Funkcja skrótu - sprawozdanie

Podstawy kryptografii, laboratorium

1. Wyniki testów funkcji skrótu:

Obraz zawierający tekst

Opis wygenerowany automatycznieObraz zawierający tekst

Opis wygenerowany automatycznie

1. Wyniki testów czasu przetwarzania funkcji skrótu dla plików o różnej wielkości:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Funkcja/ rozmiar pliku | 0.5MB | 1MB | 2MB | 10MB |
| MD5 | 0.0009146 | 0.0034623 | 0.0027782 | 0.0141639 |
| SHA-1 | 0.0005562 | 0.0009999 | 0.0021329 | 0.0105396 |
| SHA-244 | 0.0011993 | 0.0021406 | 0.0043056 | 0.0220748 |
| SHA-256 | 0.0010962 | 0.0021776 | 0.0042959 | 0.0221757 |
| SHA-384 | 0.0007884 | 0.0014254 | 0.0029118 | 0.0147274 |
| SHA-512 | 0.0007501 | 0.0014217 | 0.0030703 | 0.015068 |
| SHA-3-244 | 0.0013006 | 0.0026076 | 0.0056204 | 0.0261882 |
| SHA-3-256 | 0.0014806 | 0.0026987 | 0.0053439 | 0.0265981 |
| SHA-3-384 | 0.0018822 | 0.003462 | 0.0074517 | 0.0370282 |
| SHA-3-512 | 0.0032072 | 0.0049352 | 0.0102961 | 0.0509141 |

1. Czy funkcję MD5 można uznać za bezpieczną? Czy dotychczas zostały znalezione dla niej jakiekolwiek kolizje?
2. Badanie kolizji na pierwszych 12 bitach skrótu dla funkcji SHA-1
3. Sprawdzenie losowości wyjścia funkcji skrótu (kryterium SAC)

W celu sprawdzenie spełnienia kryterium SAC wykorzystano funkcję skrótu SHA2-256 i słowo wejściowe „kot” reprezentowane przez następujący ciąg bitów: 011010110110111101110100.

Obraz zawierający tekst

Opis wygenerowany automatycznie

Obraz zawierający tekst

Opis wygenerowany automatycznie

Obraz zawierający stół

Opis wygenerowany automatycznie

Średnio po zmianie jednego bitu na wejściu funkcji skrótu, zmianie uległo 59.8 z 64 (tj. ok. 93%) znaków skrótu wyjściowego (w porównaniu ze skrótem słowa bez zmian w bitach).

Kryterium SAC jest spełnione – niewielka zmiana na wejściu funkcji powoduje dużą zmianę w wynikowym skrócie.