Funkcje skrótu

Katarzyna Jaromirska 155910

# Screenshot z aplikacji:



# Omówienie sposobu implementacji

Wykorzystana została biblioteka java.security do hashowania wiadomości. Program bierze bajty z wiadomości, a następnie przepuszcza przez instancję danej funkcji skrótu. Wiadomość może być pobrana z konsoli lub z pliku ”hash\_input.txt”. W konsoli wyświetlana jest zhashowana wiadomość w dostępnych funkcjach, tj.: MD5, SHA-1, rodzina SHA-2 oraz rodzina SHA3.

# Rola soli w tworzeniu skrótów

Sól w kryptografii to losowe dane dodawane do hasła. Hashowanie z użyciem soli pomaga w zapobieganiu przed atakami z użyciem tablic tęczowych (baza skrótów używana do łamania zahashowanych haseł). Sprawia również, że dwa takie same hasła będą miały różne wyjście po zahashowaniu.

# Czy funkcja MD5 jest bezpieczna? Czy znaleziono kolizje?

Funkcja MD5 nie jest bezpieczna. Jest uznawana za kryptograficznie złamaną funkcję hashującą. Kolizje zostały już znalezione w 2004 przez chińskich naukowców. Można stworzyć z różnych wiadomości M taki sam skrót H(M).

# Wyniki pomiaru czasu funkcji skrótu

Najszybszą funkcją skrótu jest funkcja MD5. Im dłuższa ilość znaków, tym dłuższy czas przetwarzania.

| \*\*Funkcja\*\* | \*\*Ilość znaków\*\* | \*\*Czas (ns)\*\* |  
|:-----------:|:----------------:|:----------------------------:|  
| MD5 | 32 | 9783,872 ± 157,788 ns/op |  
| SHA-1 | 40 | 11018,111 ± 699,964 ns/op |  
| SHA-224 | 56 | 15082,798 ± 3848,182 ns/op |  
| SHA-256 | 64 | 16700,877 ± 3332,223 ns/op |  
| SHA-384 | 96 | 25973,673 ± 285,811 ns/op |  
| SHA-512 | 128 | 32587,728 ± 328,029 ns/op |  
| SHA-512/224 | 56 | 18090,603 ± 246,513 ns/op |  
| SHA-512/256 | 64 | 17954,568 ± 317,539 ns/op |  
| SHA3-224 | 56 | 21269,212 ± 184,617 ns/op |  
| SHA3-256 | 64 | 22495,650 ± 2774,016 ns/op |  
| SHA3-384 | 96 | 33306,211 ± 1248,769 ns/op |  
| SHA3-512 | 128 | 49332,271 ± 11358,554 ns/op |