CmpE 526 Operating System and Network Security, Spring 2017, Dr. M. Ufuk Çağlayan
Term Project 2, Assigned: 13.04.2017 Thursday, Due: End of Final Exam, as scheduled

PLEASE READ CAREFULLY

Design then implement and test a C or C++ or Java program to encrypt and decrypt first a single file, then a directory of files in a recursive manner. Your program should be able to authenticate the user by public key cryptography (private key and public key, public key not necessarily by a certificate), then use any symmetric encryption/decryption algorithm (of course, for performance reasons) as a black-box subprogram to actually provide confidentiality. You must implement your program to work with encryption/decryption algorithms of your choice. You can use implementations of public key encryption/decryption algorithms and symmetric encryption/decryption algorithms/modes already available in Internet, but you MUST provide references about implementations you use.

Assume the user will have his/her private and public key pair (very large keys, whose length will be selected by you) stored in two files, of course the private key in a secure manner, for example on USB memory, and will be used by your program on its demand. Your program should be capable of creating private/public key pairs (how?), and encode/decode (how?) the private key by using a short (say 8 characters) passphrase (=password) and store the private key in an encrypted file so that the physical theft of the private key file on some external memory (ie USB flash memory) will not result in private key disclosure (Also, discuss the implications of this approach, especially the movement of the private key between the PC and external memory). The user must be able to use multiple private and public key pairs (Keybags, PGP key ring concept?), obviously for different purposes according to different confidentiality needs of the user. Note that, the user must remember only one passphrase (=password) for all of her/his key pairs. Moreover, the key to be used by symmetric encryption/decryption algorithm is to be generated by your program (do you need to store this key on external memory ? Under which conditions? Discuss…!)

You must measure the performance of your program and report on how long it will take to encode/decode files/directories of sizes of the order 1M, 10M, 100M, 1G, 10G and 100G bytes and under which conditions (processor, memory size, OS, middleware/crypto API, etc).

Your final project document on paper should include all of your assumptions, the logic and the design of your software, all of your design decisions (design specifications document), the whole source code and a discussion of pros and cons of your approach plus the strengths and weaknesses of the encryption techniques together with a discussion of key management and performance of your program. The whole source code and binaries together with the soft copy of your final project document should be emailed to me in a single zip/rar file whose name will be **YourLastname-CMPE526-Project-2.zip**. Alternatively, you can provide a CD. Assume your program will work preferably on Windows PC's with a simple and reasonable interface, but LINUX machines are also OK. I will prefer a demonstration of your software, if you can give me a demo in a few days following the due date.

Notes:

- **All students work individually, THAT MEANS ALONE, to produce answers.**
- **You must turn in your answers in paper form, except that you additionally supply files as described above.**
- **Copy/paste from Internet resources without clear references are strictly prohibitied and will be punished (that is, you get ZERO for the project).**