Project 1: SECURE EMAIL

Description:

In this project, you will learn how to hide your words and files, in the form of packets, from those prying eyes and ears of Eve. To do this you will be using pretty good privacy (PGP) to encrypt and sign email correspondences with your instructor or grader, using the email address you were given by them. As discussed in the textbook, Introduction to Computer Security, encryption is the process of securing communication and doing so involves just a few easy steps.

Instructions:

The first step is to determine the operating system (OS) that you will be using. Once you've completed that difficult task, it's on to using Thunderbird to encrypt your emails. You can of course use other clients to encrypt your mail, in which case, you may ignore the steps described below. The steps below assume that you are using Thunderbird.

Thunderbird (version 78.x.x and above) Setup:

Thunderbird will allow you (with a bit of tinkering) to securely send emails, through the use of an encryption algorithm, to your friend Bob. For this assignment, Bob's email address is provided at the end.

- **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. Hit the "Generate Key" button, and relax - it can take a few minutes.

- **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 you public key.

- **Step 4**

  After submitting the key, verify from the site by getting verification mail or you may try to search for your key from "Keyserver > Discover Keys Online" in "OpenPGP Key Management".

Note: For this assignment, Bob published his public key for secureemail@yandex.com in the keys.openpgp.org keyserver. The fingerprint is 9F49 5599 15D7 B84E 9124 D768 F54A C72F 7D1C FC49.

Sending Encrypted/Signed Emails: (Due 11.59 pm on 09.03.2022)

Description:

Now that you've followed these instructions, it's time to let your friend Bob know that you are capable of sending encrypted messages. Of course, this process should be done from your email account for which the public key is published.

- **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 Bob's email address. You will find the public key there, check the finger print and import it.

- **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 2022 Project 1 Name Surname ID"
  - For the content, please include your name and student ID as it appears in the class roster, and **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.

EMAIL ADDRESS: secureemail@yandex.com

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