Project 1: SECURE EMAIL

Description:

In this project, you will learn how to provide confidentiality and integrity for your emails. To do this you will be using pretty good privacy (PGP) to encrypt and sign email correspondences.

Setup Instructions:

The steps below assume that you are using Thunderbird (version 78 and above).

- **Step 1**

  Download Thunderbird and install it. To configure Thunderbird for your email service, follow the appropriate instructions (or use those for your email provider), such as the following:

  - Gmail Thunderbird setup instructions

- **Step 2**

  Now you'll need to generate your public/private key pair. Open “Tools > OpenPGP Key Management”. From “Generate” menu, choose “New Key Pair”. Choose the email address you want to create a key for, and set a passphrase. You can set the expiration term for your key or set it to never expire, it's your choice. General advice is to have some expiration date. Hit the “Generate Key” button and wait.

- **Step 3**

  Export your public key form “File > Export Public Key(s) to File”. There are a number of keyservers which host such public keys, but for our purposes we will be using **keys.openpgp.org** so that we’ll be able to find the public keys from Thunderbird. Then go to https://keys.openpgp.org/ and submit your **public key**.

- **Step 4**

  After submitting the key, verify using the verification mail. Then search for your key from “Keyserver > Discover Keys Online” in “Tools > OpenPGP Key Management”.

Sending Encrypted/Signed Emails: (Due 11.59 pm on 21.03.2023)

- **Step 1**

  Before you can send an encrypted message to your instructor or grader, you must obtain his or her public key. Open “Tools > OpenPGP Key Management”. From “Keyserver” menu, choose “Discover Keys Online” and search for **kupcucrypto@outlook.com**. You will find the public key there, check the finger print matches **9DE0FC04A109BF72131D12E5BB789E61DC3D8BA1** and import the key.

- **Step 2**

  Compose an email. Just to avoid confusion, here is the format of the email you will have to make.

  - Make the title as "Spring 2023 Project 1 Name Surname ID"
  - For the content, please include your name, surname, and student ID as it appears in the class roster, and include **answers to the following questions.**

- How does usage of passphrase in generated keys affect security?
- How does usage of key expiration time affect security?
- How does usage of key revocation certificate affect security?
- Why do encryption and signing require two different keys?
- Are email titles encrypted? What are the consequences?

- **Step 3**

  Click the Security tab, and select both **Require Encryption and Digitally Sign This Message.**

- **Step 4**

  Click Send. You will then be prompted to select the recipient's key. Do so, and click OK. You may be prompted with questions about sending in plaintext or HTML, choose plaintext. Alternatively, you may want to disable “Compose Messages in HTML” in your “Account Settings” (not “Options” or “Preferences”) part of Thunderbird, under “Composition & Addressing”.

- **Step 5**

  You're done! Now you know how to send encrypted and signed messages.

Credits: This assignment is derived from an assignment by Chris Bronk at Rice University.