Lab session 1. Public key generation and web of trust building

HEY, I JUST GOT HOME FROM THE PARTY
THE ONE WITH THE IRC FOLKS?
YEAH.
HOW WAS IT?
GOT TOO DRUNK. I SCREWED UP, BAD.
WHAT HAPPENED?
THERE WAS A GIRL. NO IDEA WHO SHE WAS. DON'T EVEN KNOW HER NAME. I WAS TOO DRUNK TO CARE.
AND WHAT, YOU SLEPT WITH HER?
NO.
I SIGNED HER PUBLIC KEY.
SHIT, MAN.

(xkcd.com)

OpenPGP (PGP=`Pretty Good Privacy') is common asymmetric encryption standard and GnuPG is an application of OpenPGP used for encryption and digital signature of messages. At the Friday Lab session (bring your laptop):

1. (Preparation; you can do this step ahead of time already:) Install a PGP tool (see eg GnuPG) and generate a public key.
2. Bring your key and get some signatures from others; thus creating a web of trust spanning the class.
3. Test it by sending a signed file. Check a signature for a key you have and one for which you don't to see the difference.
4. Test it by sending an encrypted file. Try decrypting a file made for you / not made for you to see the difference.

Background information: http://cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html