Guide to Homework submission Introduction to Cryptology (2WF80)

Setting up PGP

1. To be able to receive encrypted email, each of you has to generate a public-private key pair.
   One way to do this is to use thunderbird email client (this is what we recommend).
   If you want to use outlook, there are several guides online, using tools like e.g., Kleopatra and gpgwin.
   Here are example **guides**, but you can use whatever works.

- https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq
- https://www.comparitech.com/blog/information-security/pgp-encryption-with-outlook/
- https://www.comparitech.com/blog/information-security/pgp-encryption-gmail/

2. **Check that it works**. Import your teammembers public keys and try to send an encrypted message. This will save you the trouble of debugging as the deadline approaches. Check if you can decrypt the received message and if the signature is there.
3. Share the public keys with the TA's along with your first submission
4. keep the private key file, you will need it to sign and to decrypt.

Submission Checklist

1. Check your submission: check that you are using the correct pdf, and that all teammates names are on the pdf.
2. Use a useful filename. This should include the number of the homework, and ideally one or all of your group's last names. This ensures that there are no mixups between groups, and makes it clear who contributed.
3. cc **all** your teammates when drafting your email.
4. make sure you have the correct email addresses and import the public keys of the TA's (check the course website)

5. encrypt to all TA's using your preferred method. If you are using thunderbird, just click the button on top.
6. If your public key has changed, **let us know**.
7. Make sure each teammember submits at least one homework to get the bonus.
8. Make sure the attachment is included and that attachments are encrypted (this should be enabled by default).

What not to do

1. Send multiple submissions. If you do, we will grade the first submission.
2. Change your public key without telling us.
3. Use MS Outlook email encryption. This is not the same as PGP and will not be accepted.
4. Change team members without informing us.
5. Submit by yourself. Please find a group.

Feedback

You will receive your feedback as an encrypted email, so make sure your submission includes your public keys.