IS-521 Activity **PGP**

Due Date: March 13, 2017 (before class)

1 Activity Overview

In this activity, we learn how to securely encrypt your files and personal emails with PGP. We are going to use GnuPG, an open-source implementation for PGP.

2 PGP Key-Signing Party

The goal of this exercise is twofold: (1) students get to know each other; (2) students establish the web of trust using GPG.

1. Create a PGP key of your own with GPG.
2. Push your public key to our web page (by opening a pull request).
3. Meet your colleagues and exchange your public keys.
4. A student who gets the most signatures will get an extra point (+1).
5. You can also ask course staffs to sign your key.

3 Ethical Conduct Agreement

Git allows us to sign tags and commits with your PGP key. Read this web page [**?**] and configure your PGP key with Git, and follow the steps below.

1. Fork the repository at `https://github.com/KAIST-IS521/Agreement`.
2. Modify the `Agreement.md` file appropriately: correct the date and the name.
3. Commit and push your modification.
4. Tag your commit with "Agreement".
5. Sign the tag, and push it.
6. Open a pull request.

4 Sending an encrypted E-mail

In this exercise, your goal is to send an email that is signed by your private key and encrypted by professor's public key. The content of your email should contain the following line:

`Your Name, Your GitHub ID, Your Student ID`

. Your email should be sent to is521-staff@softsec.kaist.ac.kr.