ssh
secure shell

Hashing (SHA256)

```
$ git commit -m "almost done"
[main 211935b] almost done
 1 file changed, 0 files added, ...
$ git log
commit: 211935b0ef003 ..... (40 hex char)
Author: Joe Politz
Date: Wed Oct 15 ...
```

commit hash
- computed from contents of files + commit message

```
$ ssh jpolitz@ieng6.ucsd.edu
The authenticity of host ieng6 cannot be established.
ED25519 key fingerprint is SHA256: 8avDd+O ..... (~40 char)
```

The fingerprint is a hash computed from a public key on ieng6

A hash function takes any data of any size and returns a fixed-size integer.

SHA256 returns a 256-bit integer (32 bytes)

2^{256} is a big number

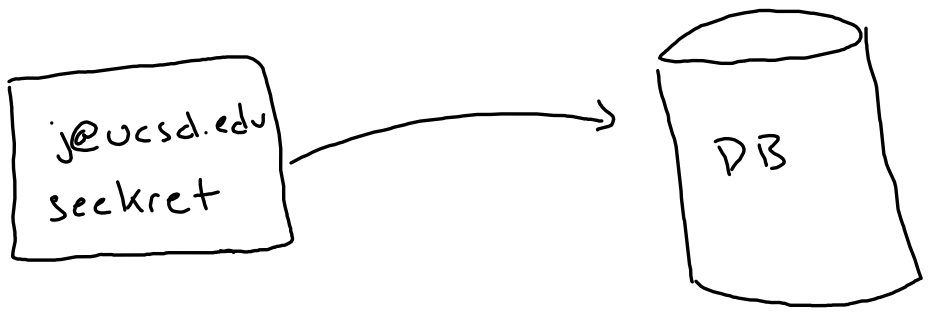
$\sim 10^{77}$ Est. # of atoms in obs. universe $\approx 10^{80}$

A secure/cryptographic hash function:

- deterministic: same input always produces same output hash
- one-way: very difficult to determine input given a hash
- unpredictably distributed: similar inputs produce very different hashes (collision-resistant)

[MD5 is an old, insecure hash function that is not collision-resistant]

Uses:
- identify a large amount of data with a short hash as "id"
- one-way function to avoid storing sensitive data - Passwords!



joe.polite@gmail.com af01123 ...

password cracking

Try all the words in dictionary!

Try all the names on facebook

```
SHA256(char* input, int size, char* hash)
```

any size input
hash this many bytes
32 bytes