* **MD5**

این الگوریتم یک مقدار هش 128 بیتی تولید می‌کند. این الگوریتم برای استفاده در رمزنگاری طراحی شده بود، اما با زمان ضعف‌هایی در آن کشف شدند و دیگر برای این منظور توصیه نمی‌شود. [اما هنوز برای تقسیم‌بندی پایگاه داده و محاسبه checksum برای اعتبارسنجی انتقال فایل‌ها استفاده می‌شود](https://heimdalsecurity.com/blog/what-is-hashing/).

* **SHA-1**

این الگوریتم نخستین نسخه از استاندارد الگوریتم هش امن (SHA) است. این الگوریتم در حالی که MD5 یک مقدار هش 128 بیتی تولید می‌کند، یک مقدار هش 160 بیتی (20 بایت) تولید می‌کند. در قالب هگزادسیمال، این یک عدد صحیح 40 رقمی است. مانند MD5، این الگوریتم برای کاربردهای رمزنگاری طراحی شده بود، اما به زودی ضعف‌هایی در آن نیز شناسایی شدند. [از امروز، این الگوریتم دیگر مقاومت کمتری در برابر حمله نسبت به MD5 ندارد](https://www.freecodecamp.org/news/md5-vs-sha-1-vs-sha-2-which-is-the-most-secure-encryption-hash-and-how-to-check-them/).

* **SHA-2**

این الگوریتم یک خانواده از الگوریتم‌های هش امن است که پس از SHA-1 طراحی شدند. این الگوریتم‌ها مقادیر هش با طول‌های مختلفی را تولید می‌کنند، از جمله 224، 256، 384 و 512 بیت. [این الگوریتم‌ها مقاومت بیشتری در برابر حملات رمزنگاری دارند و برای امنیت اطلاعات و ارتباطات استفاده می‌شوند](https://heimdalsecurity.com/blog/what-is-hashing/).

* **NTLM**

این الگوریتم یک پروتکل احراز هویت چالش-پاسخ است که توسط مایکروسافت برای سیستم‌های ویندوز طراحی شده است. این الگوریتم از الگوریتم MD4 برای تولید مقادیر هش از گذرواژه‌های کاربران استفاده می‌کند. این الگوریتم در سه نسخه مختلف وجود دارد NTLMv1، NTLMv2 و NTLM2 Session. [این الگوریتم نیز ضعف‌های امنیتی دارد و برای جایگزینی آن با پروتکل‌های احراز هویت مدرن‌تر توصیه می‌شود](https://en.wikipedia.org/wiki/NTLM).

* **LANMAN**

این الگوریتم یک الگوریتم هش قدیمی است که توسط مایکروسافت و آی‌بی‌ام برای شبکه‌های محلی طراحی شده است. این الگوریتم از الگوریتم DES برای تولید مقادیر هش از گذرواژه‌های کاربران استفاده می‌کند. این الگوریتم بسیار ضعیف است و به راحتی قابل شکستن است. [این الگوریتم دیگر در ویندوز‌های جدید پشتیبانی نمی‌شود](https://en.wikipedia.org/wiki/NTLM).

[**الگوریتم SHA-256**  
 یکی از شاخه‌های (Secure Hash-2) است که در سال ۲۰۰۱ توسط آژانس امنیت ملی به عنوان جانشین SHA-1 ایجاد شده است](https://zoomarz.com/what-is-the-sha-256-algorithm/).

برای ایجاد هش SHA-256، ابتدا داده ورودی به بلوک های ۵۱۲ بیت تقسیم می‌شود. سپس هر بلوک با یک مقدار اولیه ۲۵۶ بیتی (که از ۸ مقدار اولیه مشخص شده انتخاب می‌شود) و ۶۴ بار از یک تابع که از ۳ تابع کمکی تشکیل شده است، عبور می‌کند. [در نهایت، مقدار هش نهایی به دست می‌آید](https://zoomarz.com/what-is-the-sha-256-algorithm/).

به عنوان مثال، برای هش کردن رشته داده “Hello, World!”، ابتدا باید آن را به بلوک های ۵۱۲ بیت تقسیم کنیم. بلوک اول شامل کاراکترهای “Hello,” و بلوک دوم شامل " World!" است. سپس هر بلوک با مقدار اولیه SHA-256 و ۶۴ بار از تابع کمکی عبور می‌کند. [در نهایت، مقدار هش نهایی برابر با b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9   
خواهد بود](https://zoomarz.com/what-is-the-sha-256-algorithm/).

