Miłosz Sobol 155905 Funkcje skrótu

1. Zestawienie zależności czasu potrzebnego na wykonanie funkcji skrótu do wielkości przetwarzanego pliku.

A graph of a graph

AI-generated content may be incorrect.

Widoczny jest liniowy wzrost czasu zależnego od wielkości pliku przyjmowanego na wejście funkcji. Czasy te, mimo sporej wielkości plików, są bardzo niskie, świadczy to o niskiej złożoności obliczeniowej haszowania. Jest to zarówno plus jak i minus, niska złożoność obliczeniowa pozwala na stosunkowo szybkie przeprowadzanie ataków takich jak „atak urodzinowy” polegający na znalezieniu kolizji funkcji haszującej.

A screenshot of a graph

AI-generated content may be incorrect.

Na przedstawionych na poprzedniej stronie wykresach możemy zaobserwować pewną rozbieżność. Haszowanie za pomocą funkcji skrótu MD5 zajmuje niemalże tyle samo czasu co za pomocą SHA384. Owa rozbieżność najprawdopodobniej wynika z specyfikacji implementacji funkcji MD5 w Pythonowej bibliotece „hashlib” (<https://stackoverflow.com/questions/59955854/what-is-md5-md5-and-why-is-hashlib-md5-so-much-slower>).

1. Test SAC

A screen shot of a computer

AI-generated content may be incorrect.

Test został parokrotnie przeprowadzony dla plików o różnych rozmiarach (Na obrazku widoczny wynik dla pliku o wielkości 150MB oraz funkcji haszującej SHA384). Za każdym razem wynik oscylował w okolicach wartości 0.5.

1. Test kolizji

A screenshot of a computer program

AI-generated content may be incorrect.

Mimo wykorzystania funkcji haszującej MD5, test charakteryzował się zupełnym brakiem kolizji dla stringa o długości 3 znaków. Poniżej widoczne wyniki dla kolejno, słowa „k” oraz słowa „ko”.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.