

Part 3: What is Hashing?

Task 3.1: Hash a word by hand (no code for this part!)

First hash function

Replace each letter with its place in the alphabet:

G P N

Now add the numbers together:

Every time we follow this process for the acronym 'GPN', we will get the same number!

Now try hashing this word:

P N G

=

What number did you get? Is this a good thing? What happened here is called a collision!

Second hash function

Now try again but this time multiply the letter's place in the alphabet by its place in the word:

G P N

=

P N G

=

What do you notice?

Hint

You can use the table below to help find what number in the alphabet a letter is:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Task 3.2: Hash your name

Follow the same process as the second hash function and try to hash your name!

★ Bonus 1.4: Does Method 2 always work? ★

Can you find a word that collides with GPN using our second hash function?

Hint

Collision is when 2 different words are hashed to the same number.

☑ CHECKPOINT ☑

If you can tick all of these off you can go to Part 4:

- ☐ Found the hash of GPN and PNG for both methods
- ☐ Found the hash value of your name

Extension 6: Let's get Cracking!

Here is a list of the 10 most common passwords. However, we only have the hashes and forgot to write down what the plain password is! In this part, you will use your python program from parts 0 to 5 to figure what the plain text for each hash is.

Plain text	Username	Hash
	James	b'\x81\xdc\x9b\xdbR\xd0M\xc2\x006\xdb\x81>\xd0U'
	Robert	b"\xad\xffD\xc5\x10/\xca'\x9f\xceuy\xab\xf6o\xee"
	John	b'%\xf9\xe7\x942;E8\x85\xf5\x18\x1f\x1bbM\x0b'
	Joseph	b'\xd5\xaa\x17)\xc8\xc2S\xe5\xd9\x17\xa5&HU\xea\xb8'
	Andrew	b'\xd0v>\xda\xa9\xd9\xbd*\x95\x16(\x0e\x90D\xd8\x85'
	Ryan	b'\n\xcfE9\xa1K:\xa2}\xee\xb4\xcb\xdfn\x98\x9f'
	Brandon	b'\x1b\xbd\x88d'\x82p\x15\xe5\xd6\x05\xedD%"Q'
	Jason	b'vA\x9cXs\r\x9f5\xdez\xc58\xc2\xfdg7'
	Sarah	b'[\xad\xca\xf7\x89\xd3\xd1\xd0\x97\x94\xd8\xf0!\xf4\x0f\x0e'
	Amber	b"_M\xcc;Z\xa7e\xd6\x1d\x83'\xde\xb8\x82\xcf\x99"

Each of these hashes will match one of these plain text passwords:

monkey	11111111	qazwsx	ashley
password	freedom	michael	starwars
	123456789	1234	

Task 6.1: What is the password?

Go back to the website for today's workshop. In your room folder, you should be able to find a text file called `account_info.txt` with the list of the hashes provided above for you to copy and paste into your python program for convenience.

For each hash given above, see if you can use the code you made today to work out the hash of each of the possible plain passwords and match them up!

Once you figure out a username and password pair, try putting it into the Meme Exchange website.