COMP7481 April 2020

“Take-Home” Final Exam

Designing a Cryptographic System

# Overview:

Propose an experimental system, using the algorithms and techniques we have learnt in this course.

In this system there are two parties, Bob and Alice, who live far away, but wish to communicate with each other. Here are some possible elements of the system:

1. Symmetric key
2. Asymmetric keys
3. Passphrase (for private key)
4. Keyed hash
5. Salted hash
6. Some enemy (Eve)
7. Other

References on how to generate keys with openssl

<https://developers.yubico.com/PIV/Guides/Generating_keys_using_OpenSSL.html>

<https://rietta.com/blog/2012/01/27/openssl-generating-rsa-key-from-command/>

<https://www.czeskis.com/random/openssl-encrypt-file.html>

An example scenario:

1. Person1 generates an RSA public key, and private key
2. Person1 emails the public key to Person2
3. Person2 generates a symmetric key to encrypt a big file with AES
4. Person2 uses the public key to encrypt a symmetric key
5. Person2 emails the encrypted symmetric key to Person1, and the encrypted file
6. Person1 decrypts symmetric key, and decrypts big file

# Your Task and Submission:

**Prepare one report document that includes the following:**

1. Propose a system (goals, objective, big picture, key elements)

Prepare a diagram to capture what you system includes.

1. Scenario walkthrough (step by step, chronological order)

As you mimic yourself being each of the persons in the system, document what you do, and see.

You must clearly describe everything that you type and see, step by step.

For each person in the system, explain:

* 1. What you did, What you typed, What you see
  2. Use screen captures and annotations to demonstrate these steps

1. Discussion and conclusions
   1. Discuss key observations, pros and cons of your system, such as:
      1. confidentiality,
      2. integrity,
      3. authentication,
      4. cost/speed
   2. Concluding thoughts

**Submit ONE zip folder.**

It should include one sub-folder for each “person” in the system, to have:

* All the files used for by that “person”.
* A makefile (or bash file) that includes the commands that you typed during your experiment, so that we can reproduce or repeat the experiment again.
* A README file to describe what all the samples files are.