combination to check against the obtained hash. md5s can be computed with a modern desktop computer at a rate of millions of passwords per second. There do exist hashing functions made for the sake of password hashing. bcrypt is an example. It's designed to take *longer* as computers become more powerful (not in actual time, but more time relative to computer strength). This is acceptable for a user login form, because the web server only needs to compute a single password when a user logs in, while a brute-forcer needs to compute billions. Fifty extra milliseconds is negligible when a user logs in, but it makes brute-forcing effectively impossible.

The other problem with md5 is that it's well-known. There exist databases called 'rainbow tables' that attempt to index *every single md5 hash* along with its original text. They obviously can't feasibly have too many entries, because there are a *lot* of possibilities, but they are definitely effective.

The primary counter to this is to use salts. When you salt a hash algorithm, you provide additional information (sometimes just by appending it to the plaintext) to add more entropy to the hash. If you store a random number along with the user's account information, you can use that number as a salt. Now, a rainbow table is useless with all these new possible values. Brute-forcing takes the same amount of time, but rainbow tables become pointless.

bagels are yummy

Commentary on Silas:

I was in a creative fictional writing sort of mood, but I've never been very successful at coming up with ideas for my writing. I had the idea to use a character that I already invented for the story, which made things a lot easier.

This character (the narrator) is a character that I roleplayed last year in a *Dungeons and Dragons* campaign. He went through a lot, and this entry in my writer's notebook was an attempt to start to chronicle his experiences. The start of the story picks up where the campaign left off, but the extensive flashback already happened in the campaign. The idea was that if I could write out what had already happened from my character's viewpoint, I'd be able to get into the 'mood' of writing as the character.

I'll warn you now that I never actually finished "Silas". I discovered shortly after writing this that I don't actually like to write fiction. The portion of the flashback that I wrote about is only the beginning of a *very* long journey that our characters went through. Keep in mind that we would meet for three hours every Tuesday night, and this campaign ran for about a year. We had covered a *lot* of ground. I intended to continue entries every few weeks, picking up where I left off each time. That never happened.

Part of the discovery of my dislike of fiction (or, at least, writing it) was that I found out that I'm actually terrible at writing fiction. My word choice in the first few paragraphs is painfully excessive, and I didn't actually notice when I was writing it. I'm disturbed to think of what could have happened if I had let myself continue to write for too long.

Writer's Notebook: Silas 31 October 2012

I woke up and the thought had really sunk in. I unclenched my fingers and spread the crumpled newspaper I was holding onto the mahogany floor. I performed for myself a little jig and