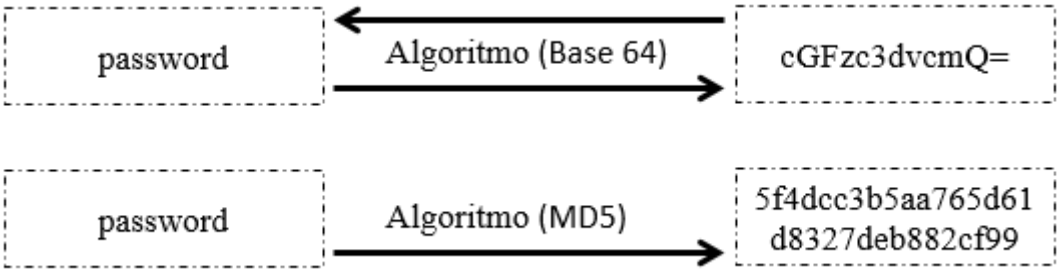
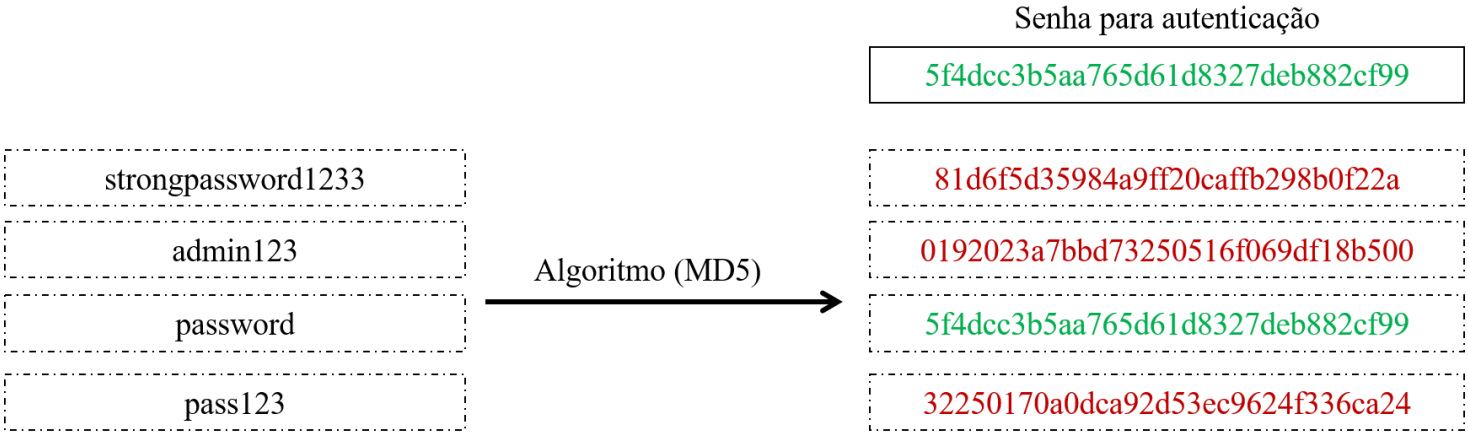
Fábrica de Noobs

Criptografia – Funções de Hash

Neste vídeo, trabalharemos com as funções de hash, tais como MD4, MD5, SHA1, SHA256, entre outros. Ao contrário dos métodos de criptografia estudados até agora, essas funções são unidirecionais.

Isso significa que é possível criptografar utilizando um algoritmo, mas não é possível fazer o processo contrário. Esses recursos são utilizados, por exemplo, para realizar autenticações de login ou armazenar senhas em bancos de dados.





A única forma de se quebrar uma função de hash, como MD5 é a partir de um ataque de força bruta, onde uma lista com possíveis senhas e suas respectivas codificações é comparada com a hash até uma correspondência ser encontrada. Logo, uma hash gerada de uma senha forte é resistente a ataques de força bruta.

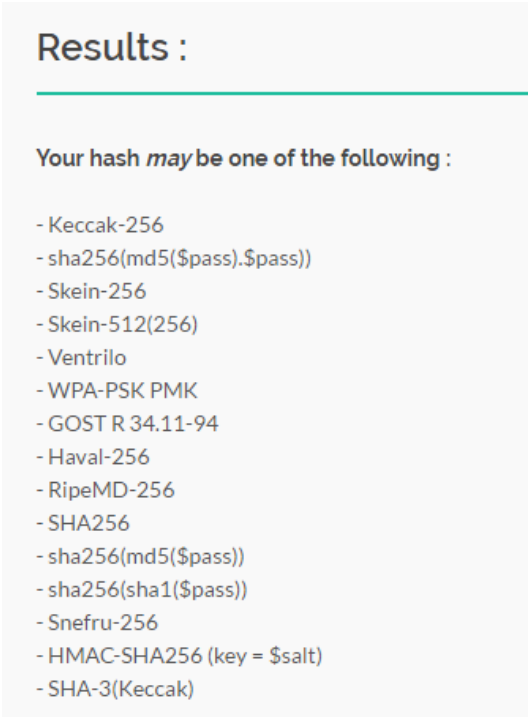
Segue a lista de algoritmos disponível para encriptação:

- AMID-97C: http://crypo.bz.ms/secure-amid97c-online
- YARRO-30S: http://crypo.bz.ms/secure-yarro30s-online
- GELOC-8: http://crypo.bz.ms/secure-geloc8-online
- HUST-10/D: http://crypo.bz.ms/secure-hust10d-online

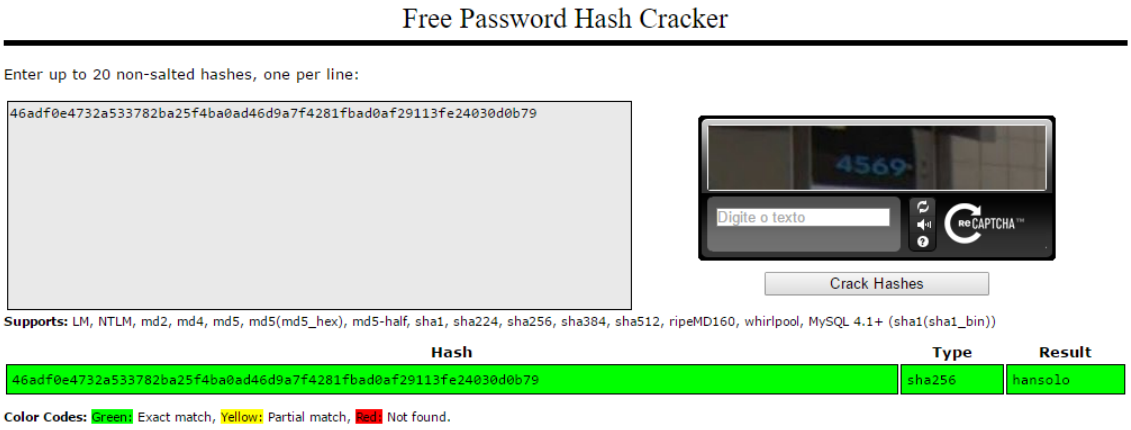
- GUGON-26: http://crypo.bz.ms/secure-gugon26-online
- MIHO-78: http://crypo.bz.ms/secure-miho78-online
- LEPAD-18: http://crypo.bz.ms/secure-lepad18-online
- TRAN-15X: http://crypo.bz.ms/secure-tran15x-online
- ESTYA-6: http://crypo.bz.ms/secure-estya6-online
- ZUNE-32: http://crypo.bz.ms/secure-zune32-online
- MD2: http://crypo.bz.ms/secure-md2-online
- MD4: http://crypo.bz.ms/secure-md4-online
- MD5: http://crypo.bz.ms/secure-md5-online
- CRC32: http://crypo.bz.ms/secure-crc32-online
- RIPEMD-160: http://crypo.bz.ms/secure-ripemd-online
- SHA1: http://crypo.bz.ms/secure-sha1-online
- SHA256: http://crypo.bz.ms/secure-sha256-online
- SHA512: http://crypo.bz.ms/secure-sha512-online
- HIX-25: http://crypo.bz.ms/secure-hix25-online
- SHARK-35: http://crypo.bz.ms/secure-shark32-online

Existem serviços online que permitem a identificação e uma possível quebra da hash.

O OnlineHashCrack (http://www.onlinehashcrack.com/hash-identification.php#res) nos retorna uma lista de potenciais criptografias em que uma hash foi codificada. Em determinadas situações, esse processo é importante para se iniciar um ataque de força bruta direcionado.



Já o CrackStation (https://crackstation.net) realiza o ataque de wordlist e procura retornar uma hash correspondente.



O Hashkiller (https://hashkiller.co.uk/) também realiza esse serviço.