

Hell, why not have a key party? That's what they did in *Little Brother*. And it worked!

As long as you have a *trusted* network of people, you can later exchange keyrings with others over the Internet. If Bob went to a party and got Carol's public key, Alice can receive Carol's public key (assuming Bob has good intentions) through an already-secure channel that's been established with Bob.

At a workplace, if all of the local computers are trusted, they can share keys with each other. This is used often in practice, especially when sending email. Email is an insecure protocol, and anyone can pretend to be anyone else (sometimes I pull *hilarious* (trust me) pranks using this concept). RSA encryption allows people using email to verify others' identity. RSA is also used in https and SSH. It's pretty widespread, and I love it.

There you have it.

### Writer's Notebook: Acronyms

13 January 2013

I like coming up with acronyms for things. Acronyms help me remember things, and they're often pretty funny. Sometimes I'll have problems keeping track of items I'm trying to recall. A nice jog of my memory is all it takes to fetch the information.

Take the eight characteristics of life as an example:

- |                        |                          |
|------------------------|--------------------------|
| - adaptation over time | - made up of cells       |
| - reproduction         | - growth and development |
| - homeostasis          | - responds to stimuli    |
| - uses energy          | - exhibits organization  |

I wanted to remember these characteristics.

Do you think that I'll ever forget that CHAD is SORE?

I'll spell it out for you, in case you don't get it...

cells/homeostasis/adaptation/development/stimuli/organization/reproduction/energy

It's as simple as that.

I also like SNORF for the Enlightenment. FRONS works, too, but SNORF sounds funnier.  
secularism/naturalism/optimism/rationalism/freedom

Our Biology teacher gave us "CHNOPS" to remember the six elements that are important in organic compounds. If you allow me to repeat oxygen, I can give you

PONCHOS.

Beat that.

No, really. Try it. It's fun.

### Reflection on Acronyms

Try it for yourself. Mr. Petrushun did. He wrote:

"SCHNOP... just sounds funny.                      like quickly skidding towards a stop."

I made it through a lot of the school year using acronyms. It's surprising how helpful they really are, and you don't realize it until you really think about it. I've scribbled more of these silly acronyms in the margins of my tests than I can count. It's frustrating to know that though my mind has all of this information, I can't retrieve it until I enumerate it or assign letters to it. Unless I can count on my hand which terms I've already used, and assign each one to a number, I have a lot of trouble remembering things. For the same reason, I couldn't tell you the name of each person in any of my classes. Brains are funny that way.