

ISA 656, Assignment 4 ***due December 10th, 11:59pm***

GENERAL INSTRUCTIONS

This homework has two parts: one part with a set of theory questions and a programming part. Programming can be done in either C or Java. Submissions should include the **annotated** source code. Programs that do not compile will get a low grade. Make sure your programs do not crash when given bad input, but rather produce a useful warning or error message and take the appropriate action (recover or quit).

SUBMISSION INSTRUCTIONS

The compressed files (either tar or zip) will be submitted using email to astavrou@gmu.edu.

A compressed (zip or tar, and gzipped) file named {your last name}-hw3.tgz or {your last name}-hw3.zip containing a subdirectory for each problem, named p1, p2, etc. Each subdirectory should contain:

- All source code, including any test programs, for the problem, if required.
- A file answering any questions posed.
- Any additional files required.

Please make sure that you send me a **single compressed file with all the documents and code. The compressed file should not exceed 1MB.**

THEORY/WRITTEN QUESTIONS (40 points)

- 1) List all the different types of Denial of Service (DoS) attacks for networked applications and mechanisms to defend against them.
- 2) Why do we implement several different forms of encryption when we protect Voice over IP (VoIP) systems and more specifically SIP?
- 3) How do we protect wireless communications against eavesdropping?
- 4) What are the current security problems with Domain Name Service? Are there any proposed solutions?

PROGRAMMING (80 points)

Create a secure IMAP client using code from the previous assignments and the JavaMail API from sun:

<http://java.sun.com/products/javamail/javadocs/index.html>

The client will allow mail encryption and signing based on known public and private keys. In detail, the client should be able to:

- a) Connect to the IMAP server using the Simple Authentication and Security Layer (SASL) (part of JavaMail package) and establish a secure communication channel.
- b) Retrieve the mail from the IMAP server, and store it locally encrypted.
- c) If the received mail is encrypted and the key of the recipient is known, the mail should be decrypted, displayed and then re-encrypted with the user's key.
- d) If a mail is signed then the mail is going to be displayed with the indication signed.