PV204- Security Technologies

Project - "Password Based Key Generation Function using Java Card" (PBKGFJ)

Phase-1

Description - Draft

1. As suggested in the seminar, to get a jump start in the project work, an internet survey was conducted.
2. Several skeleton Java framework applications were analyzed and tested. Subsequently, a skeleton framework of a Java project was found suitable for our work and was downloaded from the internet. The website address of the skeleton project "Cryptbox" is as follows:

   https://www.codeproject.com/articles/546069/cryptbox
3. After examining the source code and executing the executable, it was observed that the following functionalities are incorporated into the Cryptbox:
4. The project allows the users to select a file to be encrypted and asks user to enter a password. Then it adds a 64 bit random number salt to the password and generates a 128 bit MD5 hash. This hash is finally used as key to encrypt the user file using DES algorithm.
5. By utilizing the Cryptbox frame work, our project "Password Based Key Generation Function using Java Card" (PBKGFJ) will be implemented.
6. Following are the proposed functionalities to be implemented as a part of the project:
   a. Providing the GUI to user.
   b. Allowing the user to select a file to be encrypted.
   c. Ask the user to enter password (could be 4 digits).
   d. Combine this password P with locally generated number L which results to a number R.
   e. Establish connection with Java card.
   f. Send the number R to java card to carryout secret key generation using AES algorithm in Java applet. This secret key will be sent to PC application. The PC application will use this secret key as DES key to encrypt/decrypt the user file.
7. Subsequent to the implementation, the project will be submitted for review.