

Laboratorium 3 – Funkcje Skrótu

1. Screenshot z aplikacji

```
Kot
MD5 time: 21100 ns - result - c0d03d2d3e717da54ffdfc8a76c0f089
SHA-1 time: 4900 ns - result a0e5cd812455e04d6e33646cd8dc17e05b674231
SHA-2-256 time: 4100 ns - result aedaac3e798149ebaec99435ea67f2ff1fc8b5cd2f3b039b885bdf8c04678c03
SHA-3-256 time: 6100 ns - result 16c6f78ba37ae968b2602249278aad82aea653662b3e9583d598030f0fef5c4d
Kou
MD5 time: 8400 ns - result - 5aca6ec2885546912b2ea534d5225e60
SHA-1 time: 1200 ns - result f2c526b471623ac117ed27682b293f397c75ea4e
SHA-2-256 time: 1100 ns - result f20417e10d864ea23cc002ced9e9aec51babf1aa8660054c36b870fa4a834784
SHA-3-256 time: 1700 ns - result 631a3fb9a3a9de3a7c0e93807d44c5b4e79ffa8ab6c248a911065c6478f56004
```

2. Omówienie sposobu implementacji

Wykorzystana została wbudowana biblioteka hashlib, która zapewnia łatwy dostęp do popularnych funkcji skrótu.

Pomiar czasu operacji realizowany przez `time.time_ns()`, co pozwala na dokładne porównanie wydajności poszczególnych funkcji.

W eksperymentach SAC i badaniu kolizji wykorzystane zostało dodatkowe przetwarzanie – konwersję skrótów do postaci binarnej oraz losowe generowanie wejść.

3. Określenie roli soli w tworzeniu skrótów

Sol to losowy ciąg dodawany do hasła przed jego skróceniem.

Zapobiega to atakom przy użyciu precomputed hash tables (rainbow tables), ponieważ nawet dla takich samych haseł skrót będzie inny, jeśli sol jest inna.

4. Odpowiedź dotycząca bezpieczeństwa MD5

MD5 nie jest uważany za bezpieczny, ponieważ znane są praktyczne ataki kolizyjne.

Można znaleźć różne dane wejściowe, które generują ten sam skrót MD5, co czyni go nieodpowiednim do zastosowań wymagających wysokiego poziomu bezpieczeństwa.

Przykłady kolizji:

Kolizja: 845 dla aKNXWuL0 oraz oxWGso5m

Kolizja: 19c dla iVSTxTaE oraz eQVJ4mUW

Kolizja: 268 dla ELs0P1kP oraz k4v8iQS5

5. Wnioski

Porównanie szybkości: MD5 i SHA-1 są zazwyczaj najszybsze, ale kosztem bezpieczeństwa, natomiast SHA-256 i SHA3-256 są wolniejsze, ale bezpieczniejsze i generują dłuższe skróty.

Badanie kolizji na pierwszych 12 bitach: Przy analizie dużej liczby wejść można zauważyć, że kolizje na pierwszych 12 bitach występują stosunkowo wcześnie (przy około 4096 różnych wejściach) – co jest zgodne z teorią.

Właściwość SAC: Eksperyment pokazuje, że nawet niewielka zmiana wejścia (np. zmiana jednego znaku) skutkuje znaczną zmianą w skrócie, co potwierdza kryterium SAC.