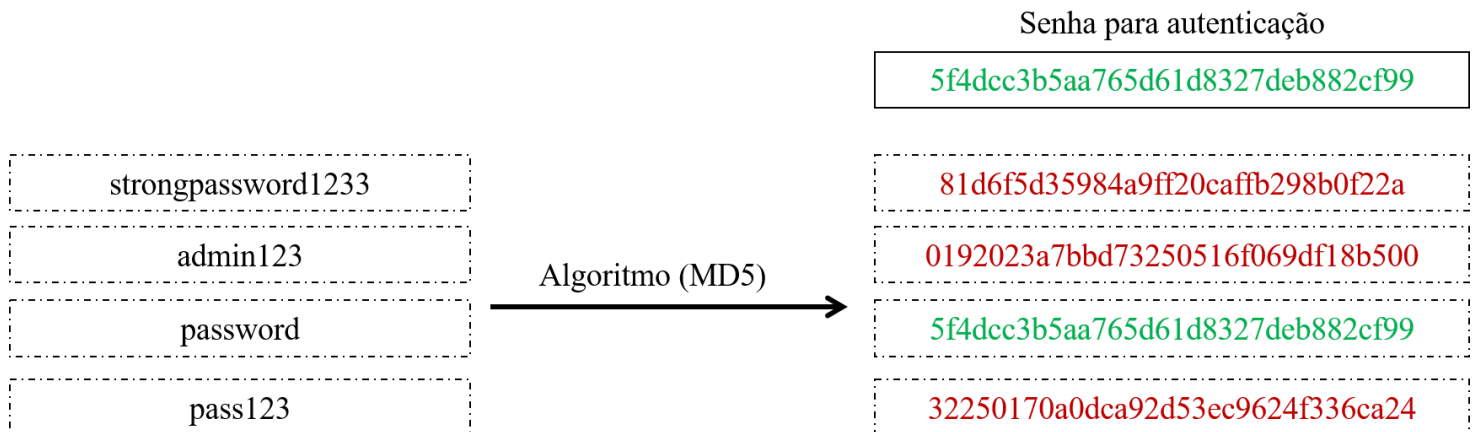
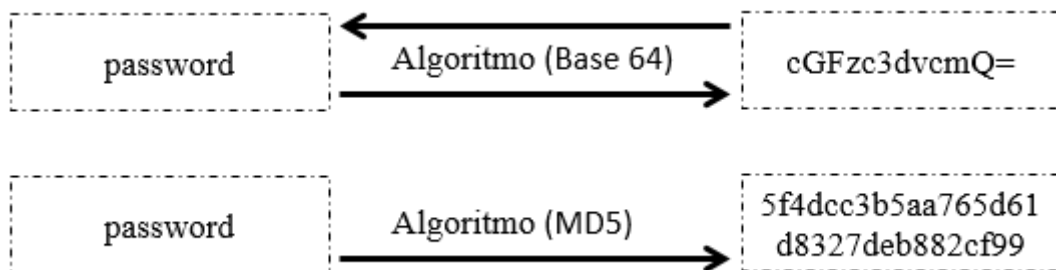


## Fábrica de Noobs

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

## Results :

Your hash *may* be one of the following :

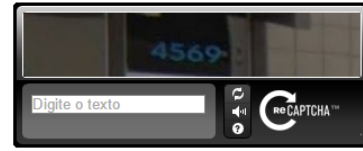
- Keccak-256
- sha256(md5(\$pass).\$pass))
- Skein-256
- Skein-512(256)
- Ventrilo
- WPA-PSK PMK
- GOST R 34.11-94
- Haval-256
- RipeMD-256
- SHA256
- sha256(md5(\$pass))
- sha256(sha1(\$pass))
- Snefru-256
- HMAC-SHA256 (key = \$salt)
- SHA-3(Keccak)

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

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
46adf0e4732a533782ba25f4ba0ad46d9a7f4281fbad0af29113fe24030d0b79
```



Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin))

Hash	Type	Result
46adf0e4732a533782ba25f4ba0ad46d9a7f4281fbad0af29113fe24030d0b79	sha256	nansolo

**Color Codes:** ■ Exact match, ■ Partial match, ■ Not found.

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

Status: ■ We found 1 hashes! [Timer: 134 m/s] Please find them below...

SHA1 Hashes:

```
f865b53623b121fd34ee5426c792e5c33af8c227
```

Max: 64

Please use a standard list format

```
f865b53623b121fd34ee5426c792e5c33af8c227 SHA1 : admin123
```