Data and Information Security

Project Requirement

Form a team

- Form a team of 1 – 3 people to complete the final project.
- The project has 100pts

Program project

- Write a program with GUI that
  - takes a plaintext/cipheretxt as input and outputs the encryption/decryption result using a secret key cryptography method like AES.
  - takes a plaintext/ciphertext as input and outputs the encryption/decryption result using a public key cryptography method like RSA
  - Takes a plaintext as input and outputs its digital signature
  - Takes a message with digital signature as input and outputs the verification result.
  - Takes a plaintext as input and outputs its hash (MD5 or SHA256)

Program project

- You can directly use the crypto functions/classes offered by a crypto library to encrypt/decrypt/sign verify/compute hash, etc.
- You get extra **10 points** if you chose to design a secure instant messaging tool for Alice and Bob instead of this project

Program project with bonus points

- Design a secure instant messaging tool for Alice and Bob. The system supports the following functions
  - Alice and Bob can use the tool to send instant messages to each other.
  - Alice and Bob share the same password (or passphrase), they must use the password to set up the tool to correctly encrypt and decrypt messages shared between each other.
  - Each message during Internet transmission must be encrypted

Program project with bonus points

- You can use any computer language (Java, C++, Python)
- You can leverage any existing open-source software, tools, or commands (e.g., md5sum, sha1sum) to design the system.
- A graphical user interface (GUI) is preferred.
  - When send a message, display the sent ciphertext. When receive a message, display the received ciphertext and decrypted plaintext

Program project with bonus points

- Some design issues you need to think about:
- What cipher you should use?
- DONOT directly use the password as the key, how can you generate the same key between Alice and Bob to encrypt messages?
- How should Alice and Bob set up an initial connection and also maintain the connection with each other on the Internet?

Format requirements

- Final report (due on Dec/5)
  - at least 5 pages, at most 1.5 line spacing, using Time New Roman, 11pt.
  - Describe what you have done for this project, the main components of your project, the evaluation results, etc.

Schedule

- I plan to start the first lab on Sep/28
- Before we do the lab, TA will introduce you the steps to setup lab environment, and the tasks for the first lab

Schedule

- Our class meetings on Sep/28, Sep/30, Oct/05, Oct/07 are set aside for lab guidance.
- Please bring your laptop to the classroom to complete the lab.
- If you cannot come to the classroom, TA will upload a video that shows you how to complete the lab in a step-by-step way. Please watch the video and complete the lab at home.
- You first lab report is due on Oct/08

About the Midterm

- This is a take-home exam.
  - Exam will start at 12:30pm on Oct 14
  - Please check out exam materials from Canvas-> Files -> Midterm
  - Please submit your solution to Canvas by 12:30pm on Oct 15

Form of the exam

- Midterm is in the form of a reading assignment
- You will be assigned an academic paper about information and data security
- Read this paper and answer questions about this paper
- Open book, notes, computer, and internet, but closed friends.