**Lab 3. Asymmetric Encryption**

**Name:**

Submit your lab on Canvas. If you have any questions, email Dr. Vance at [anthony@vance.name](mailto:anthony@vance.name).

**Important**: To receive full credit, you must complete Part 1 of the lab by end of day **Saturday,** **September 15**, which entails setting up GPG on your computer and sending Dr. Vance (at [anthony@vance.name](mailto:anthony@vance.name)) your PGP **public** (not private) key. This is required for the PGP key signing class activity on Tuesday, February 6. Instructions for creating your PGP public key is described in the “Install PGP and Create a Public-Private Key Pair” section at the end of this document.

Part 2 of the lab is due on **Tuesday, September 25**.

**Part 1. Install PGP and Create a Public-Private Key Pair**

In this section of the lab, you will generate a PGP public-private key pair. You can do this using a variety of software, including the free implementation of PGP, GPG. For Mac users, I recommend using Apple Mail and GPG Tools (<https://gpgtools.org>). For Windows users, I recommend Gpg4Win (not the Lite version; <http://www.gpg4win.org>) in conjunction with Outlook, Thunderbird, or Claw Mail.

A setup guide for GPG Tools (for Mac users) is available at:

<http://support.gpgtools.org/kb/how-to/first-steps-where-do-i-start-where-do-i-begin>

A setup guide for Gpg4Win (Windows users) is available at:

<http://www.gpg4win.org/doc/en/gpg4win-compendium_11.html>

<https://www.gpg4win.org/doc/en/gpg4win-compendium_12.html>

(if you’re using the lab vm, you can skip to the second link).

Save/export your generated key in a text file with the extension “.asc” and email this file to Dr. Vance. With gpg4win’s Kleopatra, do this by clicking “Create a backup of your key pair,” and make sure to select the ASCII armor option.

Save this key in a text file with the extension “.asc” and send this file to Dr. Vance at [anthony@vance.name](mailto:anthony@vance.name). With gpg4win, do this by clicking “Create a backup of your key pair,” and make sure to select the ASCII armor option.

**Note**: Your PGP public key should be **4096-bits** in length. Also, make sure that your public key includes all of the email address you want to send and receive encrypted messages with. Finally, make sure that you include your first and last name so that people can look up your public key on a key server like pgp.mit.edu.

**Important**: You should end up with a .asc file that contains the following string at the top of the file:

-----BEGIN PGP PUBLIC KEY BLOCK-----

If instead your .ASC file contains the string:

-----BEGIN PGP PRIVATE KEY BLOCK-----

Then is the wrong key. Do NOT send this private key to Dr. Vance.

Finally, record your PGP fingerprint below. For example, Dr. Vance’s PGP fingerprint is:

1AE2 A6B7 638D 4F40 EC43 203E 57D7 F68C F3E0 2337

**PGP fingerprint**:

**Part 2. Understanding Asymmetric Cryptography**

**Note**: To help you answer the questions in this section, view this “RSA Algorithm” video:

<https://youtu.be/Z8M2BTscoD4>

**Key Exchange Problem**

1. Imagine 200 people wish to communicate securely using symmetric keys, one symmetric key for each pair of people. How many symmetric keys would this system use in total? (See <http://en.wikipedia.org/wiki/Metcalf%27s_law>).

**Answer:**

2. Does a 256-bit RSA key (a key with a 256-bit modulus) provide strength similar to that of a 256-bit AES key? Explain. Note: This site gives estimates for good key lengths:

<http://www.keylength.com>

**Answer:**

3. Complete encryption and decryption using the RSA algorithm, for the following data (show all work): p = 5, q = 11, e = 3, M = 9. See the “RSA Algorithm” video link above. Also:

<http://en.wikipedia.org/wiki/RSA_(cryptosystem)>

**Answer:**

4. In a public-key system using RSA, you intercept the ciphertext, C=10, sent to a user whose public key is e=5, n=35. What is the plaintext M?

**Answer:**

**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.  BYU Library: <http://search.lib.byu.edu/byu/id:byu2657194>  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.  BYU Library: <http://search.lib.byu.edu/byu/id:byu2931203>  Amazon: <http://amzn.com/0140244328> |
| 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.  BYU Library: <http://search.lib.byu.edu/byu/id:byu4424191>  Amazon: <http://amzn.com/0470474246> |