Commentary on RSA Encryption:

If you're not looking to read about Internet security, you can go ahead and skip this section.

I really like 'teaching' things in my writing. Most of the thought that I do is prompted by explaining concepts to others, or at least to imaginary friends. The problem with this is that if I'm in the middle of teaching something to someone and I suddenly make new revelations, they get angry with me for interrupting the instruction. This is why imaginary stupid people are useful. I can explain things to them all day and they never get annoyed.

"RSA Encryption" is about RSA encryption (duh) in specific, which allows for secure communication on the Internet. It's pretty cool, which is why I wrote about it. The math for it is even cooler. Something I really like about the collection of writer's notebook entries that I have collected over the course of the school year is that I can use these documents to explain concepts to people. I normally don't write guides of this nature because I don't like writing in general. When I'm forced to write, though, it makes perfect sense to write about something that interests me. I've successfully explained RSA encryption, SQL injection, and a few other concepts by pasting writer's notebook entries.

Writer's Notebook: RSA Encryption 22 December 2012

I survived the end of the world, so I suppose I need to finish writing my pages. People always get annoyed when I explain security concepts to them. Part of the reason is that I tend to interrupt myself a lot, going deeper and deeper into a topic.

You're essentially obligated to read this, though. So... HA!

I'd like to write about public- and private-key encryption.

RSA encryption is all about communication. There are primarily two factors to secure communication:

- Privacy, which ensures that only the intended recipient can read the message.
- Authentication, which allows the recipient of a message to verify the sender's identity.

RSA provides both of these, and is very simple to use. I'm not going to write down the intricacies of the math, because I don't actually have them memorized. They're very cool, though, and are accessible on the Internet.

To use RSA encryption, you must have two *keys.* The keys are intertwined, and they are dependent on each other. It is not possible, however, to find one key with only the other.

These keys can be represented in a few different ways. In reality, they're just really large strings of ones and zeroes. *Anything* on a computer can be represented like that, of course. The keys can also be expressed as long numbers, or hexadecimal numbers, or base-64 numbers. It doesn't really matter how the keys are expressed, but in reality they're nothing more than large numbers.

The two keys are *public* and *private* keys. Predictably, the public key is meant to be shared with the public. The private key is only meant for the person who generated the keypair.

When a 'message' (which is also converted into a number) is encrypted with a public key, the ciphertext can only be decrypted with the corresponding private key. In the same way, a message encrypted with a private key can be decrypted only with the corresponding public key.

This is a basic principle in RSA encryption, but it is very powerful. I'll use Alice and Bob as