

## Fundamentals of Information Security: Cybersecurity (88252)

Ana M Herrera Flores

### Crypto Attacks

1. Create a password hash. Use a web browser to go to [www.fileformat.info/tool/hash.htm](http://www.fileformat.info/tool/hash.htm)
2. Under String Hash, enter the simple password apple123 in the Text: box.
3. Click Hash.
4. Scroll down the page and copy the MD4 hash of this password to your Clipboard by selecting the text, right-clicking and choosing Copy.
5. Open a new tab on your web browser. Go to <https://crackstation.net/>
6. Paste the MD4 hash of apple123 into the text box beneath Enter up to 10 non-salted hashes:
7. In the RECAPTCHA box, enter the current value being displayed in the box that says Type the text.

8. Click Crack Hashes.

- How long did it take the rainbow table to crack this hash?

1 second

10. Click the browser tab to return to FileFormat.Info.
11. Under String hash, enter the longer password 12applesauce in the Text: box.
12. Click Hash.
13. Scroll down the page and copy the MD4 hash of this password to your Clipboard.
14. Click browser tab to switch to the CrackStation site.
15. Paste the MD4 hash of 12applesauce into the text box beneath Enter up to 10 non-salted hashes:
16. In the RECAPTCHA box, enter the current value being displayed in the box that says Type the text.
17. Click Crack Hashes.
- How long did it take the rainbow table to crack this hash?

1 second

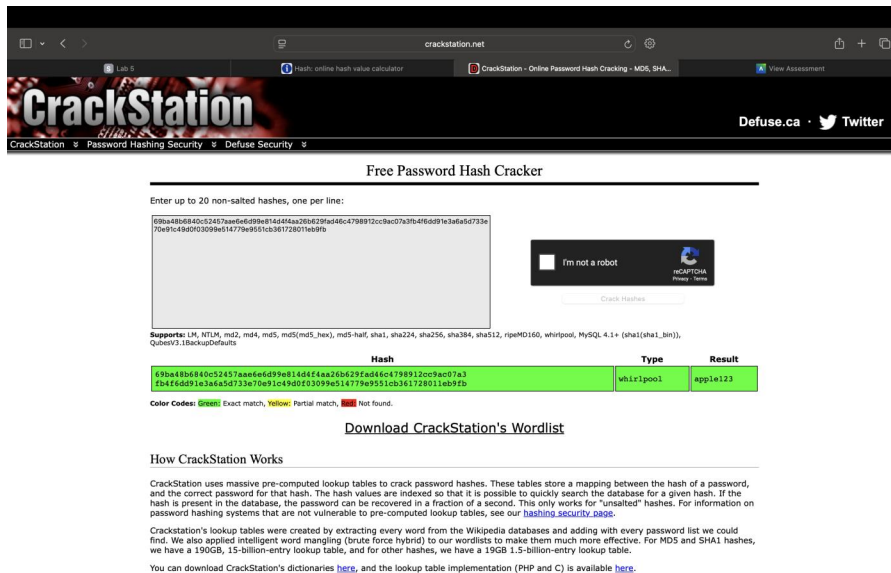
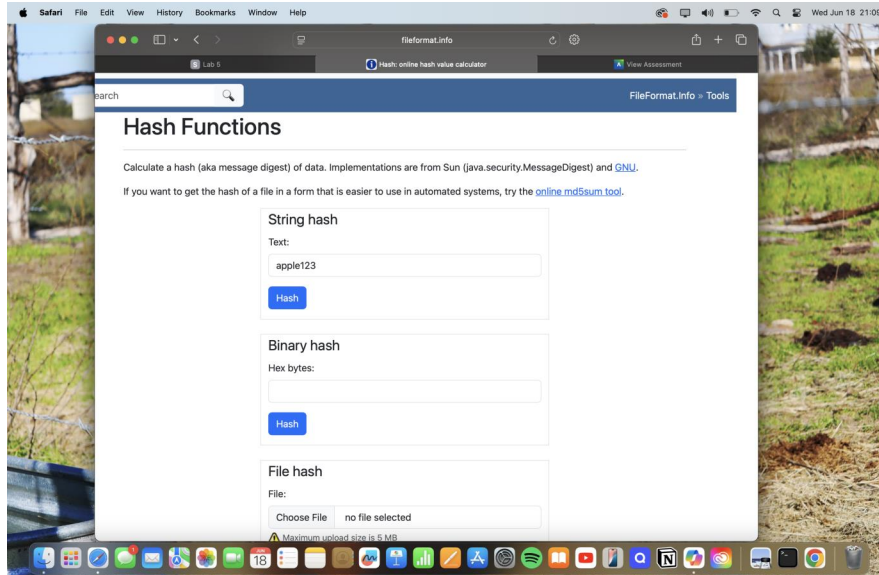
18. Try to do some other password cracks. Answer the question: What is more important the algorithm or the complexity of the password? Explain...

The complexity is more important; this means we should avoid common passwords patterns, making it harder for hackers to crack the password.

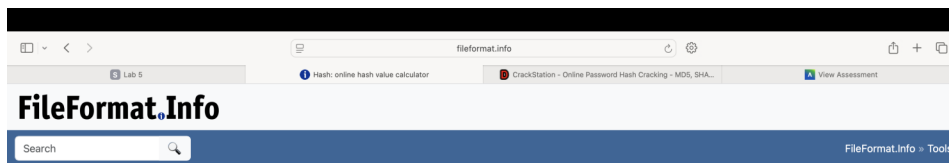
WHAT TO TURN-IN.

- 1) Show me screen shots that you have created hash values and cracked them.

- a. Explain the screen shots/snippets
- 2) Make sure you answer Question 18.



These 2 screenshots are for apple123 example, and we can see that we were able to obtain the password from the rainbow table.



## Hash Functions

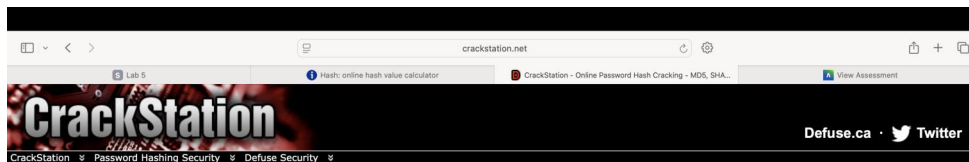
Calculate a hash (aka message digest) of data. Implementations are from Sun (java.security.MessageDigest) and [GNU](#).

If you want to get the hash of a file in a form that is easier to use in automated systems, try the [online.md5sum tool](#).

**String hash**  
Text:

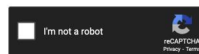
**Binary hash**  
Hex bytes:

**File hash**  
File:  
 no file selected  
Microsoft.com contacted you for E.M.D



## Free Password Hash Cracker

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



**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1{sha1\_bin}), Quibev3.1BackupDefaults

Hash	Type	Result
12aad86e5e5b1844b4c7bc6ed743ea7b83e4ee38d3f1439d13c77fbc5ae26034f5d85fcaaf49fab533cfc2518c3095624b39ea55ce42ef1do214d1f44c00537	whirlpool	12applesauce

**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](#).

As in the previous example, these 2 pictures are also from the examples provided in class. This one is for 12applesauce. The rainbow table was also able to crack the password.

fileformat.info

Lab 5Hash: online hash value calculatorCrackStation - Online Password Hash Crack...View AssessmentTry to do some other password cracks. Answ...

FileFormat.Info

SearchFileFormat.Info » Tools

Hash Functions

Calculate a hash (aka message digest) of data. Implementations are from Sun (java.security.MessageDigest) and [GNU](#).

If you want to get the hash of a file in a form that is easier to use in automated systems, try the [online md5sum tool](#).

String hash

Text:

SczMq3jT@

Hash

Binary hash

Hex bytes:

Hash

File hash

File:

Choose Fileno file selected

Maximum upload size is 5 MB

crackstation.net

Lab 5Hash: online hash value calculatorCrackStation - Online Password Hash Crack...View AssessmentTry to do some other password cracks. Answ...

CrackStation

Defuse.caTwitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

6d7f5cd09c032f187e208498292b780c07924e7be5d58904c66e3e3d52a1f0f3252c83dd2386c47740f8b1220be4e473798059ad5ad4345ba601cae7ef98e040

I'm not a robot

reCAPTCHA

PrivacyTerms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QuiesY3.1BackupDefaults

Hash	Type	Result
6d7f5cd09c032f187e208498292b780c07924e7be5d58904c66e3e3d52a1f0f3252c83dd2386c47740f8b1220be4e473798059ad5ad4345ba601cae7ef98e040	Unknown	Not found.

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](#).

In these other 2 screenshots I introduced a password from an old wi-fi card that I used in Cuba. The password is not long, but it is a combination of upper and lower cases, numbers, and symbols. It doesn't mean anything, and the rainbow table was unable to crash into it.

fileformat.info

Lab 5Hash: online hash value calculatorCrackStation - Online Password Hash Cracki...View AssessmentTry to do some other password cracks. Answ...

FileFormat.Info

SearchFileFormat.Info > Tools

Hash Functions

Calculate a hash (aka message digest) of data. Implementations are from Sun (java.security.MessageDigest) and GNU.

If you want to get the hash of a file in a form that is easier to use in automated systems, try the [online md5sum tool](#).

String hash

Text:  
capitanamerica

Hash

Binary hash

Hex bytes:

Hash

File hash

File:  
Choose Fileno file selected

Maximum upload size is 5 MB

crackstation.net

Lab 5Hash: online hash value calculatorCrackStation - Online Password Hash Cracki...View AssessmentTry to do some other password cracks. Answ...

CrackStation

Defuse Hashing SecurityDefuse Security

Defuse.caTwitter

Free Password Hash Cracker

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

abdd4774f1d1862e889b40b5e14ba5623f2e744c3cd7ad5094a3a4a183bb2e274  
22f705f6ca24acec14515e5315f5df57e0bea5e08ffe8

I'm not a robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-hair, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1{sha1\_bin}), QubesV3.1BackupDefaults

Hash	Type	Result
abdd4774f1d1862e889b40b5e14ba5623f2e744c3cd7ad5094a3a4a183bb2e274	whirlpool	capitanamerica
589387686b95cab7c6a22f705f6ca24acec14515e5315f5df57e0bea5e08ffe8		

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](#).

This last example used the password capitanamerica. The rainbow table was able to crash the password in less than a second. The password is simple and refers to something that a lot of people know and use in their passwords.