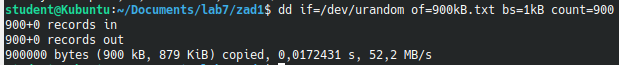
Sprawozdanie

LABORATORIUM 5. SKRÓTY KRYPTOGRAFICZNE.

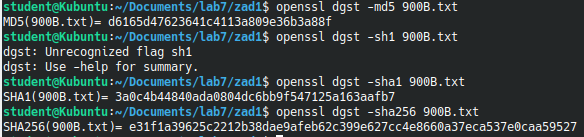
# Zadanie 5.1. Wykorzystanie algorytmów nieodwracalnej funkcji skrótu go generowania skrótu wiadomości

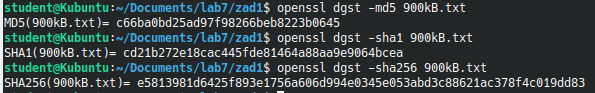
## P.5.1. Dla każdego z tych plików oblicz wartość funkcji skrótu za pomocą trzech wybranych algorytmów wykorzystując funkcjonalność openssl. Omów i porównaj otrzymane skróty wiadomości.

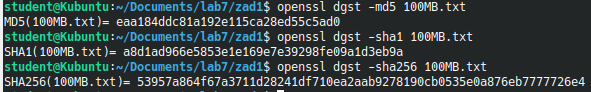










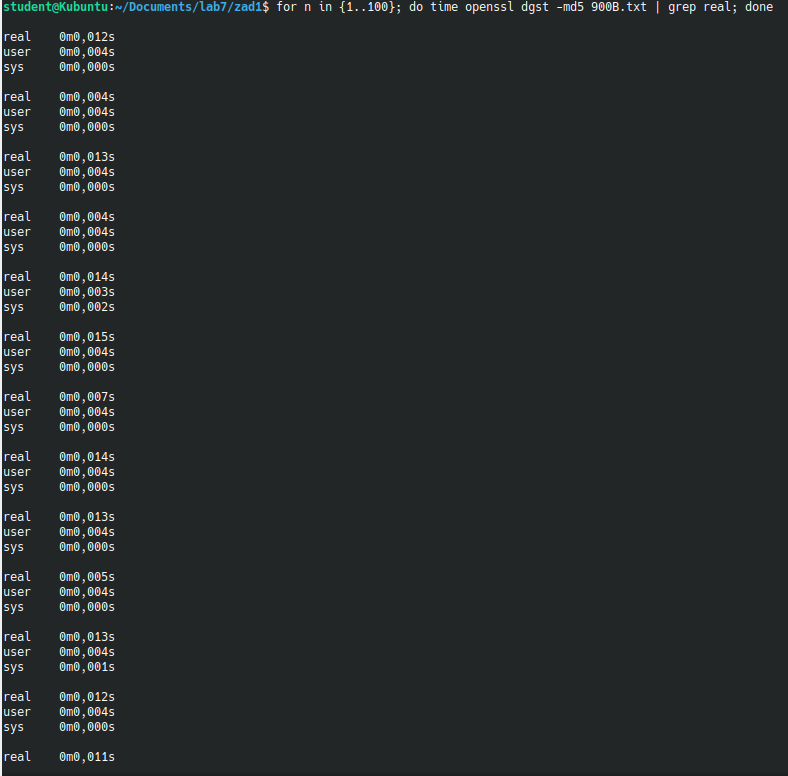


Algorytm sha256 jest najbezpieczniejszy, gdyż używa najdłuższej wartości skrótu.

## P.5.2. Określ średni czas przetworzenia 1MB danych dla każdej z kombinacji: rozmiar pliku – algorytm obliczenia skrótu. W celu określenia czasu wykonania polecenia skorzystaj z systemowego polecenia "time". Jako wynik zapisz sumy czasów user+sys. Wynik należy zapisać, jako średnia z minimum 100 pomiarów. Otrzymane wyniki umieścić w tabeli, a następnie sporządzić wykresy dla zastosowanych algorytmów. Przykładowe polecenie do wykonania 100 pomiarów.

Dla pliku 900B.txt:

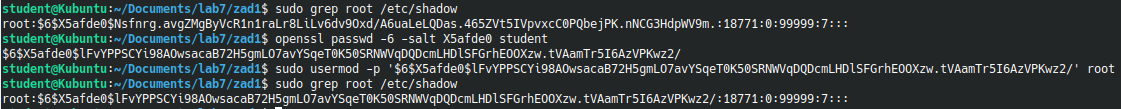
Średni czas MD5: 0,00557s



Średni czas SHA1: 0,00583s

Średni czas SHA256: 0,00646s

# Zadanie 5.2. Funkcje skrótu a bezpieczeństwo przechowywanych haseł



## P.5.3. Jakie zmiany zauważyłeś w pliku shadow? Zaloguj się na konta root lub student. Jakiego hasła użyłeś? Udokumentuj wykonanie ćwiczenia. Omów wykonane ćwiczenie i jego efekty. Czy dana metoda zmiany hasła jest bezpieczna? Jeśli nie zaproponuj zmiany i wyjaśnij dlaczego.

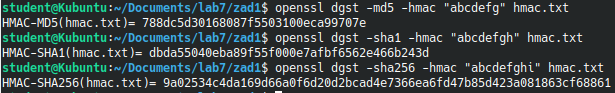
Do pliku shadow wprowadziliśmy nowe hasło dla roota. Metoda dobrze szyfruje hasło, więc jest bezpieczna jeżeli osoba trzecia nie widzi naszej konsoli.

# Zadanie 5.3. Keyed Hash oraz HMAC

Tworzenie pliku:



Algorytm:



## P.5.4. Czy w algorytmie HMAC konieczne jest używanie kluczy o stałej długości?

Nie, klucze mogą być różnej długości.