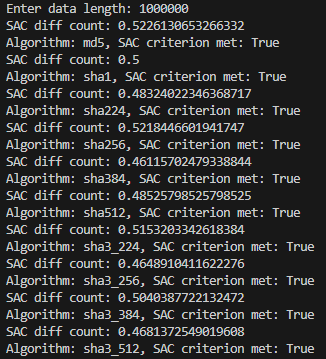
Badanie kolizji dla algorytmu MD5. Test został przeprowadzony dla 10000 losowych ciagów znaków o długości 10 bajtów każdy. Kolizje zostały dodatkowo sprawdzone na różnych poziomach długości hashy wynikowych: od 12 do 100 pierwszych bitów.



Ilość kolizji na poziomie około 30%.

Zadanie 6

Zbadanie wartości kryterium SAC dla wszystkich badanych algorytmów:



Wypisana dodatkowo została wartość SAC, która reprezentuje procentowo ile bitów zmieniło się w hashu po zmianie 1 bitu w hashowanym haśle.

Zadanie 7

Rola soli w tworzeniu skrótów. Sól jest dodawana do hashowanych haseł aby zapewnić ich lepsze zabezpieczenie. Daje ona większą gwarancję, że hasła nie będzie się dało odczytać z tablic hashy. Nawet jeśli dwa razy poddamy hashowaniu tą samą tajemnicę, dzięki użyciu soli, będzie ona reprezentowana przez zupełnie inną wartość.