
OMU
HACKERS

Announcements

- Quiz

Quiz

This Monday!!

OMU HACKERS

Announcements

- Quiz
- Christmas Meal

Christmas Meal

Announcements

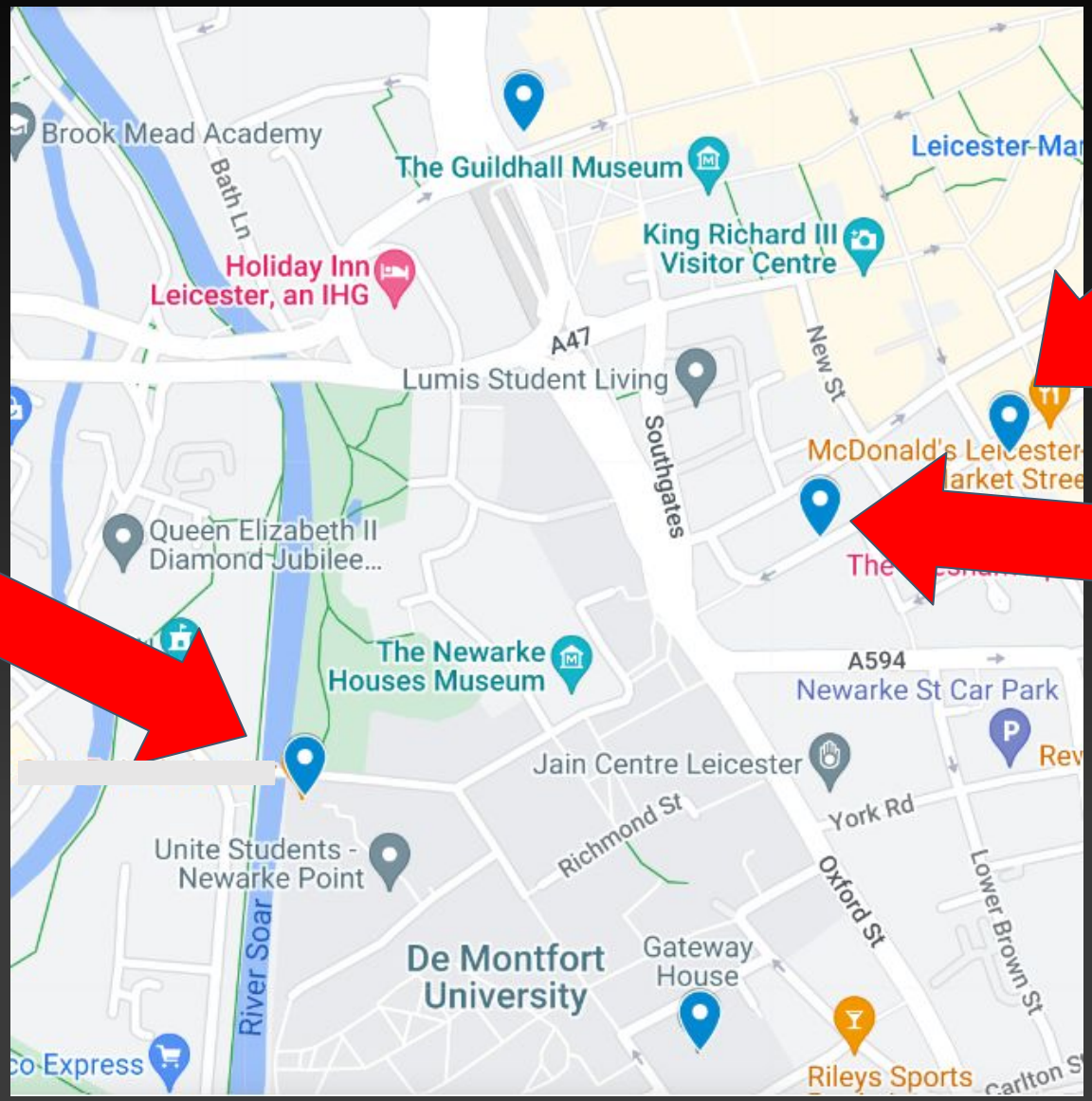
- Quiz
- Christmas Meal
- Lanyards
- And last but not least…

TryHackMe Advent of Cyber 2023

OMU HACKERS

Social

THE SOAR POINT



FIREBUG
BAR . VENUE . FOOD

oddbar

DMU HACKERS

Hash Functions & Cracking

Don't do illegal shit

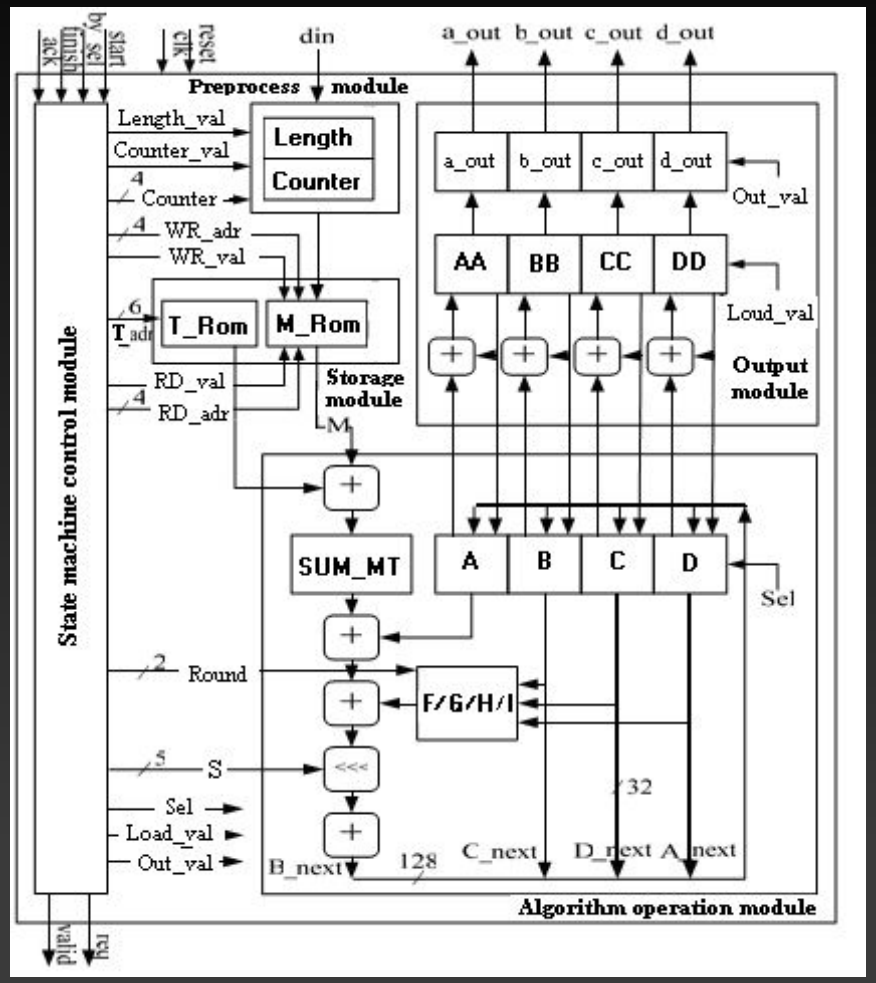
Pretending you are 12

- Capital Letters, Numbers, Symbols, Sentences over just words
- Don't leave passwords laying around
- Update regularly

What is a hash function?

- An irreversible, complex calculation
- Takes an input (plaintext) and produces a fixed-size output (digest aka hash)

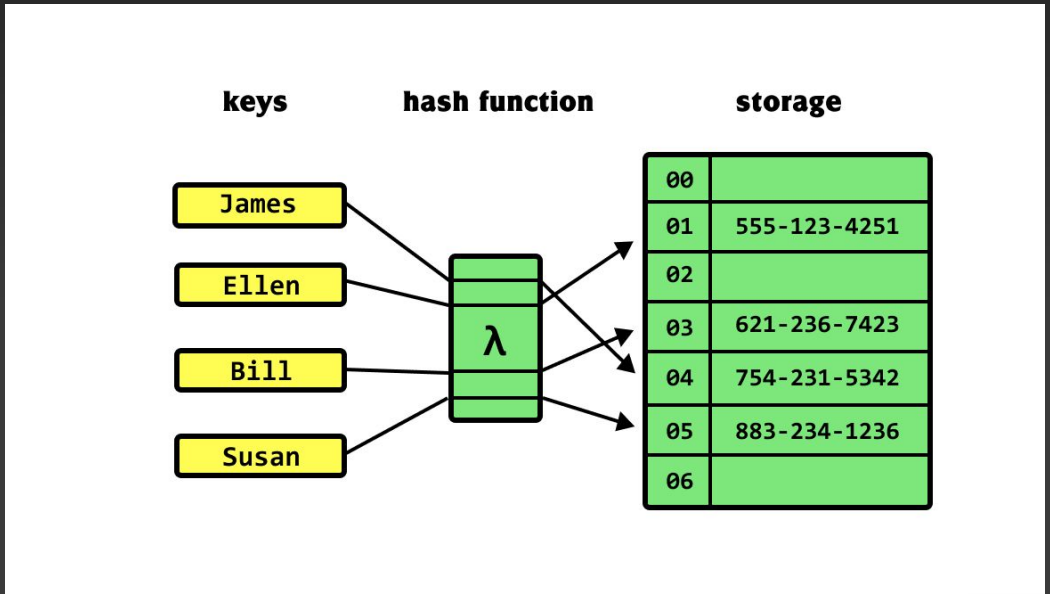
What is a hash function?



MD5 Algorithm

What is a hash function?

- Should be a case of:
- 2 ***same*** plaintexts will always give the ***same*** hash
- 2 ***different*** plaintexts should always have **unique hashes**



What is a hash?

- Changing just 1 part of a plaintext will change the hash drastically

password123	482c811da5d5b4bc6d497ffa98491e38
password1234	bdc87b9c894da5168059e00ebffb9077

- Case-sensitive (as 'A' and 'a' are different binary values)

confusion	c52e29d93f53d6098cc31d7e185008d0
Confusion	54894e44b2caf1104cfb21288a0e449e

Security of Hashes

- Longer hashes provide more security because there are more possible combinations
- For example
  - MD5 creates a message digest of 128-bits
  - SHA1 creates a message digest of 160-bits
- And so SHA1 is more secure than MD5
- SHA256 uses 256-bits, which is much more secure than both SHA1 and MD5.

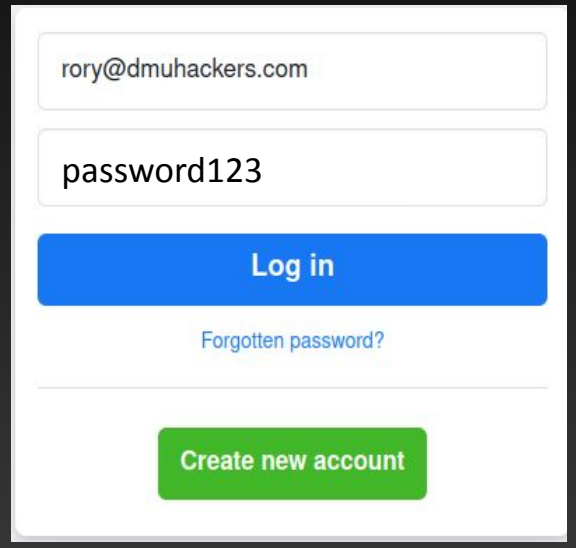
What are hashes actually used for?

Passwords

- Password stored in database as a hash
  - This means if passwords are stolen, makes it harder for attacker to find out what it is
- When you log in, it hashes your input and then compares this to your stored password
  - Server will respond with either 'yes' or 'no'

What are hashes actually used for?

Passwords



Email	Salt	Password
rory@dmuhackers.com	ba	9c1b25a3a226d7747189deda42c12e52

Lookup the 'salt'

- Random value added to password
- Means 2 users who have same plaintext password very unlikely to have same hash

What are hashes actually used for?

Passwords

Email	Salt	Password
rory@dmuhackers.com	ba	6c1b25a3a226d7747189deda42c12e52

password123 482c811da5d5b4bc[illegible]497ffa98491e38

password123ba 6c1b25a3a226[illegible]189deda42c12e52

These are MD5 hashes and would (hopefully) not be used as it's been broken!
(more on this later)

What are hashes actually used for?

Rainbow Tables

- Hashes are irreversible - right?
- Nothing to stop somebody looking up hashes in advance… (we'll pretend salts aren't a thing)

Password	MD5 Hash
123456	e10adc3949ba59abbe56e057f20f883e
12345	827ccb0eea8a706c4c34a16891f84e7b
123456789	25f9e794323b453885f5181f1b624d0b
password	5f4dcc3b5aa765d61d8327deb882cf99
iloveyou	f25a2fc72690b780b2a14e140ef6a9e0

What are hashes actually used for?

Rainbow Tables

- Can create a custom rainbow table - e.g if you think a victim might use their cat's name as a password - nibbles, Nibbles, Nibbles44 …

- Not effective when salting is in use
- Still works against systems where salting is not implemented

What are hashes actually used for?

File Integrity Checking

- Usually measures in place to ensure files download wholly and completely
- Only way to check **for sure** is to compare hashes!
- Software developer will provide 'initial hash', you download file and calculate 'subsequent hash' and compare the two - if the same, the file is a carbon copy!
- Used in forensics too to check files are same as when you first took the evidence


Kali Linux 2023.3 Changelog
64-bit
32-bit
Apple Silicon (ARM64)
Recommended
64
Installer
Complete offline installation
with customization
3.9G
torrent
sum


Kali Linux 2023.3 Changelog
64-bit
32-bit
Apple Silicon (ARM64)
SHA256sum
ffe5aa3932397895
257252a144f9c62f
2b8663f6b3f8bcf1
20b5ae53045d6031
3.9G
torrent
sum


OMU
HACKERS

Other Uses of hashing

Digital Signatures

Blockchain and Cryptocurrency

Data Deduplication

Combatting Online Child Abuse

Cracking Hashes

Cracking Hashes

- Although hashes are supposed to be secure, they can be cracked!
- Depending on the algorithm, can take **a lot** of compute power (especially GPU)
- GPU speeds up hash cracking as it's much better than a CPU at completing tasks in parallel (at the same time)

Cracking Hashes

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Take these with a pinch of salt!

rockyou.txt

- Company RockYou was breached - attackers stole 32 million user records - with passwords stored in PLAIN TEXT!!!!

rockyou.txt

- After the breach, the complete list of passwords was leaked
- In amateur pentesting (ie CTFs), without a doubt the most common 'wordlist'
- Comes as standard with Kali Linux

```
root@kali:~# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst        sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt.gz  wfuzz
root@kali:/usr/share/wordlists# gzip -d rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst     sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt  wfuzz
root@kali:/usr/share/wordlists#
```

NameThatHash (nth)

- To crack a hash, you need to know it's type!
- Most commonly MD5 in CTFs/TryHackMe but don't be surprised if it's something else
- Also now comes as standard with Kali Linux

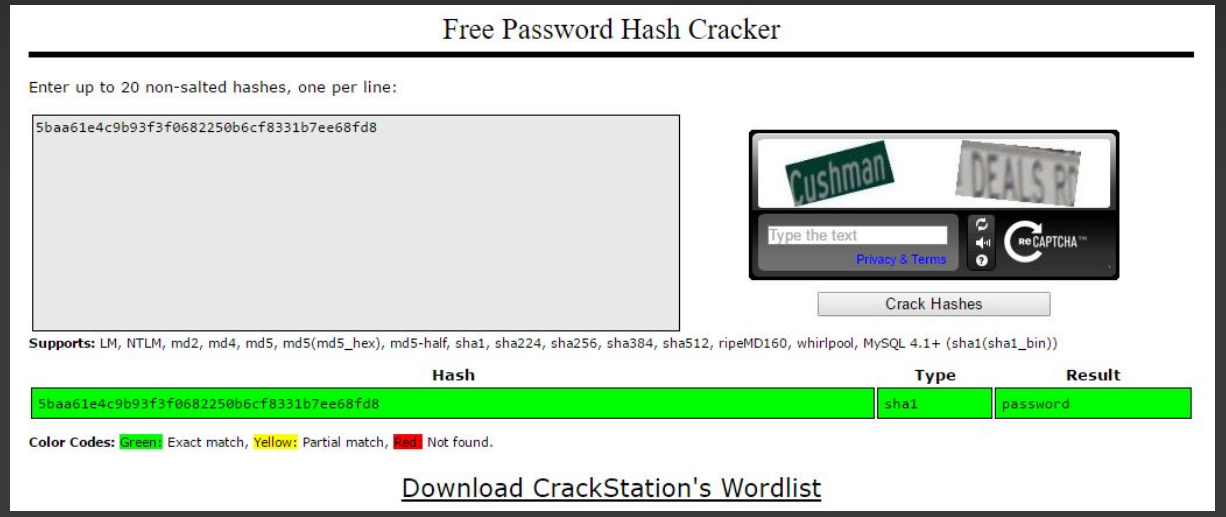
```
871f16813da4f554a8c2dcd8034e1c74d4c58fd246196b1e14b0dc0cbedfadd
5caf651dd8b019afa7414c15c5113eed8d829049b353f63eccdfda8641342e4
09

Most Likely
SHA-512, HC: 1700 JtR: raw-sha512 Summary: Used in Bitcoin
Blockchain and Shadow Files.
Keccak-512, HC: 1800
Blake2, HC: 600 JtR: raw-blake2 Summary: Used in Wireguard,
Zcash, IPFS and more.
Keccak-256, HC: 17800

Least Likely
Whirlpool, HC: 6100 JtR: whirlpool Salsa10, Summary: Not
considered a hash function. Salsa20, Summary: Not considered a
hash function. SHA3-512, HC: 17600 JtR: raw-sha3 Skein-512,
JtR: skein-512 Skein-1024(512),  sha512($pass.$salt), HC: 1710
```

How to crack a hash?

- First port of call - crackstation.net
- A website that supports a wide range of hash algorithms
- Will work especially on common passwords, and saves your own compute power and time



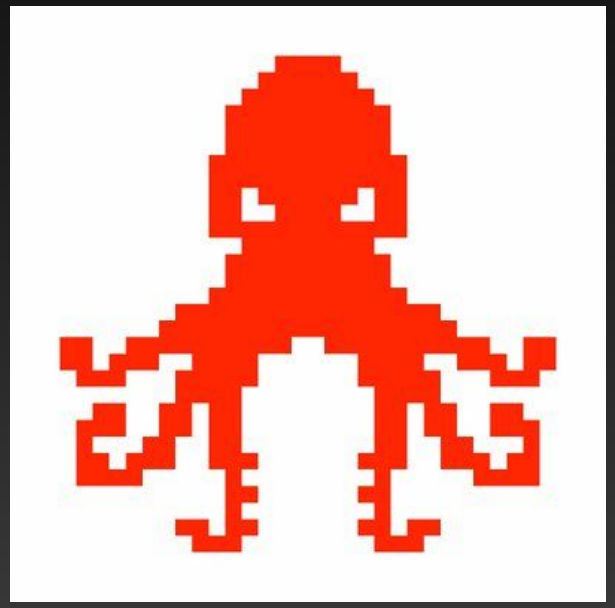
JohnTheRipper

- Password cracking tool
- Purely CPU based - doesn't utilise GPU
- Supports more traditional-types of hash
- BleedingJumbo: Expanded version of john with a wider range of supported hashes

Hashcat

- Another password cracking tool
- Utilises GPU too - can be a lot faster
- Supports a wider range of hashes than John
- Ability to create custom wordlists
- Better documentation available online

Password Cracking



Crack the Hash

https://tryhackme.com/room/crackthehash

Password Cracking

sudo apt install hashcat

Hash Mode Values

Md5 = 0

SHA1 = 100

Decrypt MD5, SHA1, MySQL, NTLM, SHA256, MD5 Email, SHA256 Email, SHA512, Wordpress, Bcrypt hashes for free online

Hash Type Identifier - Identify unknown hashes

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc.

Crack the Hash
https://tryhackme.com/room/crackthehash

Tips:

- Use a tool like Crackstation/CyberChef for the easier tasks
- Hashcat's wiki pages are really handy
- Tab to autocomplete file paths/commands

EXTENSION: Crack the Hash 2
https://tryhackme.com/room/crackthehashlevel2


Le Beaujolais nouveau
est arrivé


OMU
HACKERS