**Public-Key Infrastructure Lab**

1. **Overview**

Public-Key Cryptography (PKI) is the foundation of modern digital communication. The problem is that there is no easy way to verify the ownership of a Public-Key. This lab is designed to demystify PKI and give students first-hand experience using PKI to send and receive encrypted digital messages and files. This lab covers the following topics:

* Public-Key
* Private-Key
* Public-Key Infrastructure (PKI)
* Publishing a Public-Key to a key server
* Validating a Public-Key
* Encrypting a message using an individual’s Public-Key
* Decrypting a received message using your Private-Key

**Learning Objectives**

Students should be able to gain a better understanding of how PKI works and how it can be appropriately implemented and used to secure enterprise environments.

**Readings**

Additional detailed information about PKI can be found in the following:

* Chapter 7 – Cryptography and PKI in your TestOut e-book.
* Supplemental materials provided by your instructor.

**Related Labs**

None

**Lab Environment**

This lab has been tested using the environment listed below. Any variation outside this environment may cause certain aspects of this lab to not perform as indicated or desired.

* A Windows, macOS, or Chromebook laptop, or desktop computer.
* An e-mail account using Google’s webmail platform G-Mail[[1]](#footnote-2).
* The Firefox[[2]](#footnote-3) web browser.
* The Mailvelope extension.
* An Internet connection.

*Ensure that you have created and/or logged into your G-Mail account before starting section two of this lab.*

**Read Ahead**

You are required to submit a lab report for this lab. Read section three of this lab, review the requirements, you may need to take screenshots throughout each of the tasks in section two.

1. **Lab Tasks**

The following tasks and corresponding screenshots were written using the Firefox web browser and Google’s webmail platform G-Mail. Deviation from the lab environment listed above is not recommended and may require outside research to complete this lab’s tasks.

* 1. **Task 1: Installing Mailvelope**

In this task, we are going to install the Mailvelope extension on the Firefox web browser.

1. Open the Firefox web browser.
2. Click the sandwich  icon located on the upper right of the Firefox browser window.
3. Click "Settings" from that menu; the "Settings" tab will appear.

Graphical user interface, application

Description automatically generated with medium confidence

1. Click on the puzzle-piece icon "Extensions & Themes" located on the lower left of the "Settings" tab; the "Add-ons Manager" tab will appear.



1. In the "Add-ons Manager" tab, type “Mailvelope” into the "Find more add-ons” search box.

A picture containing text

Description automatically generated

1. From the search results locate and click on Mailvelope, then click the “Add to Firefox” button to install the add-on.

Graphical user interface, text, application

Description automatically generated Graphical user interface, text

Description automatically generated

1. When prompted click the “Add” button to grant permission to the Mailvelope extension.

Graphical user interface, text, application, email

Description automatically generated

1. Click the checkbox to permit Mailvelope in private windows, then click the “Okay” button.

Graphical user interface, diagram, text, application, email, website

Description automatically generated

1. Return to the "Add-ons Manager" tab. Ensure that the Mailvelope extension is turned on.

Graphical user interface, text, application

Description automatically generated

1. Locate the Mailvelope  icon located on the upper right of the Firefox browser window and click it to reveal the Mailvelope menu; click the “Let’s start!” button.

Diagram

Description automatically generated

* 1. **Task 2: Setup Mailvelope**

In this task, you are going to set up the Mailvelope extension. You will start by generating a public/private key pair. Then you will validate your Public-Key by decrypting the e-mail sent to your G-Mail account by the Mailvelope key server. You will then export and upload your Public-Key to one (1) additional key server. Finally, you will export your public/private key pair to protect your keys from loss or corruption.

1. Click on the “Key Management” tab in Mailvelope. On the “Setup” screen, click the “Generate Key” button.

Graphical user interface, text, application, email

Description automatically generated

1. On the “Generate Key” screen fill in the following information:

**Name:** Your Full Name

**Email:** Your G-Mail address.

**Password:** This is used to protect your Private-Key, ***DO NOT FORGET IT!***

Graphical user interface, text, application, email

Description automatically generated

Ensure the “Upload public key to Mailvelope Key Server” checkbox is selected. Then click the “Generate” button, then wait while your key pair is generated.

Graphical user interface, text, application, email

Description automatically generated

1. Upon successful key generation, you will be taken back to the “Key Management” screen in Mailvelope. Your new key will be listed with your name, e-mail address, the key’s identifier, and the key’s creation date.

Graphical user interface, application

Description automatically generated

1. On the “Key Management” screen in Mailvelope, click on the right arrow next to your public/private key pair. You will be taken to your key pair details. If you see the message, “The key is not synchronized with the Mailvelope key server.” Click the “Synchronize” button.

Graphical user interface, application

Description automatically generated

1. There should be a confirmation e-mail from Mailvelope3[[3]](#footnote-4) in your G-Mail inbox. This e-mail is encrypted and will look similar to the screenshot below. This e-mail contains a link to confirm your e-mail address.

A picture containing graphical user interface

Description automatically generated

1. From your G-Mail inbox, click on the e-mail from Mailvelope. You will be prompted in a separate window to enter your password; enter the password for your Private-Key that you generated in step two above. Then click the “OK” button.

Graphical user interface, text, application, chat or text message

Description automatically generated

1. Click the hyperlink from the decrypted e-mail to validate your e-mail address and to have your Public-Key listed on Mailvelope’s global key servers.

Graphical user interface, text

Description automatically generated with medium confidence

A successful message from the “Mailvelope Key Server” looks like this.

Graphical user interface, text, application

Description automatically generated

1. Return to your key pair details on the “Key Management” screen in Mailvelope. You should now see the message, “The key data on the Mailvelope server is up to date.”

Graphical user interface, application

Description automatically generated

1. From the key pair details screen in Mailvelope, click the “Export” button.

Graphical user interface, application, email, website

Description automatically generated

1. On the Export Key screen, ensure “Public” is selected and click the “Save” button. Then click the “Close” button. This will save your Public-Key to your downloads folder with the name of <key name>\_pub.asc.

Graphical user interface, text, application

Description automatically generated

1. Open a new Firefox tab and go to https://keys.openpgp.org. Then find and click on the upload hyperlink.

Graphical user interface, text, application, email

Description automatically generated

1. From the “Upload your key” screen on *keys.openpgp.org*, select the Public-Key you exported in step ten and click the upload button.

Line chart

Description automatically generated with low confidence

1. You will receive notification that a key with the cryptographic fingerprint was uploaded to the key server. To make this key searchable by your identified e-mail address, click the “Send Verification Email” button.

Graphical user interface, text, application, email

Description automatically generated

1. Click the verification hyperlink sent to your e-mail address, to receive a confirmation message that your key has been published with your e-mail address.

Graphical user interface, text, application

Description automatically generated

1. To make a backup of your public/private key pair, repeat steps nine – ten selecting “All” followed by the “Save” button. This will save your public/private key pair to your downloads folder. Keep this key pair in a safe place.
   1. **Task 3: Sending An Encrypted E-Mail**

In this task, you are going to search for your instructor’s Public-Key on one of the two key servers that were used in this lab. Then you will send them an encrypted e-mail. You will collect your instructor’s response and include it in your lab report.

1. Click on the “Options” tab in Mailvelope. Then select the “Gmail API” located on the left of the screen. Click the slider-switch to enable “Gmail API Integration”.

Graphical user interface, text, application

Description automatically generated

1. Return to your G-Mail inbox, and click the Mailvelopeicon located on the left above your inbox.
2. When you click the Mailvelope icon in G-Mail, you will receive an error screen in a pop-up window.

Graphical user interface, text, application, chat or text message

Description automatically generated

1. On the “Key Management” screen in Mailvelope, in the “Using the Gmail API” window, authorize the use of the API by clicking the “Sign in With Google” button.

Graphical user interface, text, application, email

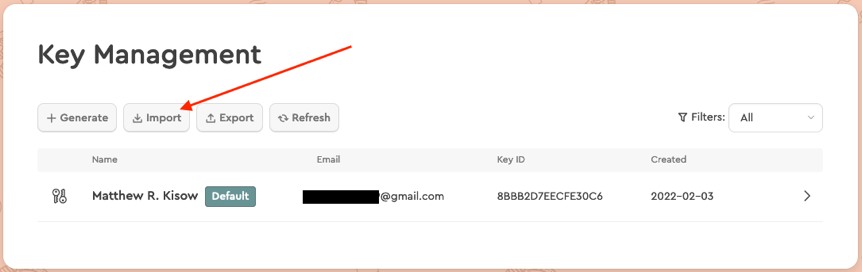
Description automatically generated

1. After providing your G-Mail credentials, click the “Allow” button to permit Mailvelope access to your G-Mail account. For now, you can close the “Mailvelope – Compose Secure Email” pop-up window.

Graphical user interface, text, application, email

Description automatically generated

1. On the “Key Management” screen in Mailvelope, click on the “Import” button.



1. On the “Add Keys” screen in Mailvelope, click the “Search” tab. Then verify that the “Key server” listed under the search box defaults to *keys.mailvelope.com4*[[4]](#footnote-5). In the search box, type in your instructor’s e-mail address, then click the “Search” button.

Graphical user interface, text, application

Description automatically generated

From the “HPK key server” drop-down list, find and select *keys.mailvelope.com*, then click the “Save” button. Once the key server has been updated, return to step two above.

*Graphical user interface, application, email

Description automatically generated*

1. If the search is successful a new web browser tab “Mailvelope Key Server” will open. Click the key to import it into the Mailvelope keyring.

Graphical user interface, text, application

Description automatically generated

1. On the “Confirm Key” screen, click the “Confirm” button to finish importing your instructor’s Public-Key.

Graphical user interface, text, application

Description automatically generated

1. After the key import, you will be returned to the “Key Management” screen in Mailvelope. Your instructor Public-Key will be displayed, note the icon indicating this is only one key in the key pair.

Graphical user interface, application

Description automatically generated

1. Return to your G-Mail inbox and click the Mailvelopeicon. The “Mailvelope – Compose Secure Email” pop-up window will open. In the recipient box type your instructor’s e-mail address, a completion box should appear with their Public-Key ID.

Graphical user interface, text, application, email

Description automatically generated

1. Compose your message per your instructor’s requirements, then click the “Submit” button. You will receive an encrypted reply from your instructor.

Graphical user interface, text, application, email

Description automatically generated

1. **Submission**

You need to submit a detailed lab report with screenshots that describe what you have done and what you have observed. You will also need to provide a narrative that explains your observations, particularly anything that you found interesting or surprising.

At a minimum your lab report must include:

* A cover page.
* A summary paragraph that describes your experience using PKI.
* A narrative of your observations, noting any findings you found interesting or surprising.
* A screenshot of your public/private keypair from the Mailvelope Key Management tab.
* Screenshots from *keys.mailvelope.com* and *keys.openpgp.com* that show your Public-Key’s listed on these two (2) key servers.
* A redacted screenshot of the backup of your public/private key pair.
* A copy of the decrypted e-mail that your instructor sent you.

This report should be written in Microsoft Word. The title page should include the name of the lab, your name, class number and section and, the date.

Send your lab report in an encrypted e-mail to your instructor.

**Rubric**

|  |  |  |
| --- | --- | --- |
| **X** | **POINTS** | **REQUIREMENT OR LEARNING OBJECTIVE** |
|  | 5 | Cover Page |
|  | 20 | Summary paragraph that describes students experience using PKI |
|  | 20 | Narrative of the students observations and findings |
|  | 5 | Screenshot of the students public/private key pair |
|  | 5 | Screenshots from the two public key servers |
|  | 5 | Screenshot of the backup of the students redacted public/private key pair |
|  | 10 | A copy or screenshot of the decrypted e-mail that was sent from the instructor to the student. |
|  | 5 | The lab report was written in Microsoft Word or equivalent format |
|  | 5 | The lab report title page has all requested information |
|  | 10 | There are no spelling or grammatical issues |
|  | 10 | The report was sent to the instructor in an encrypted e-mail. |

1. *The Mailvelope web browser extension is designed to work with different webmail platforms. This lab was written using G-Mail and is the preferred webmail platform for this lab. If you do not use G-Mail you can sign up for a free account by visiting https://gmail.com, and clicking on the “Create Account” hyperlink.* [↑](#footnote-ref-2)
2. *This lab was written using the Firefox web browser and it is the preferred web browser for this lab.* [↑](#footnote-ref-3)
3. *If you have more than one e-mail from Mailvelope, only click on the most recent one. If you are redirected to a page that states “User ID not found” follow the link from the other e-mail.* [↑](#footnote-ref-4)
4. *If the key server has not defaulted to keys.mailvelope.com, click the “Change” hyperlink and follow the instructions below to change it to the proper key server.* [↑](#footnote-ref-5)