

To crypt or not to crypt

Description: Your friend says he loves to 'encrypt' his passwords. Fearing that you might crack it, he has decided not to tell you the hash function he used! Find his password to punish him for hiding his passwords from you!

Format: RM{the_password}

Type: Crypto

Level: Easy

En téléchargeant le fichier `encrypt.enc`, nous obtenons la chaîne de caractère

suivante: `621ec23e9e9bc5a442c280eb8ff66e0c6a6d571f69c155bbc53015e1195feaae9c918be1507554c8efff680446f32eebff74d0d907e0fc239da947849b049811`

A l'aide d'outils simple et puissants, comme

<https://crackstation.net/>, nous pouvons cracker le Hash

CrackStation

Free Password Hash Cracker

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

```
621ec23e9e8c5a442c280ebff66ebc6ad571f69c155bbc53015e1195feae9c918be1507554c8efff66844cf32eebf7764b2b0768ff2239da947849b049811
```

Je ne suis pas un robot

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), QubesV3.1BackupDefaults

Hash	Type	Result
621ec23e9e8c5a442c280ebff66ebc6ad571f69c155bbc53015e1195feae9c918be1507554c8efff66844cf32eebf7764b2b0768ff2239da947849b049811	win1pool	p@ssw0rd!

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security page](#).

CrackStation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries [here](#), and the lookup table implementation (PHP and C) is available [here](#).

Last Modified: May 27, 2019, 8:19am UTC
Page Hits: 44495036
Unique Hits: 8679752

Nous obtenons ainsi le password: p@ssw0rd!

Ainsi le flag est: RM{p@ssw0rd!}