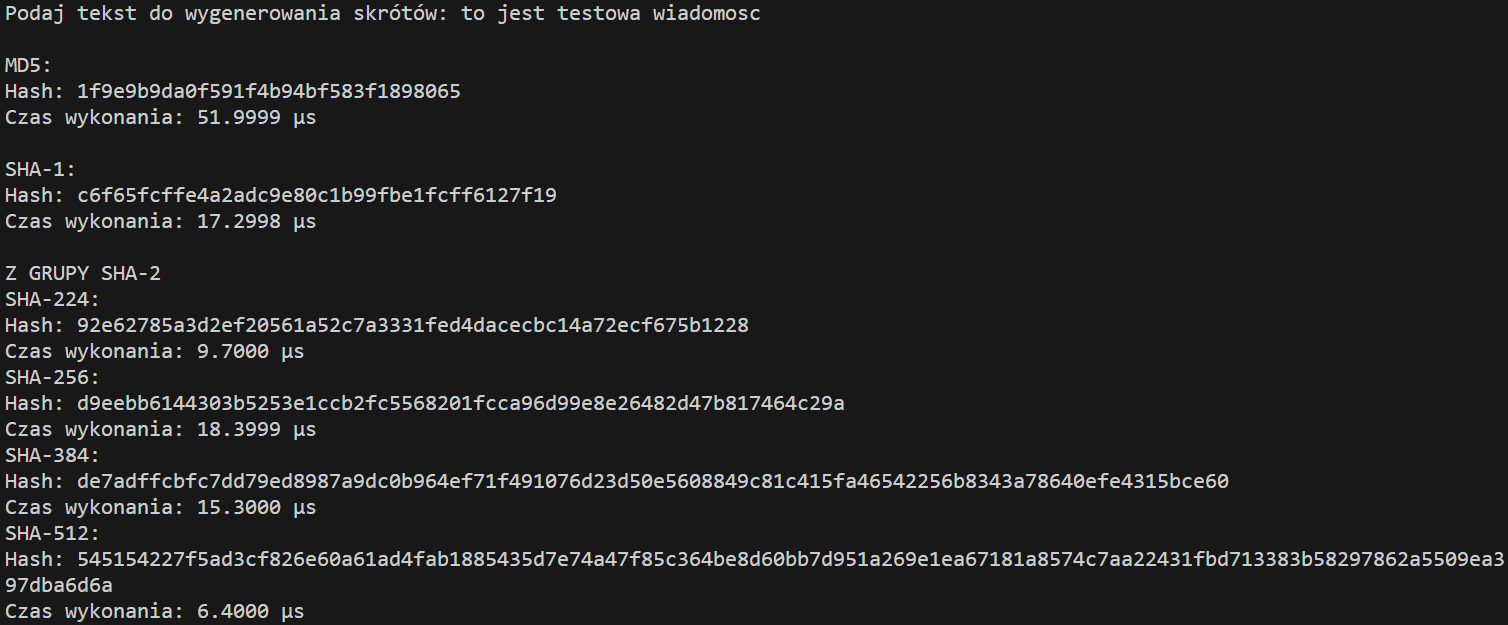
Sprawozdanie  
Funkcje skrótu

Mikołaj Pluta 151827

1 Screenshot.

2. Omówienie sposobu implementacji.

Aplikacja to prosty skrypt korzystający z funkcji skrótów dostępnych w środowisku Python. Dla każdej z badanych funkcji mierzy czas jej wykonania. Tekst wejściowy podawany jest przez użytkownika, program wyświetla wynik hashowania i czas operacji dla każdej z funkcji.

3. Określenie roli soli w tworzeniu skrótów.

Sól w tworzeniu skrótów to losowa wartość dodawana do haseł przed ich zaszyfrowaniem, co zapobiega atakom typu słownikowego i bruteforce poprzez zapewnienie unikalności skrótów nawet dla tych samych haseł. Dodanie soli zwiększa bezpieczeństwo haseł, szczególnie tych o niskiej entropii, poprzez zwiększenie ich losowości i utrudnienie ich złamania.

4. Czy funkcję MD5 można uznać za bezpieczną? Czy dotychczas zostały znalezione dla niej jakiekolwiek kolizje?

Funkcję MD5 nie można uznać za bezpieczną w kontekście zastosowań kryptograficznych ze względu na udokumentowane podatności. Wiele badań wykazało, że jest ona podatna na kolizje, co oznacza, że istnieją dwie różne wiadomości, które generują ten sam skrót MD5. Ataki takie są wykonywalne w praktyce, co znacząco osłabia bezpieczeństwo funkcji MD5.

Dla przykładu, poniższe dwa obrazy mają taki sam hash MD5



5. Wnioski i podsumowanie.

Analiza naszego eksperymentu z funkcjami skrótu ukazuje ich różnorodność i znaczenie dla bezpieczeństwa danych. Testowanie różnych wariantów funkcji, takich jak MD5, SHA-1, SHA-2 i SHA-3, pozwoliło na zrozumienie ich własności i potencjalnych zagrożeń. Wnioskiem jest, że wybór odpowiedniej funkcji skrótu powinien być starannie przemyślany z uwzględnieniem poziomu bezpieczeństwa, wydajności i zastosowania danego systemu.

Początek formularza