Algoritmos de hash

MD5- O algoritmo MD5 é um algoritmo de hash que a partir de uma entrada qualquer é gerado uma saída de 128 bits. O algoritmo MD5 foi inicialmente projetado para criptografia, porém o mesmo apresenta algumas vulnerabilidades, tornando a mesma ineficiente para esse propósito, porém utilizando a técnica de salting, que é escolher uma string de tamanho fixo e adicionar a string a ser codificada, assim aumentando a dificuldade em decodificar o conteúdo. Mesmo com suas vulnerabilidades já descobertas e documentadas, o MD5 continua sendo amplamente utilizado.

SHA2- SHA2 é um conjunto de funções hash criptográficas desenvolvidas pela NSA, o mesmo possui 4 variantes dependendo do número de bits *SHA-224, SHA-256, SHA-384 e SHA-512.*

SHA256- Entre os algoritmos da família SHA2, o SHA-256 é um dos algoritmo mais utilizados, pelo seu equilíbrio em segurança e custo computacional de geração, pois é um algoritmo muito eficiente para a alta resistência à colisão que possui.

O Algoritmo SHA-256 é considerado mais seguro que o MD5 que tem vulnerabilidades amplamente documentadas e o SHA-1, porém ele é cerca de 20-30% mais lento de calcular que esses algoritmos.

Uma das características do SHA-256 é que sua saída tem sempre 256 bits. O mesmo é considerado extremamente seguro, e é implementado em várias aplicações e protocolos como o TLS, SSL, PGP e SSH.

Em bitcoin por exemplo o SHA-256 é usado para o processo de mineração (criação de bitcoins), mas também no processo de geração endereços de bitcoin. Isso se deve ao alto nível de segurança que oferece.

BCRYPT- é uma função hash desenvolvida por Niels Provos e David Mazières e baseado na cifra simétrica blowfish, o mesmo foi desenvolvido para criptografar senhas em texto plano para uma hash. Uma das vantagens do BCRYPT é o uso de um salt, que é uma string fixa que é adicionada na senha a ser criptografada, assim conseguindo aumentar a segurança contra ataques de força bruta como o *rainbow tables*, pois utilizando um salt aleatório para cada senha, mesmo que a senha seja a mesma para dois usuários as hash geradas serão diferentes. Um mecanismo que o algoritmo usa para aumentar a segurança são os *salt rounds*, que são as iterações para a geração da hash, por padrão o algoritmo utiliza 10 rounds, mas o mesmo pode ser alterado, aumentando o tempo para geração da hash, mas garantindo uma maior segurança. O BCRYPT é considerado um algoritmo de hash seguro, e não têm vulnerabilidades documentadas, mas o mesmo não é recomendados para encriptar uma grande quantidade de dados, pois o algoritmo foi projetado para gerar hash de senhas, e com um grande volume de dados o algoritmo se torna lento.