

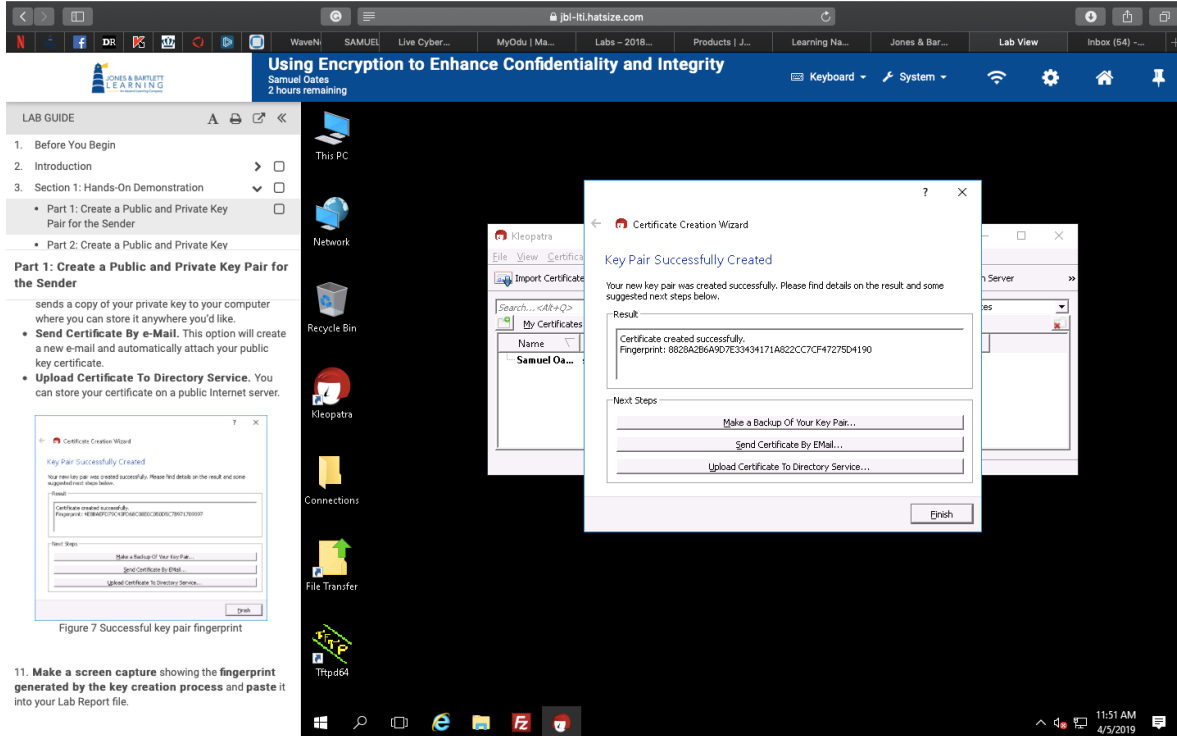
Samuel Oates

IT-315

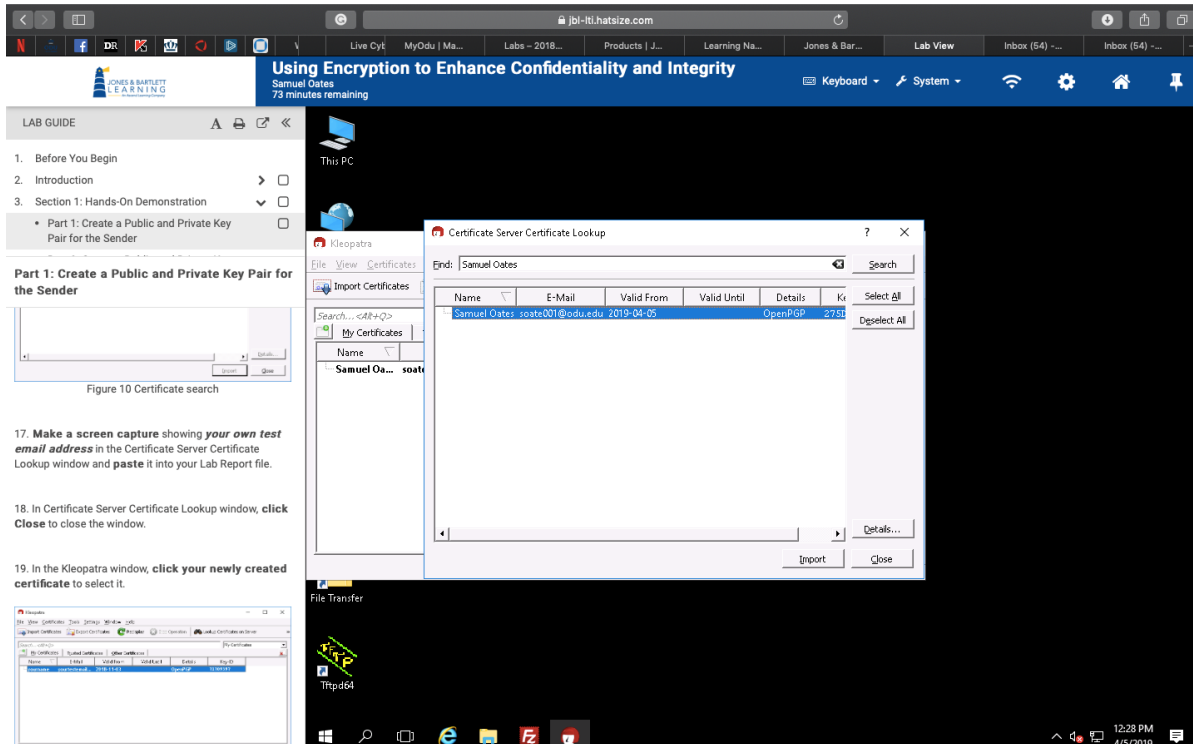
4/5/2019

Hands on # 7

Generated by the key creation process



Your own test email address



## Kleopatra decryption results window

The screenshot shows a virtual machine desktop with a taskbar containing icons for This PC, Tftp64, Network, TargetWin..., Recycle Bin, TargetWin..., secret-message - Notepad, FileZilla Server..., Kleopatra, putty, Mozilla Firefox, and secret-mes... The desktop background is dark. A window titled "Decrypt/Verify Files" is open, displaying "Results" and "All operations completed." with a progress bar at 100%. Below the progress bar, a message states "secret-message.txt.gpg -> secret-message.txt: Decryption succeeded." There is a checkbox for "Keep open after operation completed" which is checked. Buttons for "Back", "OK", and "Cancel" are at the bottom. In the background, a Notepad window is open with the text "I like information systems security" and "Samuel".

## Fingerprint generated by the key creation process

The screenshot shows the Kleopatra application interface. The main window displays a table of certificates under the "My Certificates" tab. A "Certificate Creation Wizard" dialog box is open, titled "Key Pair Successfully Created". The dialog contains the following text: "Your new key pair was created successfully. Please find details on the result and some suggested next steps below." Under the "Result" section, it says "Certificate created successfully. Fingerprint: 14643485E67618E9189F91DAE3D09A0538E2735E". Under the "Next Steps" section, there are three buttons: "Make a Backup Of Your Key Pair...", "Send Certificate By EMail...", and "Upload Certificate To Directory Service...". An "Finish" button is at the bottom right of the dialog. The background shows the Kleopatra application window with a menu bar (File, View, Certificates, Tools, Settings, Window, Help) and a toolbar with buttons for Import, Export, Redisplay, Stop Operation, and Lookup Certificates on Server. The application window also shows a table of certificates with columns for Name, E-Mail, Valid From, Valid Until, Details, and Key-ID.

## Your own email address

**LAB GUIDE**

4. Section 2: Applied Learning

- Part 1: Create a Public and Private Key Pair
- Part 2: Import Another Private Key
- Part 3: Decrypt a File with the Imported Certificate

**Part 1: Create a Public and Private Key Pair**  
your name and email address are visible in their entirety.

Figure 31 Certificate search

9. Make a screen capture showing **your own email address** in the Certificate Server Certificate Lookup window and paste it into your Lab Report file.

10. Close the Certificate Lookup.

11. Select your certificate, then select File > Export Secret Keys and save your private (secret) key to the Workstation desktop as DesktopKey-private.gpg.

Recent Windows Defender Summary  
No threats were found since your last summary. Your PC was scanned 2 time(s).

## Certificate Details (I already past the trust options) (Showing the trust has been done)

**LAB GUIDE**

Pair

- Part 2: Import Another Private Key
- Part 3: Decrypt a File with the Imported Certificate
- Part 4: Encrypt a Reply Using the Imported Certificate

**Part 2: Import Another Private Key**

3. Change the Trust Level for this certificate.

Notice that only the This is my certificate option is available. This is a private key created by the workstation, so this is the correct option.

Figure 34 Trust imported certificate

4. Make a screen capture showing the Certificate Details for the student certificate and paste it into your Lab Report file.

# Kleopatra decryption results window

The screenshot shows a Windows desktop environment. At the top, a web browser displays a page titled "Using Encryption to Enhance Confidentiality and Integrity" by Samuel Oates, with 48 minutes remaining. The page includes a "LAB GUIDE" with four parts: 1. Create a Public and Private Key Pair, 2. Import Another Private Key, 3. Decrypt a File with the Imported Certificate, and 4. Encrypt a Reply Using the Certificate. The third part is currently active. Below the lab guide, a file explorer window shows the contents of a folder named "Key". A Kleopatra "Decrypt/Verify Files" window is open, showing a progress bar at 100% and a message: "All operations completed. Secure\_note.txt.gpg -> Secure\_note.txt: Signed by jbl\_student@securevcenbriq.net". A Notepad window titled "Secure\_note - Notepad" is also open, containing the text: "Please send a reply with your contact details. Name: Samuel Oates Email: soate001@odu.edu". A small inset image shows a window arrangement for screen capture.

Figure 35 Window arrangement for screen capture (secure\_note contents redacted)

5. Make a screen capture showing the Kleopatra decryption results window and the Secure\_note.txt file in Notepad, and paste it into the Lab Report.

6. Close the Notepad window, Decrypt/Verify Files