Funkcje skrótu - własności i zastosowania na przykładzie SHA-256

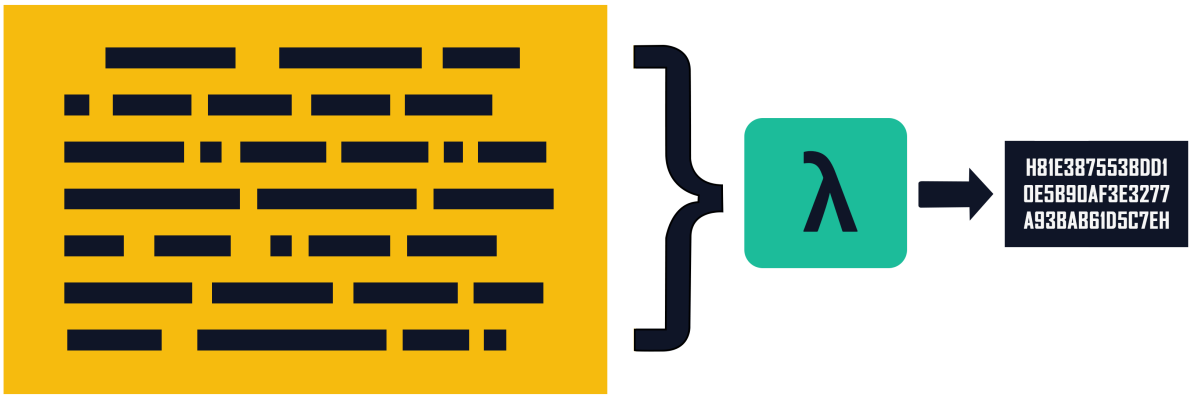
Jan Kocierz, Szymon Bizoń

9 kwietnia 2025

Wprowadzenie

Funkcja skrótu

Funkcja skrótu to odwzorowanie, które dowolnemu skończonemu ciągowi bitów przyporządkowuje ciąg o stałej, ustalonej z góry długości.



Rysunek: Ilustracja funkcji skrótu. Źródło: opracowanie własne.

Zastosowania funkcji skrótu

- Przechowywanie haseł w bazach danych
- Podpisy cyfrowe
- Sprawdzanie integralności danych
  - Pod kątem autentyczności
  - Pod kątem przypadkowych uszkodzeń

Zastosowania funkcji skrótu

- Przechowywanie haseł w bazach danych
- Podpisy cyfrowe
- Sprawdzanie integralności danych
  - Pod kątem autentyczności
  - Pod kątem przypadkowych uszkodzeń

Zastosowania funkcji skrótu

- Przechowywanie haseł w bazach danych
- Podpisy cyfrowe
- Sprawdzanie integralności danych
  - Pod kątem autentyczności
  - Pod kątem przypadkowych uszkodzeń

Definicja

Definicja

Niech $n \in \mathbb{N} \setminus \{0\}$. Przez $\{0,1\}^*$ będziemy oznaczać zbiór wszystkich ciągów bitów skończonej długości, ponadto $\{0,1\}^n$ będzie zbiorem informacji bitowych długości n, ustalonej z góry i stałej dla funkcji. Funkcją skrótu nazywamy każde odwzorowanie

$$H : \{0,1\}^* \to \{0,1\}^n.$$

Własności kryptograficznych funkcji skrótu

Własności

1. Jednokierunkowość
2. Słaba odporność na kolizje
3. Silna odporność na kolizje
4. Deterministyczność

Definicja

Kolizja to para wejść (m_1, m_2) taka, że $m_1 \neq m_2$ i $H(m_1) = H(m_2)$.

Uwagi

- Przez $A(x, y)$ będziemy oznaczać dowolny algorytm probabilistyczny.
- Przez U_t będziemy oznaczać zmienną losową przyjmującą wartości w $\{0,1\}^t \subset \{0,1\}^*$ z rozkładem jednostajnym, gdzie $t \in \mathbb{N}$.

Jednokierunkowość

Funkcja skrótu powinna być jednokierunkowa, to znaczy, że dla danego $y \in \{0,1\}^n$ trudno jest znaleźć $x \in \{0,1\}^*$ takie, że $H(x) = y$.

Jednokierunkowość

Funkcja skrótu powinna być jednokierunkowa, to znaczy, że dla danego $y \in \{0,1\}^n$ trudno jest znaleźć $x \in \{0,1\}^*$ takie, że $H(x) = y$.

Definicja

Funkcja $H : \{0,1\}^* \longrightarrow \{0,1\}^n$ jest jednokierunkowa, jeśli spełnia następujące warunki

1. H jest obliczalna przez deterministyczny algorytm wielomianowy
2. Dla każdego probabilistycznego algorytmu wielomianowego A prawdopodobieństwo

$$\mathrm{P}\left[A(H(U_t), t) \in H^{-1}(H(U_t))\right]$$

jest zaniedbywalne.

Słaba odporność na kolizje

Funkcja skrótu powinna posiadać słabą odporność na kolizje, to znaczy, że dla danego m_1 trudno jest znaleźć m_2 takie, że $m_2 \neq m_1$ i $H(m_2) = H(m_1)$

Słaba odporność na kolizje

Funkcja skrótu powinna posiadać słabą odporność na kolizje, to znaczy, że dla danego m_1 trudno jest znaleźć m_2 takie, że $m_2 \neq m_1$ i $H(m_2) = H(m_1)$

Definicja

Funkcja $H : \{0,1\}^* \to \{0,1\}^n$ jest słabo odporna na kolizje, jeśli dla ustalonego m_1 i każdego algorytmu probabilistycznego A prawdopodobieństwo

$$\mathrm{P}\left[A(H(U_t), t) = m_2 \text{ takie że } m_1 \neq m_2 \wedge H(m_1) = H(m_2)\right]$$

jest zaniedbywalne.

Silna odporność na kolizje

Funkcja skrótu powinna być silnie odporna na kolizje, to znaczy, że znalezienie dwóch różnych wejść m_1, m_2 takich, że $H(m_1) = H(m_2)$ powinno być trudne.

Silna odporność na kolizje

Funkcja skrótu powinna być silnie odporna na kolizje, to znaczy, że znalezienie dwóch różnych wejść m_1, m_2 takich, że $H(m_1) = H(m_2)$ powinno być trudne.

Definicja

Funkcja $H : \{0,1\}^* \to \{0,1\}^n$ jest odporna na kolizje, jeśli dla każdego algorytmu probabilistycznego A prawdopodobieństwo

$$\mathrm{P}\left[A(H(U_t), t) = (m_1, m_2) \text{ takich że } m_1 \neq m_2 \wedge H(m_1) = H(m_2)\right]$$

jest zaniedbywalne .

SHA-256

Secure Hash Algorithm

Funkcja skrótu SHA-256 generuje skrót o stałej długości 64 znaków w zapisie szesnastkowym dla dowolnej wiadomości wejściowej, niezależnie od jej długości.

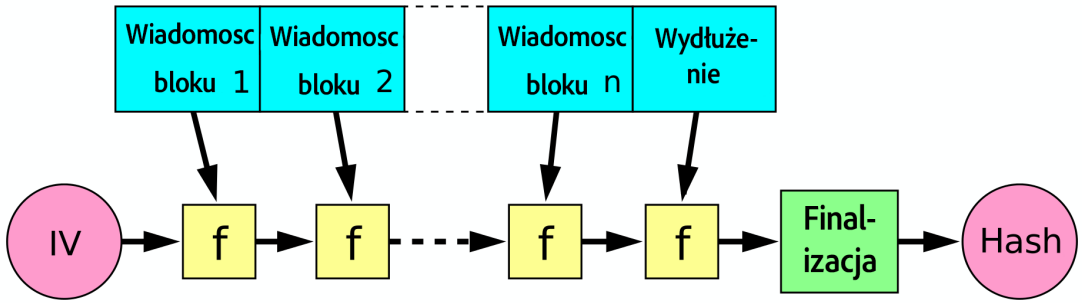


Rysunek: SHA-2. Źródło: Opracowanie własne.

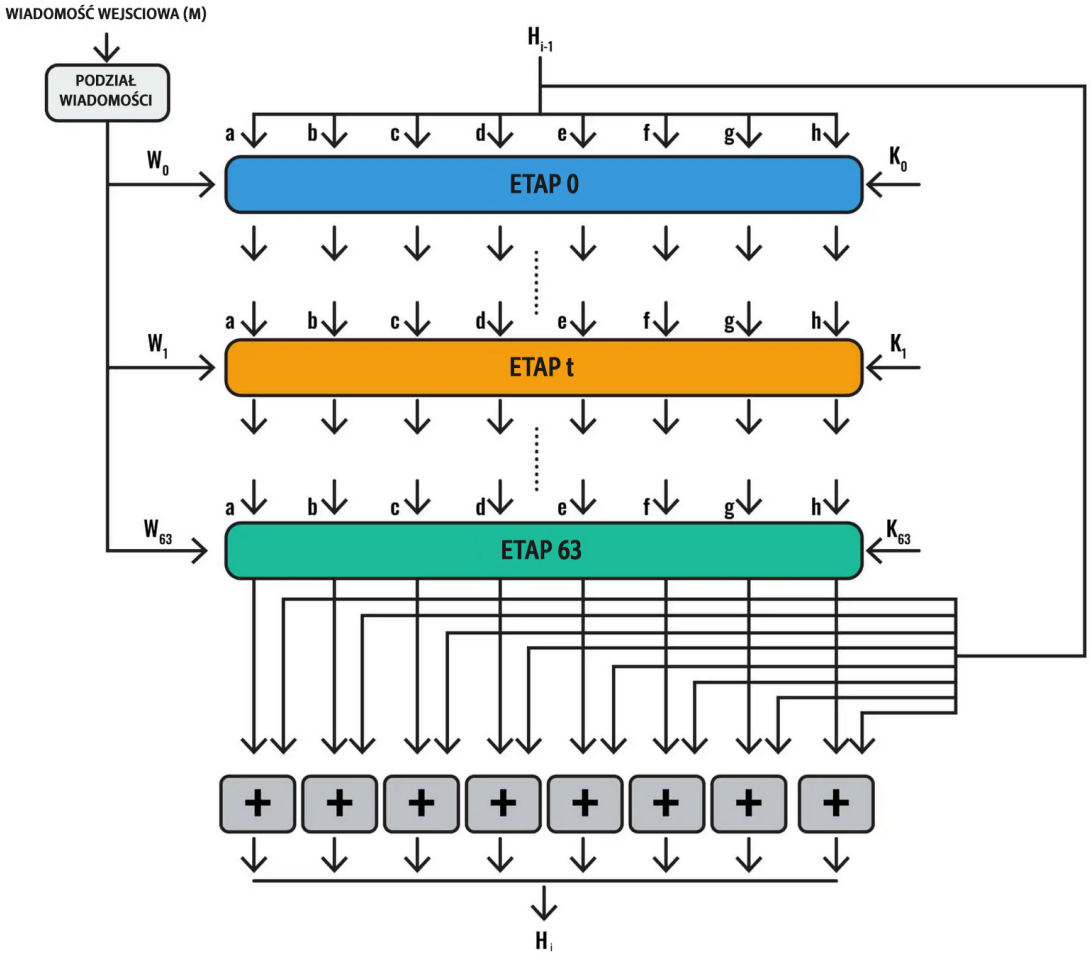
Jak działa algorytm SHA-256?

- $H : \{0,1\}^* \mapsto \{0,1\}^t$
- $f : \{0,1\}^b \mapsto \{0,1\}^t$
- M - wiadomość na wejściu przed rozszerzeniem,
- M^* - wiadomość po rozszerzeniu.

$$M^* \equiv 0 \pmod{b}$$



Rysunek: Konstrukcja Markle-Damargd

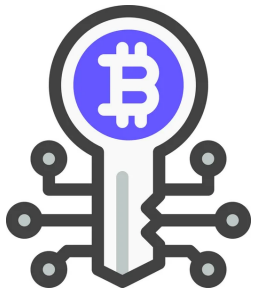


Rysunek: Schemat algorytmu i etapów funkcji SHA-2. Źródło: [4]

Zastosowania funkcji SHA-256

Kryptograficzna funkcja skrótu SHA-256 pełni centralną rolę w systemie blockchain Bitcoina.

- Identyfikowanie bloków w blockchainie za pomocą skrótu obliczanego przez SHA-2
- Generowanie adresów portfeli z klucza publicznego



Rysunek: Bitcoin. Źródło: [7]

Bibliografia I

[1] Oded Goldreich, Foundations of Cryptography Basic Tools, Press Syndicate Of The University of Cambridge, 2004, str. 33.

[2] Oded Goldreich, Foundations of Cryptography II Basic Applications, Press Syndicate Of The University of Cambridge, 2004, str. 513.

[3] Wahome Macharia, Cryptographic Hash Function, https://www.researchgate.net/profile/Wahome_Macharia/publication/351837904_Cryptographic_Hash_Functions/links/60aca8aa45851522bc156067/Cryptographic-Hash-Functions.pdf, Data dostępu: 6 kwietnia 2025.

Bibliografia II

[4] Josh Lake, comparitech.com, https://www.comparitech.com/blog/information-security/what-is-sha-2-algorithm/ dostep: 6 kwietnia 2025

[5] Operacja na blokach https://en.wikipedia.org/wiki/SHA-2 dostęp: 6 kwietnia 2025

[6] Grafika wektorowa, https://depositphotos.com/pl/vectors/znak-bitcoin.html Data dostępu: 6 kwietnia 2025

Dziękujemy za uwagę.