Podstawowe informacje o algorytmach

1. MD5:

MD5 (Message Digest 5) to algorytm funkcji skrótu, który tworzy 128-bitowy ciąg znaków z dowolnie długiego tekstu wejściowego. Jest stosunkowo szybki i prosty w implementacji, ale obecnie uważa się go za niebezpieczny do zastosowań, które wymagają wysokiego poziomu bezpieczeństwa. Algorytm MD5 został zaprojektowany w 1991 roku i od tego czasu został złamany, co oznacza, że ​​istnieją sposoby na łatwe odtworzenie tekstu wejściowego na podstawie wyniku funkcji skrótu.

1. SHA1:

SHA-1 (Secure Hash Algorithm 1) jest również algorytmem funkcji skrótu, który generuje 160-bitowy ciąg znaków z dowolnie długiego tekstu wejściowego. Został opracowany przez National Security Agency (NSA) w USA i opublikowany w 1995 roku. W przeszłości był powszechnie stosowany, ale obecnie uważa się go za niewystarczająco bezpieczny ze względu na to, że można go złamać w krótkim czasie za pomocą zaawansowanych metod obliczeniowych.

1. SHA256:

SHA-256 jest jednym z najnowszych i najbezpieczniejszych algorytmów funkcji skrótu. Tworzy 256-bitowy ciąg znaków z dowolnie długiego tekstu wejściowego. Jest to popularny algorytm stosowany w różnych aplikacjach, w tym w kryptografii i systemach uwierzytelniania. Jego złożoność obliczeniowa jest znacznie większa niż w przypadku MD5 i SHA1, co czyni go bardziej odpornym na ataki typu brute-force.

1. bcrypt:

bcrypt jest algorytmem szyfrowania haseł, który stosuje funkcję skrótu do przechowywania haseł użytkowników w bazie danych. Jest to jeden z najbezpieczniejszych algorytmów stosowanych w celu zapewnienia bezpieczeństwa haseł. Wykorzystuje funkcję skrótu, która jest powolna i wymaga większej mocy obliczeniowej, co utrudnia atakującym złamanie haseł metodami brute-force lub słownikowymi. Jego zastosowanie jest szerokie, zwłaszcza w przypadku aplikacji webowych, gdzie istnieje ryzyko ataków na hasła użytkowników.