Sprawozdanie

Funkcje skrótu

Mikołaj Pluta 151827

1 Screenshot.

```
Podaj tekst do wygenerowania skrótów: to jest testowa wiadomosc

MD5:
Hash: 1f9e9b9da0f591f4b94bf583f1898065
Czas wykonania: 51.9999 µs

SHA-1:
Hash: c6f65fcffe4a2adc9e80c1b99fbe1fcff6127f19
Czas wykonania: 17.2998 µs

Z GRUPY SHA-2
SHA-224:
Hash: 92e62785a3d2ef20561a52c7a3331fed4dacecbc14a72ecf675b1228
Czas wykonania: 9.7000 µs
SHA-256:
Hash: d9eebb6144303b5253e1ccb2fc5568201fcca96d99e8e26482d47b817464c29a
Czas wykonania: 18.3999 µs
SHA-384:
Hash: de7adffcbfc7dd79ed8987a9dc0b964ef71f491076d23d50e5608849c81c415fa46542256b8343a78640efe4315bce60
Czas wykonania: 15.3000 µs
SHA-512:
Hash: 545154227f5ad3cf826e60a61ad4fab1885435d7e74a47f85c364be8d60bb7d951a269e1ea67181a8574c7aa22431fbd713383b58297862a5509ea3
97dba6d6a
Czas wykonania: 6.4000 µs
```

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.