GNU Privacy Guard: A CompSoc guide to daily use of email encryption

Mac Edition

Martin Dehnel
James Fielder
(Durham University)

May 2012

What is GPG?

GPG, or The GNU Privacy Guard is, in a nutshell, *a free and easy way to send and receive emails securely*. The way most emails are currently sent is completely insecure, and is directly analogous to sending all of your mail on a postcard, available for any postman or eavesdropper along the way to read: we don't think this is good enough, and want to encourage more people to care about their privacy.
GPG allows you to send **completely secure** emails to anyone else with an email address and a key.

How does it work?

To make sure that only the intended recipient can read the email you've sent them, you need to encrypt the message. This will mean that to anyone without the right password (or 'key') the message will look like undecipherable random noise. As you may not have ever met the person you're emailing, you probably won't have a way of agreeing a password (key) together without the possibility that someone else could have intercepted it. Instead, conceptually, you create an electronic padlock and key. You can't send anyone a copy of the padlock's key over the internet as someone could copy it, but instead you can send out an unlocked padlock to anyone who wants to send you an email; this way they can 'lock' (encrypt) the message with the padlock, but can't 'unlock' (decrypt) it – only you, the person with the key can do that.

- Test Item
- two and
- three