Aplicações
-Resumir Dados
-Verificar a integridade de arquivos
-Segurança e senha de servidores

Resumir Dados

É fácil visualizar essa aplicação em download de arquivos ai baixar um arquivo na internet o seu smartphone ou pc irá pedir ao banco de dados do servidor o arquivo com a sua respectiva hash. E como isso ocorre tão rápido ? Isso é devido a existir uma função criptografada que é responsável por armazenar o arquivo, portanto o servidor consegue localizar o arquivo tão rapidamente.

Função Associada

Message Digest(MD) versões comuns MD2, MD3, MD4 e MD5 e a função RIPEMD que é uma versão melhorada da MD

Verificar a integridade de arquivos

O papel principal do antivírus é verificar a integridade de um arquivo e para isso ele utiliza o hash. E como isso ocorre ? Resumidamente o antivírus compara a hash do arquivo que está sendo baixado com a hash do servidor caso sejam diferentes é um indício que o arquivo foi corrompido e ao fazer qualquer alteração o hash é modificado em relação ao original.

Função associada

SHA-1 que inclusive é usada como chave de criptografia do Git.

Segurança de senhas e arquivos

Servidores bem construídos não armazenam as senha dos usuários invés disso armazenam as hash associada às senhas por isso que quando você esquece a senha e pede a sua recuperação normalmente o site ou aplicativo pede para que você crie uma nova pois o não é possível decifrar o hash.

Funções associadas

Scryp

O scryp é uma função "CPU-hardned", mas também tem a vantagem de ser "Memory-hard". Ele consome não apenas a CPU como também utiliza mais recursos de memória.

Argon2

Argon2 adiciona uma terceira dimensão de complexidade e custo: o número de threads usados para calcular o hash.Os invasores precisam ter não apenas uma grande quantidade de recursos de computação e memória disponíveis, mas também mais núcleos de CPU físicos. O que torna os ataques de força bruta substancialmente mais caros para serem executados.

PBKDF2

O ASP.NET Identity utiliza o PBKDF2 com HMAC-SHA256, um Salt de 128 bit e uma sub-chave de 256 bit. E por padrão 10.000 iterações.

PHP
Utiliza as funções md5 e sha1

Python
SHA-1, Argon2 e PBKDF2

Java
SHA-1, Argon2 e PBKDF2

Javascript
SHA-1, Argon2 e PBKDF2