Badanie funkcji skrótu

Badanie skrótów pliku oryginalnego i zmodyfikowanego

Plik oryginalny

```
LOREMIPSUMISSIMPLYDUMMYTEXTOFTHEPRINTINGANDTYPESETTINGINDUSTRYLOREMIPSUMHASBEENTHEIN
```

Zmodyfikowany plik

```
JOREMIPSUMISSIMPLYDUMMYTEXTOFTHEPRINTINGANDTYPESETTINGINDUSTRYLOREMIPSUMHASBEENTHEIN
```

SHA-256

```
Oryginalny plik:
11011100100101011110010111101110011001011000110100001101001001001101001010101011111(
Zmodyfikowany:
10010111101001111001111010110000100100011000101011101101011111111110110011101010111(
Diff:
1x01x1xx10xx01x11xxxx1xx1x1xxxx0xxxx0x0110001xxxxxx011010x1xx1xx11xxxxx01x10101x1110
```

Około 48.868778280542985% bitów zostało zmienionych w sumie kontrolnej po zmianie pliku źródłowego.

SHA-512

```
Oryginalny plik:
11000011100001101100111100010111101001111001011000010111110011011101101111111101101(
Zmodyfikowany:
11000011000011111011011101101110101111011101010011010000110001011101111001111110100
Diff:
11000011x000x11x1xxxx1110xxxx11x101xx11x1xxxxx100xxxxxxxx1x0xxxx11xx1x11xx1111x1xxxx
```

Około 49.065420560747663% bitów zostało zmienionych w sumie kontrolej po modyfikacji pliku źródłowego.

Kolizje sum kontrolnych SHA-1

Dla 16 bitów

Dwa pierwsze bajty sum kontrolnych SHA-1 są identyczne.

```
1e6dccfacff2d4d67d94b30b04921e30fb4e2e02  printable-dangerous.txt
1e6d198933b24f1538febdb787597b97188ccb22  printable-harmless.txt
ea66f5a7faf9c86ef6a7944a6af1c0b4bd0a1e1c  unprintable-harmless.txt
ea662f54e5c580183af4194f9de9583463243dca  unprintable-dangerous.txt
```

Statystyki szukania kolizji dla wersji "printable":

RunNo.	Steps until collision	Check of the collision	Total steps
01	63	61	124
02	488	442	930
03	308	234	542
04	224	138	362
05	481	450	931

Statystyki szukania kolizji dla wersji "unprintable":

RunNo.	Steps until collision	Check of the collision	Total steps
01	198	106	304

Dla 32 bitów

Cztery pierwsze bajty sum kontrolnych SHA-1 są identyczne.

```
b66a2f54e5c580183af4194f9de9583463243dca  printable-dangerous.txt
b66a2f54afbd2d8129aac00e7ba17fa7acefdbf1  printable-harmless.txt
62887d02fd8d96a9f88d930549272f7de91ef443  unprintable-dangerous.txt
62887d0228b7973dc96356ad157f3e6d76c07580  unprintable-harmless.txt
```

Statystyki szukania kolizji dla wersji "printable":

RunNo.	Steps until collision	Check of the collision	Total steps
01	51,072	44,504	95,576
02	67,270	66,837	134,107

Statystyki szukania kolizji dla wersji "unprintable":

RunNo.	Steps until collision	Check of the collision	Total steps
01	106,560	106,549	213,109
02	58,288	57,504	115,792

Cechy funkcji skrótu

- funkcja przyporządkowująca dowolnie dużej liczbie krótką wartość o stałym rozmiarze, tzw. skrót nieodwracalny
- słaba bezkolizyjność - dany jest skrót h(m) i odpowiadaj ąca mu wiadomość m. Znalezienie wiadomości m’ ≠ m, takiej że h(m) = h(m’), jest obliczeniowo trudne.
- silna bezoklizyjność -obliczeniowo trudne jest znalezienie dowolnej pary różnych wiadomości m’ i m, takich że h(m) = h(m’).

Wnioski

Funkcje skrótu można zastosować do:

- weryfikacji integralności danych (np. pliku ISO systemu operacyjnego)
- podpisów cyfrowych
- przechowywanie haseł
- sygnatury wirusów
- generowanie ciagów pseudolosowych
- wykorzystanie w protokołach np. SSH, SSL