**Lab 4. Digital Certificates**

I recommend using the Windows 10 VM for this lab. Alternatively, you can install GPG on Windows (https://www.gpg4win.org/) or Mac (<https://gnupg.org/download/>). I list several resources at the end of this document that may be helpful for you.

**Part 1**

**Part 1a. Sign the public keys from the key signing party**

1. If you haven’t already done so, download the class PGP keyring [here](http://community.mis.temple.edu/mis3507001fall2018/files/2018/09/PGP-Keyring-MIS3507-2018.asc), and import the keyring into your PGP client.
2. For each identity you verified during the key signing party (i.e., you witnessed the person show his/her Temple or government ID and attest that his/her fingerprint was correct), sign that person’s PGP key.
3. Upload each public key you sign to a public key server so that others can see that you trust the key.

**Question**: What are the names, email addresses, and PGP fingerprints or key-ids of the three people whose keys you signed?

**Part 1b. Upload your PGP key to a key server**

1. Ensure that your public key is uploaded to a PGP key server like [keys.gnupg.net](http://keys.gnupg.net/). (In Kleopatra, you can upload by highlighting your key, right-clicking it, and selecting export certificates to server.)
2. Ensure that your public key is available on public key servers has been signed by at least three members of the class. To do this, you can re-download or refresh your public key from the key s

**Question**: What is your PGP key or fingerprint?

**Question**: What are the names, email addresses, and PGP fingerprints or key-ids of the three people who signed *your key*?

**Part 1c. Send and receive an encrypted email via PGP**

Send an **encrypted and signed** message using your PGP key to anthony@vance.name. You will receive a response encrypted with your key which contains a secret code. Use this code to answer the question below.

For Windows users, I recommend you use GPA (gnu-privacy-assistant), which is installed on the Windows 10 VM to complete this section. GPA has access to the same keyring on your machine as does Kleopatra. For Mac users, I recommend using GPG Tools and Apple Mail.app.

If using the Windows 10 VM, follow these steps:

1. Launch GPA on the Windows 10 VM. It opens with the Clipboard view.
2. In this view, type a message for Dr. Vance.
3. Click “Encrypt”. Choose at least the public key for anthony@vance.name.
	* If you also want to be able to decrypt what you encrypt, then also select your public key.
4. Check the box for Sign. Select with which key you will sign the message.

**Note**: If you are curious what a signed-but-not-encrypted message looks like, write a message, then press the “Sign” button within GPA. Observe the result—the original message in plaintext, and a block with a signed hash. If you applied your public key to this signed hash, you would obtain a hash against which you could compare your own hash of the plaintext.

1. Copy-paste the output of the previous step into whatever email provider you use (e.g., TU Mail or Gmail.com).

**Important**: Send it from an email address associated with your PGP public key.

1. If you encrypted and signed your message, then you will receive an encrypted response back, encrypted with your public key. Decrypt this response using GPA clipboard. This response is the answer to the next question in this lab.

**Question**: What is the code that you received from the encrypted message you received back from me?

**Part 2. PGP Web of Trust vs. the X.509 Model**

Read [the following article](https://en.wikipedia.org/wiki/Web_of_trust).

**Question**: Compare and contrast the trust models used by PGP public key versus X.509 certs used by websites.

**Part 3. Communicate Securely with Signal**

1. Read about WhisperSystem’s Signal app [here](https://theintercept.com/2017/05/01/cybersecurity-for-the-people-how-to-keep-your-chats-truly-private-with-signal/) (watch the video) and [here](https://signal.org/).
2. Read about the cryptographic primitives that Signal uses [here](https://medium.com/%40justinomora/demystifying-the-signal-protocol-for-end-to-end-encryption-e2ee-ad6a567e6cb4).

**Question**: What attacks does Signal protect you against? Which does it not protect you against?

**Question**: At a high level, how does the Signal protocol work?

1. Install the app “Signal” on an iOS or Android device (if you don’t have an iOS or Android device, borrow one from a friend). Ask a partner (friend or classmate) to do the same.
2. Verify the Signal safety numbers of your partner (refer back to the video you watched [here](https://theintercept.com/2017/05/01/cybersecurity-for-the-people-how-to-keep-your-chats-truly-private-with-signal/) at the 1:55 mark).
3. Using Signal, call or send a text message to your partner.
4. How does your experience using Signal compare to using encrypted email with PGP and S/MIME?

**Question**: How does your experience using Signal compare to using encrypted email with PGP?

**Resources**

Below are some resources if you would like more help.

* Using PGP with Windows with Thunderbird and Enigmail: <https://ssd.eff.org/en/module/how-use-pgp-windows>
* <https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages>
* For Signal for Android: <https://ssd.eff.org/en/module/how-use-signal-android>
* For Signal for iPhone: <https://ssd.eff.org/en/module/how-use-signal-ios>

**Lifelong Learning**

To learn more about cryptography, the following are some of the best and most readable books.

|  |  |
| --- | --- |
| Macintosh HD:Users:anthony:Desktop:51RRKXRP0RL._SY346_PJlook-inside-v2,TopRight,1,0_SH20_.jpg | “The Code Book” by Simon Singh.This is a very interesting and gripping book about the history and intrigue of cryptography and cryptanalysis.Available at [Temple Library](https://librarysearch.temple.edu/catalog/991004378459703811) Amazon: <http://amzn.com/0470474246> |
| Macintosh HD:Users:anthony:Desktop:41Tuv9saPgL._SY346_PJlook-inside-v2,TopRight,1,0_SH20_.jpg | “Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age” by Steven Levy.A very engaging look at the modern history of cryptography, including the development of DES, RSA, and PGP. Also, it describes the fight in the 1990’s to legalize the use of strong cryptography.Available at [Temple Library](https://librarysearch.temple.edu/catalog/991013963759703811)Amazon: <http://amzn.com/0140244328> |
| Macintosh HD:Users:anthony:Desktop:51oEJqoe5RL._SY346_PJlook-inside-v2,TopRight,1,0_SH20_.jpg | “The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet” by David Kahn.The bible of the history of Crytography. A deep dive (at 1,200 pages) but still readable.Amazon: <http://amzn.com/0684831309> |
| Macintosh HD:Users:anthony:Desktop:41bQahpPfJL.jpg | “Cryptography Engineering: Design Principles and Practical Applications” by Niels Ferguson, Bruce Schneier, Tadayoshi “Yoshi” Kohno.The updated successor to the classic “Applied Cryptography” by Bruce Schneier. This book explains how modern crypto works and how to implement it in your systems. Amazon: <http://amzn.com/0470474246>  |