HW/Lab 1: Email Security with PGP, and Crypto

CS 336/536: Computer Network Security
DUE 09/28/2015 (11am)

- This HW/Lab assignment covers Lectures 2 to 4. Please review these thoroughly before starting to work on the assignment.
- It is a combination of a hands-on lab exercise and conceptual problems. Problem 1 is a lab exercise while the rest are conceptual problems. You are strongly encouraged to utilize your lab session to accomplish the lab exercise.
- All soft copy submissions (with answers to the problems) must be turned in via Canvas. Name your files as “Lastname_Firstname_HW1”. Please make sure that you have correctly submitted/uploaded the files.
- You can submit hand-written hard copies, if you wish. However, we would prefer that you submit soft copies. If you choose to submit hard copies in any case, please turn them into my mailbox in the CS office or hand them in just before the lecture. Please also make sure that your hand-written solutions and handwriting is legible and easy to understand.
- You must submit by the deadline – 11 am on 09/28/2015. This applies to both soft and hard copy submissions. Late submissions will not be graded.
- **You will be graded based on the correctness of your answer and also on the steps that you took to come to that answer, whenever possible and applicable.** Please try to **show all your work**, when feasible.
- **The assignment needs to be solved individually by every student.** No collaboration of any sort is allowed, unless stated otherwise. No plagiarism is allowed. Please check the course policies against misconduct (discussed in Lecture 1). When in doubt, please consult the instructor.
- Please submit early to avoid any last minute issues.
- Please do start working on the homework early and do not wait until the deadline.
A. Lab Exercise and Conceptual Problems

1. [50pts] As per the Lab Description (Section B; provided on the next page), set up a PGP email client. When done, send the TA (Abhishek Anand) a signed and encrypted email (message “Hello”) at uabcsx36.f15@gmail.com using the public key hosted on the course webpage (link: pub-key).

2. [15pts] We studied the “textbook RSA” encryption scheme in the class.
   a. [5pts] Explain the Key Generation (“KeyGen”), Encryption (“Enc”) and Decryption (“Dec”) procedures of the textbook RSA encryption scheme.
   b. [10pts] Is textbook RSA encryption a secure encryption scheme against a known plaintext attack that we discussed? Explain why or why not.

3. [15pts] Is the following statement True or False:
   “4-DES, which uses four (single) DES encryption operations in series and four independent keys – \( C = Enc(K_4, Enc(K_3, Enc(K_2, Enc(K_1, P))) \) – has an effective keyspace size of \( 2^{224} \) under the known-plaintext attack”?
   Argue your answer in details.

4. [10pts] The RSA cryptosystem serves two main purposes in PGP when sending a signed and encrypted message -- what are they?

5. [5pts] Name an algorithm commonly used to encrypt PGP email messages:

6. [5pts] PGP is characterized by three main steps. What are they, and in what order are they applied (if used)?
B. Lab Description

Pretty Good Privacy is a mechanism using which a user can sign and encrypt email messages to ensure authentication, integrity and/or non-repudiation. There are a number of implementations of PGP, such as Symantec PGP, and the freely available the Gnu Privacy Guard, which we will explore in this Lab.

At its core, PGP relies on a number of technologies including asymmetric encryption, symmetric encryption, hashing and compression in order to sign and encrypt messages. This lab assumes that you’re already familiar with the basics behind PGP (crypto basics and PGP details were already covered in prior lectures - Lectures 2-4), and will show/teach you one way to setup PGP and send signed/encrypted messages.


PGP on Linux

First, we will need to install a GPG Key management tool, on debian. You can install these with the command: 'sudo apt-get install gnupg gnupg2'

Next, we will install IceDove, which is the rebranded Thunderbird email client for Debian, using: 'sudo apt-get install icedove'
Finally, we need to install the enigmail plugin for IceDove, using: ‘sudo apt-get install enigmail’.

GnuPG will give us a tool to manage both our own public/private PGP keypairs through IceDove, in addition to the keys of others, when we import them. IceDove is our email client, and Enigmail is the Thunderbird/IceDove plugin that implements the PGP standard and allows us to send signed and encrypted emails to others.

**Basic Setup:**
First things first, we need to generate an RSA keypair that will be used for signing and encrypting our emails. For simplicity, we will create the keys using IceDove. Launch IceDove, select the options button next to the search bar (three horizontal bars), OpenPGP, and then Key Management. From here, you should be able to select Generate, and select New Key Pair. From here, you can input basic user information and the email you want to associate with this key pair. Key generation will take up to several minutes. The tool should then generate an RSA public and private key (never share the private key!). If you want to share your public key with someone else, use the Export tool to get a text file containing your public key information (it gives you an option to export your secret key, but most of the time you won’t need to do this).

**Add an Email Address:**
This can be any email address you would like, although we would recommend using your UAB account for simplicity.

**Server Settings:**
What are the ideal Mail Server settings when you need to manually setup an email client that does not support Exchange?

- Mail Setting type: IMAP
- Mail Server: mail.ad.uab.edu
- SSL is set.
- Mail Server Port: 993
- Email address: **BlazerID@uab.edu**
- Password: BlazerID password.
- Outgoing Mail Server: Relay.ad.uab.edu
- Mail Server port: 587
- SSL is set.
- Server does require you to login with your BlazerID and password.
Configuring Enigmail
In order to use your RSA keys, you will need to configure your email account to allow it to use your RSA key pair. After adding an email account to Thunderbird, go to the Options Pane and navigate to Account Settings (or right click on the account name and select Settings). Now, select the OpePGP Options tab and check the Enable PGP Support check box. From here, you should be able to select your key, and check your signing/encryption preferences. Also, for optimal PGP usage, you will probably want to adjust your email preferences to send only text emails (Uncheck the Compose Messages in HTML Format box under Composition & Addressing).

Signing an Email
Once Enigmail is configured, sending signed emails is simple. Compose an email like usual, and then select the OpenPGP button, and check the ‘Sign Email’ option. Anyone can receive a signed email, however they won’t be able to verify it without your Public Key (and ideally a plugin like Enigmail). When you send your email, you should be prompted to unlock your keyring so you can sign the message with your private key.

Encrypting an Email
Just like with signing a message, you just need to select the “Encrypt Message” box (we would recommend signing it as well). However, in order to encrypt the message, you will need the public key of your intended recipient. Again, once you hit send, it will prompt you for your keyring password (in case of signing), and then your message will be sent.

Reading Signed/Encrypted Email
If you receive an encrypted message from someone, when you select to read the message, Thunderbird/IceDove should prompt you for your keyring password in order to decrypt the message for viewing. The Enigmail plugin will automatically verify signatures from PGP encrypted/signed emails assuming you have the sender’s public key in your keyring.

As part of the lab, you may try exchanging public keys, and sending signed and encrypted emails amongst yourselves.

PGP on OS X
You will need to install a Key Management tool for your GPG Keyring, you can install GPG Suite [https://gpgtools.org/](https://gpgtools.org/).

From here, you can install Thunderbird and do the same setup as above, or integrate it into Apple Mail.
PGP on Windows
You will need to install a Key Management tool for generating and maintaining keys; GPG4Win is a good tool for this:
http://www.gpg4win.org/

From here, you can again install Thunderbird and Enigmail.