گزارش پروژه ساختمان داده

اعضای گروه: پریا همتی - نفیسه جلیلوند

MD5 یکی از الگوریتم‌های هش رایج است که برای تولید مقدار هش یک پیام استفاده می‌شود. پیام ورودی را به عنوان ورودی می‌گیرد و مقدار هش متناظر را تولید می‌کند. این الگوریتم برای تأمین جزئیات امنیتی و تمرکز بر عملکرد طراحی نشده است و در کاربردهایی که نیاز به امنیت بالا است، توصیه نمی‌شود.

MD5از چندین گام مختلف تشکیل شده است. این گام‌ها عبارتند از:

۱.مرحله پیش‌پردازش :(Pre-processing) در این مرحله، ابتدا پیام ورودی به برخی قوانین خاص زیر تبدیل می‌شود:

- یک بیت ۱ به انتهای پیام اضافه می‌شود.
- سپس بیت‌های صفر به پیام اضافه می‌شوند تا طول کل پیام برابر با یک مقدار خاص شود.
- در انتها، طول بیتی پیام اصلی به پیام اضافه می‌شود.

۲.مرحله اصلی :(Main Loop) در این مرحله، پیام پس از پیش‌پردازش به بلوک‌های ۶۴ بایتی تقسیم می‌شود. سپس برای هر بلوک، چهل و هشت دور از محاسبات انجام می‌شود. در هر دور، مقادیر وضعیت (state)با استفاده از توابع و عملیات منطقی مختلف به روزرسانی می‌شوند.

۳.تولید خروجی :(Output) در این مرحله، مقادیر وضعیت نهایی به عنوان خروجی الگوریتم تولید می‌شوند. این مقادیر به صورت بایتی تبدیل می‌شوند و خروجی نهایی الگوریتم را تشکیل می‌دهند.

MD5دارای خصوصیات زیر است:

۱.تابع هش MD5 :تابعی است که یک پیام ورودی را به یک مقدار هش بایتی تبدیل می‌کند.

۲.یک‌طرفه: عملیات تولید مقدار هش به راحتی قابل انجام است، اما با توجه به خصوصیت یک‌طرفه بودن، بسیار سخت است که از مقدار هش به پیام ورودی متناظر برگردانده شود.

۳.قابلیت اطمینان: یک پیام با طول مشخص همواره به یک مقدار هش با طول ثابت نگاشت می‌شود. هرگونه تغییر کوچک در پیام ورودی باعث تولید یک مقدار هش کاملاً متفاوت می‌شود.

MD5در دهه‌ی ۱۹۹۰ یکی از الگوریتم‌های هش متداول است که برای تولید مقدار هش یک پیام استفاده می‌شود. هدف اصلی این الگوریتم، تولید یک مقدار هش ۱۲۸ بیتی (۱۶ بایتی) است که بر اساس ویژگی‌های خاصی از پیام ورودی محاسبه می‌شود. الگوریتم MD5 توسط رونالد ریف در سال ۱۹۹۲ ارائه

شد و در سال‌های پیشین برای مقاصدی مانند بررسی صحت داده‌ها و تأیید هویت استفاده می‌شد. اما در حال حاضر، به دلیل ضعف‌های امنیتی و شکست نسبتاً آسان آن، توصیه نمی‌شود.

MD5از چندین مرحله تشکیل شده است:

۱ .مرحله پیش‌پردازش :(Pre-processing) در این مرحله، پیام ورودی به یک طول ثابت تبدیل می‌شود. این مرحله شامل اضافه کردن یک بیت ۱ به پایان پیام، اضافه کردن بیت‌های صفر به پیام تا طول آن به یک مقدار خاص برسد، و اضافه کردن طول پیام اصلی به پیام است.

۲ .مرحله اصلی :(Main Loop) پیام پس از پیش‌پردازش به بلوک‌های ۶۴ بایتی تقسیم می‌شود. سپس برای هر بلوک، مقدار هش موقتی محاسبه می‌شود. در این مرحله، از توابع منطقی و عملیات بیتی مختلفی استفاده می‌شود تا مقدار هش موقتی به روزرسانی شود.

۳ .مرحله تولید خروجی :(Output) در این مرحله، مقدار هش نهایی با استفاده از مقادیر هش موقتی در مرحله قبلی تولید می‌شود. مقدار هش نهایی به صورت بایتی است و معمولاً به صورت مقادیر ۱۶ بیتی (۱۶ عدد از ۰ تا ۱۵) نمایش داده می‌شود.

پیچیدگی زمانی O(n) است.

پیچیدگی زمانی توابع:

Set_parents: O(h)

Depth: O(h)

Check_parents: O(h)

Check sibling: O(1)

Check distant relationship: O(2h+1)=O(h)

Common ancestor: O(h)

Farthest born: O(1)

Farthest relation: O(n)×O(n)=O(n^2)