MD5

1.HISTÓRIA

A criptografia MD5, sigla para Message Digest Algorithm 5, foi desenvolvida por Ronald Rivest, um renomado cientista da computação e criptógrafo, em 1991. Rivest projetou o MD5 como uma extensão do seu antecessor, o algoritmo MD4. Assim como o código morse, o nome MD5 deriva do acrônimo e do número de iterações que o algoritmo executa para gerar um hash exclusivo.

Originalmente concebido para verificar a integridade de dados, o MD5 logo encontrou aplicação em criptografia de senhas e verificação de integridade de arquivos. No entanto, ao longo do tempo, vulnerabilidades foram descobertas no MD5, tornando-o suscetível a ataques de colisão, onde diferentes conjuntos de dados podem gerar o mesmo hash.

2.COMO FUNCIONA

O MD5 é um algoritmo de hash que converte informações de comprimento variável em uma sequência alfanumérica fixa de 128 bits, representada geralmente por 32 caracteres hexadecimais. Ao contrário do código morse, que utiliza pulsos elétricos e pausas, o MD5 opera aplicando uma série de operações matemáticas complexas, como funções lógicas e rotações, aos blocos de dados de entrada.

A força do MD5 reside na sua rapidez e eficiência no cálculo de hashes. Contudo, sua vulnerabilidade a colisões o tornou obsoleto para muitos casos de uso, especialmente na segurança de senhas e na integridade de dados críticos. Atualmente, algoritmos mais seguros, como o SHA-256, são preferidos para garantir uma proteção mais robusta.