Project #2

Course: Security and Privacy

Fall 2020

Project description

In this project, you are required to design and implement a small security application **built on top of the DES implementation** that you have just completed in Project #1. You may also choose to carry out some in-depth study of the encryption/decryption algorithm(s). Possible topics for you to work on include, but are not limited to:

(1) **Secret-key based key exchange**: The goal is for two users (communication parties) to establish a shared secret key with the help of a trusted third party. Through a user interface, you need to demonstrate key establishment as well as the two users' sending and receiving encrypted messages using the established secret key. Some inputs through the user interface include: passwords of the two users that are shared with the trusted third party, a message (or a file) for encryption and decryption. Possible outputs from the user interface include: the shared session key (when it is successful), the message in clear and in encrypted format at various stages of the communication.

(2) **Secure communication**: The goal is to encrypt the data transferred between two or more users who are engaging in an interactive session of data exchange. Through a user interface, you need to demonstrate sending and receiving data (or file) which should be independent from each other and the data (or files) in transmission must be encrypted.

(3) **Performance comparison between different operation modes of DES and AES**: The goal is to study the performance of encryption algorithms of the same type or algorithms with different operation modes. The evaluation criterion is the amount of time that it takes to complete encryption (or decryption) of a message. You need to use a set of messages of variable sizes for your experiment to reach a conclusion.

(4) **Performance comparison between DES and RSA**: The goal is to study the performance of the two encryption algorithms of different types, i.e., secret key based algorithm and public key based algorithm. Again, the evaluation criterion is the amount of time that it takes to complete encryption (or decryption) of a message. You need to use a set of messages of variable sizes to reach a conclusion.

(5) **Your own choice**: The purpose is for you to work on a project of your own choice as long as it is related to Project #1 with comparable scale.

Requirements

There is no specific requirement on the development environment or tools that you may use to complete this project. As the outcome of this project, you are required to:

(1) clearly describe the goal of your work as well as the design;

(2) implement the application.

(3) design and implement a user-friendly interface to demonstrate the usability of your application.

Deliverables

(1) Source code of your implementation (soft copy);

(2) A report describing the architecture, design and the implementation of the application itself as well as the user interface or the experiment and the conclusion.

Demonstration

In person, a demonstration is required during which you will be asked to run the application or the experiment and demonstrate the results through a user-friendly interface.

Due date

Project due date (demo & deliverables): Friday, Nov. 13, 2020.

Grading

Correctness of the implementation: 50%;
Friendliness of the user interface: 20%;
Documentation (project report + comments in the source code): 30%.

Warning

Copying somebody else's work is strictly prohibited. If caught, both the offender and the conspirator will be asked to provide an explanation and, depending on the seriousness of the offense, may be penalized for dishonesty.